Quality of Service auf Catalyst Switches der Serie 6000

Inhalt

Einführung

In diesem Dokument werden die Quality of Service (QoS)-Funktionen erläutert, die in den Catalyst Switches der Serie 6000 verfügbar sind. Dieses Dokument behandelt QoS-Konfigurationsfunktionen und enthält einige Beispiele für die Implementierung von QoS.

Dieses Dokument ist nicht als Konfigurationsleitfaden gedacht. In diesem Whitepaper werden Konfigurationsbeispiele verwendet, um die Erläuterung der QoS-Funktionen der Hardware und Software der Catalyst 6000-Familie zu erleichtern. Die Syntaxreferenz für QoS-Befehlsstrukturen finden Sie in den folgenden Konfigurations- und Befehlshandbüchern für die Catalyst 6000-Familie:

- Catalyst Switches der Serie 6500

Definieren von Layer-2-QoS

Viele denken zwar, dass QoS in Layer-2-Switches (L2-Switches) lediglich auf die Priorisierung von Ethernet-Frames abzielt, aber nicht viele wissen, dass dies viel mehr bedeutet. L2-QoS umfasst Folgendes:

1. **Terminierung der Eingabewarteschlange:** Wenn der Frame in den Port eingeht, kann er einer von mehreren portbasierten Warteschlangen zugewiesen werden, bevor er an einen Ausgangsport umgestellt wird. In der Regel werden mehrere Warteschlangen

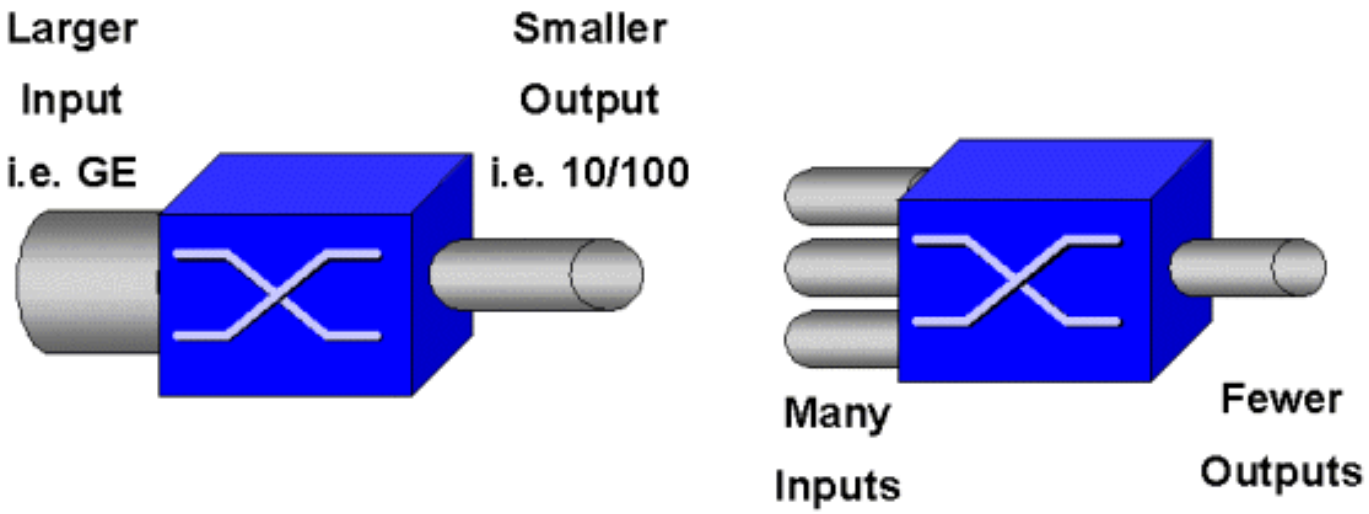
verwendet, wenn für unterschiedlichen Datenverkehr unterschiedliche Servicelevel erforderlich sind oder die Latenz des Switches auf ein Minimum beschränkt werden muss. IP-basierte Video- und Sprachdaten erfordern beispielsweise eine geringe Latenz. Daher müssen diese Daten ggf. umgestellt werden, bevor andere Daten wie File Transfer Protocol (FTP), Web, E-Mail, Telnet usw. gewechselt werden.

2. **Klassifizierung:** Zur Klassifizierung werden verschiedene Felder im Ethernet-L2-Header sowie Felder im IP-Header (Layer 3 (L3)) und im Transmission Control Protocol/User Datagram Protocol (TCP/UDP)-Header (Layer 4 (L4)) überprüft, um die Service-Level zu ermitteln, die beim Transit des Switches auf den Frame angewendet werden.
3. **Richtlinienvergabe:** Bei der Richtlinienvergabe wird ein Ethernet-Frame überprüft, um festzustellen, ob er innerhalb eines bestimmten Zeitrahmens eine vordefinierte Datenverkehrsrate überschritten hat (in der Regel handelt es sich bei diesem Zeitrahmen um eine feste Nummer innerhalb des Switches). Wenn dieser Frame außerhalb des Profils liegt (d. h. er ist Teil eines Datenstreams, der die vordefinierte Ratengrenze überschreitet), kann er entweder verworfen oder der CoS-Wert (Class of Service) wird deaktiviert.
4. **Umschreiben:** Der Prozess der Umschreibung ist die Möglichkeit des Switches, die CoS im Ethernet-Header oder die Type of Service (ToS)-Bits im IPV4-Header zu ändern.
5. **Ausgabewarteschlangenplanung:** Nach der Umschreibung legt der Switch den Ethernet-Frame in eine geeignete Ausgangswarteschlange für das Switching. Der Switch führt eine Pufferverwaltung für diese Warteschlange durch, indem er sicherstellt, dass der Puffer nicht überläuft. Dazu wird in der Regel ein Random Early Discard (RED)-Algorithmus verwendet, bei dem beliebige Frames aus der Warteschlange entfernt (verworfen) werden. Weighted RED (WRED) ist ein Derivat von ROT (wird von bestimmten Modulen der Catalyst 6000-Familie verwendet), bei dem die CoS-Werte überprüft werden, um festzustellen, welche Frames verworfen werden. Wenn die Puffer vordefinierte Schwellenwerte erreichen, werden Frames mit niedrigerer Priorität normalerweise verworfen, sodass die Frames mit höherer Priorität in der Warteschlange verbleiben.

In diesem Dokument werden die oben genannten Mechanismen und ihre Beziehung zur Catalyst 6000-Familie in den folgenden Abschnitten genauer erläutert.

Die Notwendigkeit von QoS in einem Switch

Große Backplane, Millionen von Switch-Paketen pro Sekunde und blockierungsfreie Switches sind heute alle gleichbedeutend mit vielen Switches. Warum QoS? Die Antwort liegt in der Überlastung.



Ein Switch ist möglicherweise der schnellste Switch der Welt. Wenn Sie jedoch eines der beiden in der Abbildung oben gezeigten Szenarien haben, tritt eine Überlastung des Switches auf. Wenn die Funktionen für das Überlastungsmanagement in Zeiten einer Überlastung nicht vorhanden sind, werden Pakete verworfen. Wenn Pakete verworfen werden, werden sie erneut übertragen. Bei erneuten Übertragungen kann sich die Netzwerkauslastung erhöhen. In Netzwerken, die bereits überlastet sind, kann dies zu bestehenden Leistungsproblemen und möglicherweise zu einer weiteren Leistungsminderung führen.

Bei konvergenten Netzwerken ist das Engpassmanagement sogar noch wichtiger. Latenzanfälliger Datenverkehr wie Sprache und Video kann bei auftretenden Verzögerungen erheblich beeinträchtigt werden. Durch das Hinzufügen weiterer Puffer zu einem Switch werden auch Überlastungsprobleme nicht unbedingt verringert. Der latenzempfindliche Datenverkehr muss so schnell wie möglich gewechselt werden. Zunächst müssen Sie diesen wichtigen Datenverkehr mithilfe von Klassifizierungsverfahren identifizieren und dann Puffermanagement-Techniken implementieren, um zu verhindern, dass Datenverkehr mit höherer Priorität während einer Überlastung verworfen wird. Schließlich müssen Sie Planungstechniken integrieren, um wichtige Pakete so schnell wie möglich aus Warteschlangen zu wechseln. Wie Sie in diesem Dokument lesen werden, implementiert die Catalyst 6000-Familie all diese Techniken, wodurch das QoS-Subsystem zu einem der umfassendsten der Branche geworden ist.

Alle im vorherigen Abschnitt beschriebenen QoS-Techniken werden im gesamten Dokument genauer untersucht.

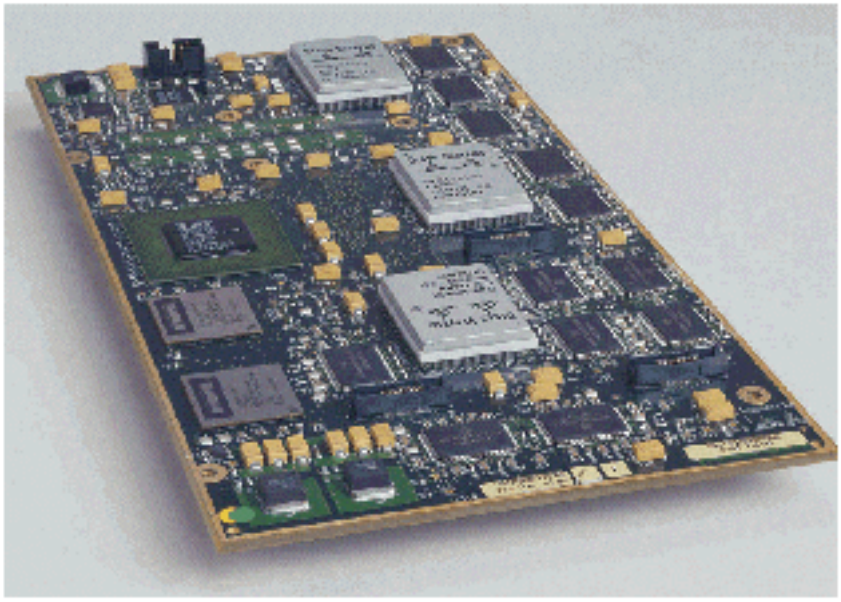
Hardwareunterstützung für QoS in der Catalyst 6000-Familie

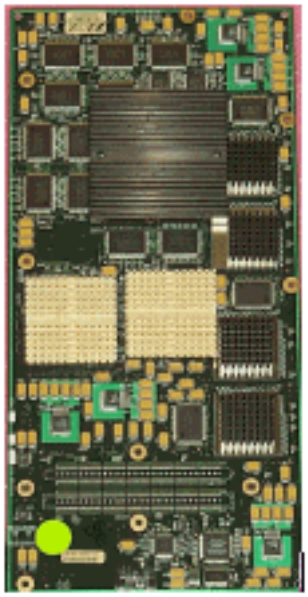
Zur Unterstützung von QoS in der Catalyst 6000-Familie ist ein gewisser Hardware-Support erforderlich. Die Hardware, die QoS unterstützt, umfasst die Multilayer Switch Feature Card (MSFC), die Policy Feature Card (PFC) und die Port Application Specific Integrated Circuits (ASICs) auf den Linecards selbst. In diesem Dokument werden die QoS-Funktionen der MSFC nicht behandelt, sondern die QoS-Funktionen der PFC und der ASICs auf den Linecards behandelt.

PFC

Die PFC-Version 1 ist eine Tochterkarte, die sich auf der Supervisor I (SupI) und der Supervisor IA (SupIA) der Catalyst 6000-Familie befindet. Der PFC2 ist ein Re-Spin des PFC1 und wird mit dem

neuen Supervisor II (SupII) und einigen neuen integrierten ASICs ausgeliefert. Während sowohl PFC1 als auch PFC2 hauptsächlich für die Hardwarebeschleunigung von L3-Switching bekannt sind, ist QoS einer ihrer weiteren Zwecke. Die PFCs sind unten aufgeführt.





Obwohl PFC 1 und PFC2 im Wesentlichen identisch sind, gibt es einige Unterschiede bei der QoS-Funktionalität. Der PFC2 fügt nämlich Folgendes hinzu:

1. Möglichkeit zum Herunterdrücken der QoS-Richtlinie auf eine Distributed Forwarding Card (DFC).

2. Richtlinienentscheidungen sind etwas anders. Sowohl PFC1 als auch PFC2 unterstützen normale Richtlinien, bei denen Frames verworfen oder markiert werden, wenn eine Aggregat- oder Microflow-Richtlinie eine Out-of-Profile-Entscheidung zurückgibt. Der PFC2 bietet jedoch Unterstützung für einen Überhang, was auf eine zweite Richtlinienebene hinweist, auf der Richtlinienaktionen ausgeführt werden können.

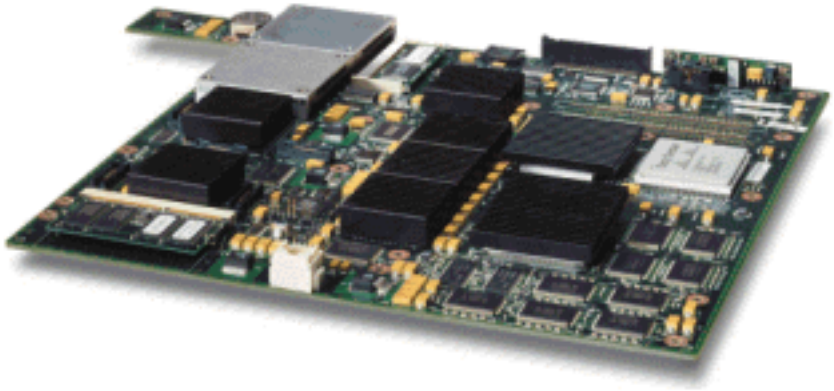
Wenn eine Richtlinie für Überschreitungen definiert wird, können Pakete verworfen oder markiert werden, wenn sie die Überschreitungsrate überschreiten. Wenn eine übermäßige Richtlinienebene festgelegt wird, wird die übermäßige DSCP-Zuordnung verwendet, um den ursprünglichen DSCP-Wert durch einen markierten Wert zu ersetzen. Wenn nur eine normale

Polizeistufe festgelegt ist, wird die normale DSCP-Zuordnung verwendet. Bei der Festlegung beider Polizeistufen wird die übermäßige Polizeiebene vorrangig die Kartenregeln auswählen.

Es ist zu beachten, dass die in diesem Dokument beschriebenen QoS-Funktionen, die von den genannten ASICs ausgeführt werden, eine hohe Leistung bieten. Die QoS-Leistung in einer Catalyst 6000-Basisfamilie (ohne Switch Fabric-Modul) ergibt 15 MPPS. Bei Verwendung von DFCs können zusätzliche Leistungssteigerungen für QoS erzielt werden.

DFC

Die DFC kann optional an den WS-X6516-GBIC angeschlossen werden. Es handelt sich jedoch um ein Standardgerät auf der WS-X6816-GBIC-Karte. Sie kann auch auf anderen zukünftigen Fabric-Linecards wie der kürzlich eingeführten Fabric 10/100-Linecard (WS-X6548-RJ45), der Fabric RJ21-Linecard (WS-X6548-RJ21) und der 100FX-Linecard (WS-X6652) unterstützt werden. (4-MM-FX). Die DFC ist unten dargestellt.



Mit der DFC kann die Fabric-Linecard (mit Crossbar verbunden) lokales Switching durchführen. Dazu müssen alle für den Switch definierten QoS-Richtlinien unterstützt werden. Der Administrator kann die DFC nicht direkt konfigurieren. Stattdessen wird sie vom Master MSFC/PFC auf dem aktiven Supervisor gesteuert. Die primäre PFC drückt eine FIB-Tabelle (Forwarding Information Base) nach unten, die der DFC ihre L2- und L3-Weiterleitungstabellen zuweist. Außerdem wird eine Kopie der QoS-Richtlinien heruntergeladen, sodass diese auch lokal auf der Linecard vorhanden sind. Im Anschluss daran können lokale Switching-Entscheidungen auf die lokale Kopie aller QoS-Richtlinien verweisen, die Hardware-QoS-Verarbeitungsgeschwindigkeiten bereitstellen und durch verteiltes Switching eine höhere Leistung erzielen.

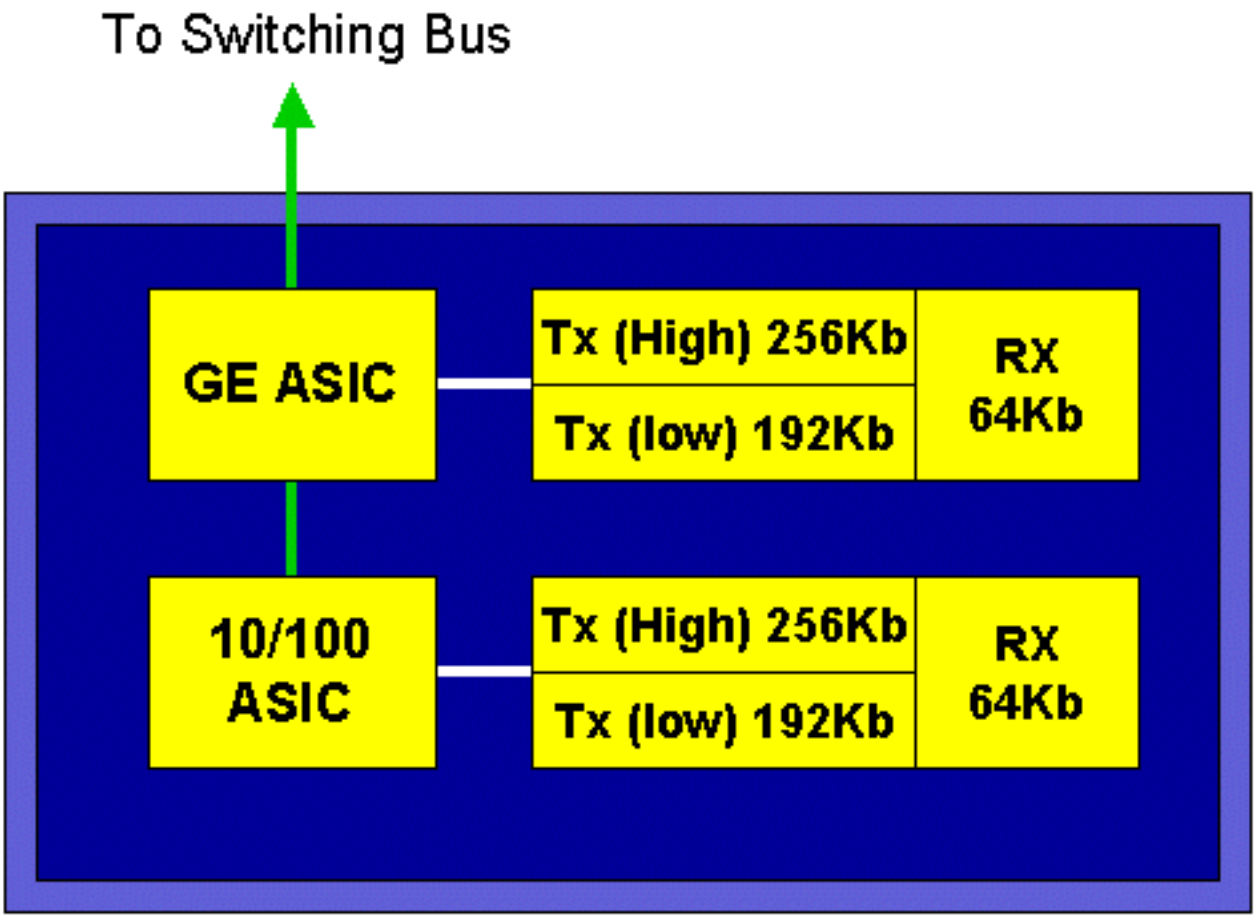
Port-basierte ASICs

Um das Hardwarebild zu vervollständigen, implementiert jede Linecard eine Reihe von ASICs. Diese ASICs implementieren die Warteschlangen, Puffer und Schwellenwerte, die für die temporäre Speicherung von Frames während der Übertragung des Switches verwendet werden. Auf den 10/100-Karten wird eine Kombination aus ASICs verwendet, um die 48 10/100-Ports bereitzustellen.

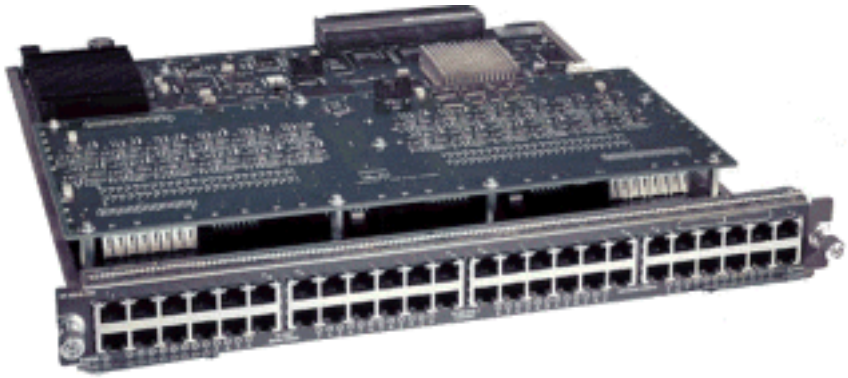
Original 10/100 Line Cards (WS-X6348-RJ45)

Die 10/100 ASICs stellen eine Reihe von Empfangs- (Rx) und Übertragungswarteschlangen (TX) für jeden 10/100-Port bereit. Die ASICs bieten eine Pufferung von 128.000 pro 10/100-Port. In den Versionshinweisen finden Sie weitere Informationen dazu, welche Port-Pufferung für die einzelnen Linecards verfügbar ist. Jeder Port auf dieser Linecard unterstützt eine Rx-Warteschlange und

zwei TX-Warteschlangen, die als hoch und niedrig gekennzeichnet sind. Dies ist im Diagramm unten dargestellt.



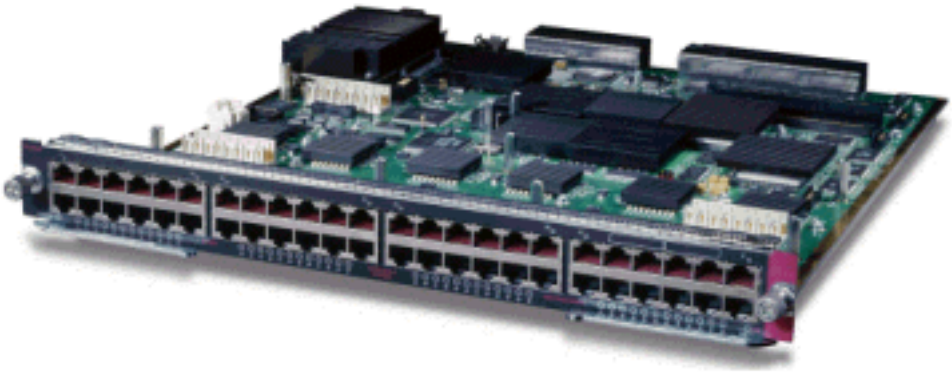
Im obigen Diagramm bietet jeder 10/100-ASIC ein Breakout für 12 10/100-Ports. Für jeden 10/100-Port werden 128.000 Puffer bereitgestellt. Die 128.000 Puffer sind auf die drei Warteschlangen aufgeteilt. Die in der Warteschlange gezeigten Zahlen sind nicht die Standardwerte. Sie stellen jedoch eher dar, was konfiguriert werden könnte. Die einzelne Rx-Warteschlange erhält 16 K, und der verbleibende Speicher (112 K) wird auf die beiden Tx-Warteschlangen aufgeteilt. In der Standardeinstellung (in CatOS) erhält die Warteschlange mit hoher Priorität 20 % dieses Raumes und die untere Warteschlange 80 %. In Catalyst IOS wird standardmäßig eine Warteschlange mit 10 % und eine niedrige Warteschlange mit 90 % festgelegt.



Während die Karte eine zweistufige Pufferung bietet, kann während der QoS-Konfiguration nur eine 10/100-ASIC-basierte Pufferung bearbeitet werden.

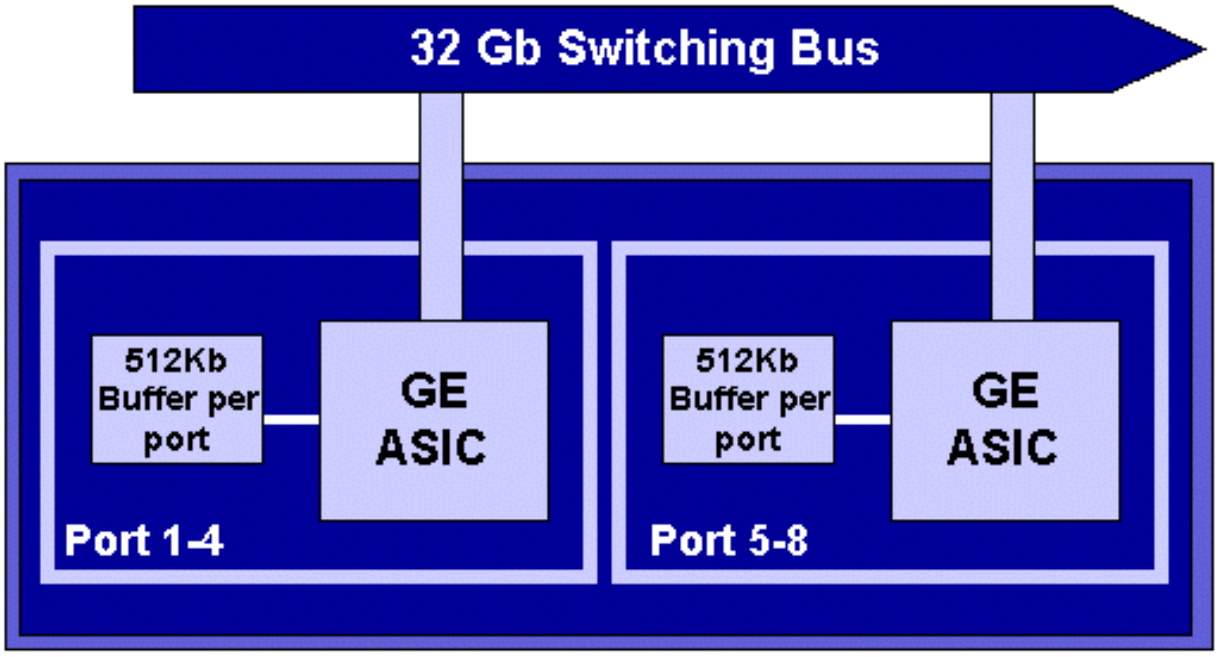
Fabric 10/100 Line Cards (WS-X6548-RJ45)

Die neuen 10/100-ASICs bieten eine Reihe von Rx- und TX-Warteschlangen für jeden 10/100-Port. Die ASICs stellen einen gemeinsamen Speicher-Pool bereit, der über die 10/100-Ports verfügbar ist. In den Versionshinweisen finden Sie weitere Informationen dazu, welche Port-Pufferung für die einzelnen Linecards verfügbar ist. Jeder Port auf dieser Linecard unterstützt zwei Rx-Warteschlangen und drei TX-Warteschlangen. Eine Rx-Warteschlange und eine TX-Warteschlange werden als absolute Prioritätswarteschlange bezeichnet. Diese Funktion dient als Warteschlange mit niedriger Latenz und eignet sich besonders für latenzempfindlichen Datenverkehr wie Voice over IP (VoIP).

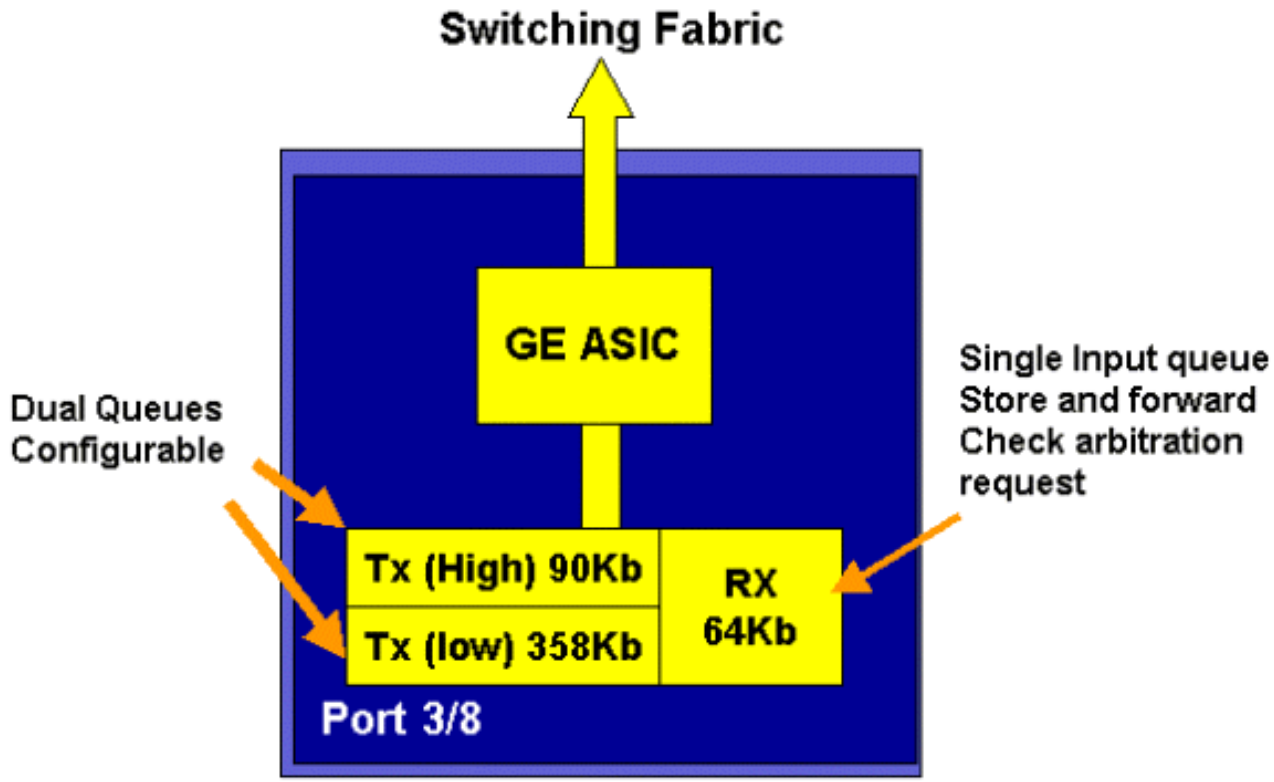


GE Line Cards (WS-X6408A, WS-X6516, WS-X6816)

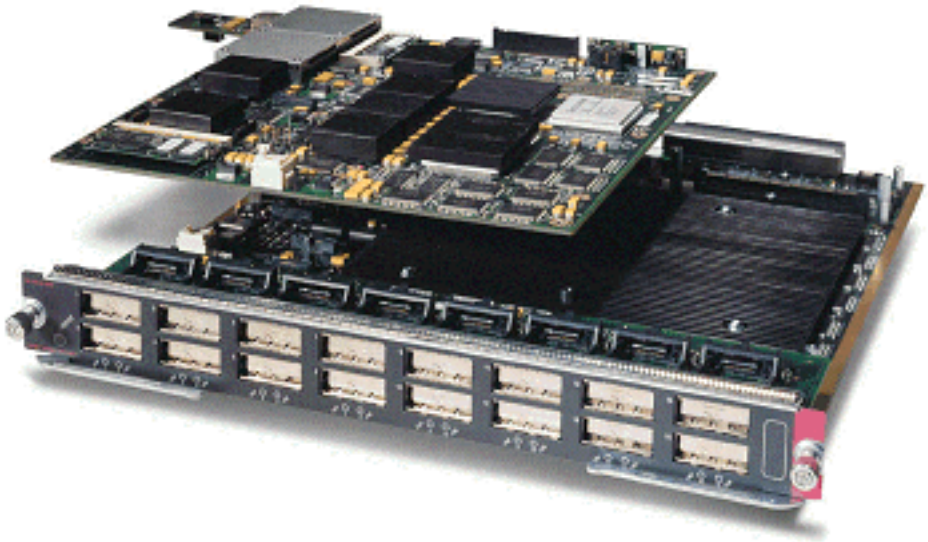
Für GE Line Cards bietet der ASIC eine Pufferung von 512 K pro Port. Eine Darstellung der GE-Linecard mit acht Ports ist im folgenden Diagramm dargestellt.



Wie bei den 10/100-Ports verfügt jeder GE-Port über drei Warteschlangen, eine Rx- und zwei TX-Warteschlangen. Dies ist der Standardwert auf der WS-X6408-GBIC-Linecard und wird im folgenden Diagramm dargestellt.



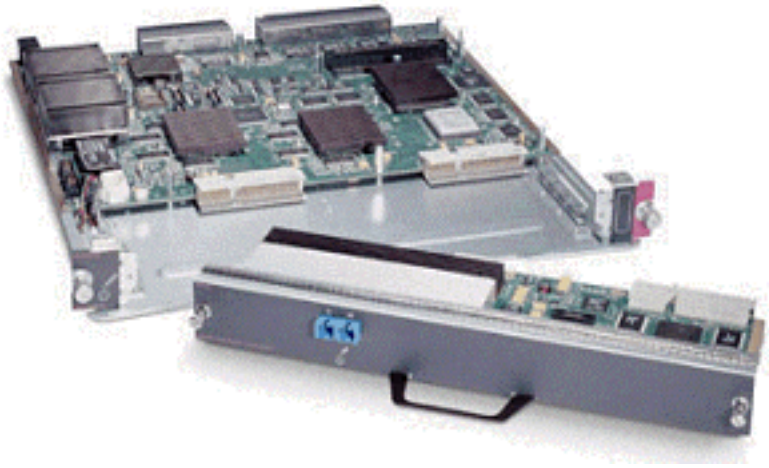
Auf den neueren Line 16-Port-GE-Karten, den GBIC-Ports der SupIA- und SupII-GE-Karte und der WS-X6408A-GBIC-GE-Karte mit 8 Ports sind zwei zusätzliche Strict Priority (SP)-Warteschlangen verfügbar. Eine SP-Warteschlange wird als Rx-Warteschlange und die andere als TX-Warteschlange zugewiesen. Diese SP-Warteschlange wird primär für latenzempfindlichen Datenverkehr wie Sprache in Warteschlangen verwendet. In der SP-Warteschlange werden alle Daten, die in diese Warteschlange gestellt werden, verarbeitet, bevor die Daten in den Warteschlangen mit hoher und niedriger Priorität gespeichert werden. Nur wenn die SP-Warteschlange leer ist, werden die Warteschlangen für hohe und niedrige Anforderungen bedient.



10-GE-Line Cards (WS-X6502-10GE)

In der zweiten Jahreshälfte 2001 führte Cisco eine Reihe von 10-GE-Line Cards ein, die einen 10-GE-Port pro Line Card bereitstellen. Dieses Modul belegt einen Steckplatz des 6000-Chassis. Die 10-GE-Linecard unterstützt QoS. Für den 10-GE-Port werden zwei Rx-Warteschlangen und drei

TX-Warteschlangen bereitgestellt. Eine Rx-Warteschlange und eine TX-Warteschlange werden jeweils als SP-Warteschlange bezeichnet. Für den Port ist außerdem eine Pufferung vorgesehen, die insgesamt 256 K Rx-Pufferung und 64 MB TX-Pufferung bietet. Dieser Port implementiert eine 1p1q8t-Warteschlangenstruktur für die Rx-Seite und eine 1p2q1t-Warteschlangenstruktur für die TX-Seite. Warteschlangenstrukturen werden später in diesem Dokument erläutert.



Catalyst 6000-Familie - QoS-Hardware - Zusammenfassung

Die Hardwarekomponenten, die die oben genannten QoS-Funktionen in der Catalyst 6000-Familie ausführen, sind in der nachfolgenden Tabelle aufgeführt.

QoS Process	Catalyst 6500 Component that performs function
Input Scheduling	Performed by port ASIC's L2 only with or without the PFC
Classification	Performed by Supervisor or PFC L2 only is done by Supervisor L2/3 is done by PFC
Policing	Done by PFC via L3 forwarding Engine
Packet Re-write	Done by port ASIC's L2/L3 based on classification done in point 2 above
Output Scheduling	Done by port ASIC's L2/L3 based on classification done in point 2 above

Software-Support für QoS für die Catalyst 6000-Produktfamilie

Die Catalyst 6000-Familie unterstützt zwei Betriebssysteme. CatOS, die ursprüngliche Softwareplattform, wurde von der auf der Catalyst 5000-Plattform verwendeten Codebasis abgeleitet. Kürzlich hat Cisco das integrierte Cisco IOS ® (Native Mode) (ehemals Native IOS) eingeführt, das eine vom Cisco Router IOS abgeleitete Codebasis verwendet. Beide Betriebssystemplattformen (CatOS und Integrated Cisco IOS (Native Mode)) implementieren Softwareunterstützung zur Aktivierung von QoS auf der Catalyst 6000-Switch-Plattform unter Verwendung der in den vorherigen Abschnitten beschriebenen Hardware.

Hinweis: In diesem Dokument werden Konfigurationsbeispiele aus beiden Betriebssystemplattformen verwendet.

Prioritätsmechanismen in IP und Ethernet

Damit QoS-Services auf Daten angewendet werden können, muss es möglich sein, ein IP-Paket oder einen Ethernet-Frame zu kennzeichnen oder zu priorisieren. Dazu werden die ToS- und die CoS-Felder verwendet.

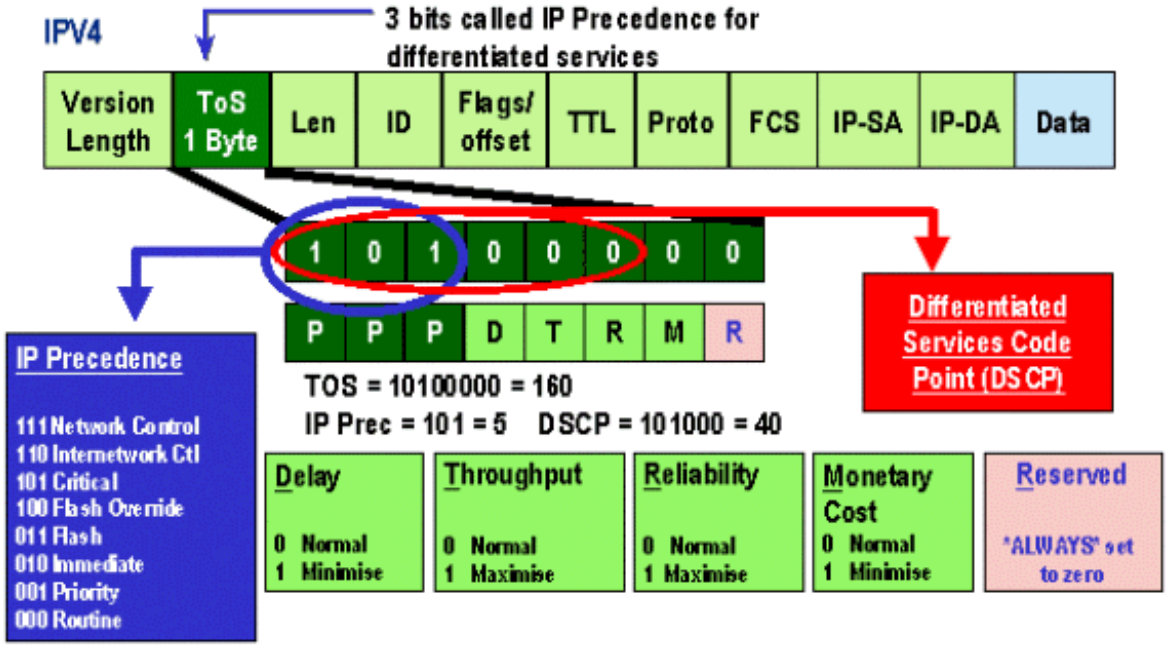
ToS

ToS ist ein 1-Byte-Feld, das in einem IPV4-Header vorhanden ist. Das ToS-Feld besteht aus acht Bit, von denen die ersten drei Bit verwendet werden, um die Priorität des IP-Pakets anzugeben. Diese ersten drei Bits werden als IP-Rangfolgebits bezeichnet. Diese Bits können von null auf sieben festgelegt werden, wobei 0 die niedrigste Priorität und sieben die höchste Priorität ist. Seit vielen Jahren wird in IOS Unterstützung für die Festlegung von IP-Rangfolgen angeboten. Die Unterstützung für das Zurücksetzen der IP-Rangfolge kann von der MSFC oder der PFC (unabhängig von der MSFC) erfolgen. Bei einer Vertrauenseinstellung von nicht vertrauenswürdigen Benutzern können auch alle IP-Prioritätseinstellungen eines eingehenden Frames gelöscht werden.

Folgende Werte können für die IP-Rangfolge festgelegt werden:

IP Precedence bits	IP Precedence Value
000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internetwork Control
111	Network Control

Das Diagramm unten stellt eine Darstellung der IP-Prioritätsbits im ToS-Header dar. Die drei höchstwertigen Bits (MSB) werden als IP-Rangfolgebits interpretiert.



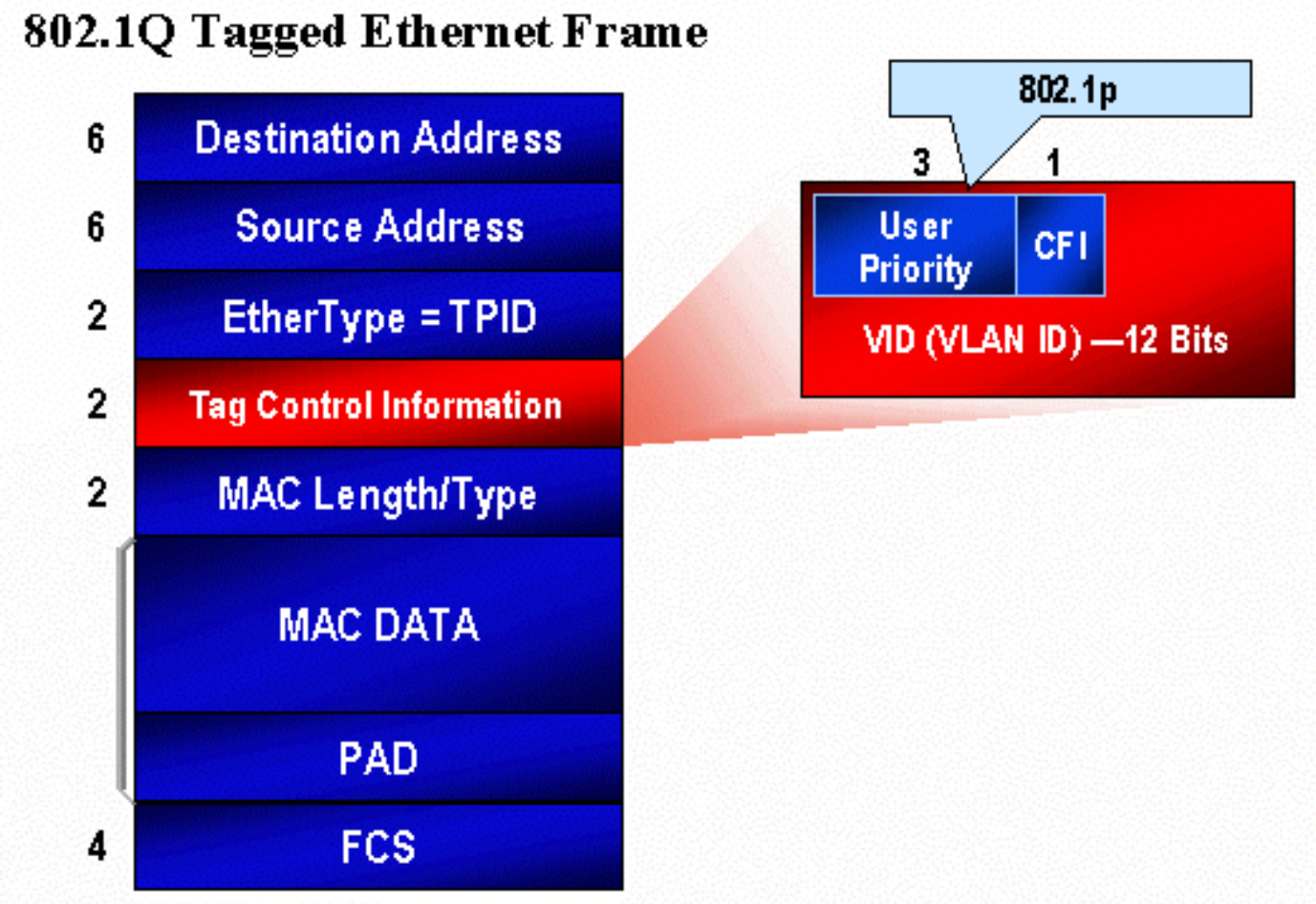
In jüngerer Zeit wurde die Verwendung des ToS-Felds auf die sechs MSB erweitert, die als DSCP bezeichnet werden. DSCP ergibt 64 Prioritätswerte (zwei bis sechs), die dem IP-Paket zugewiesen werden können.

Die Catalyst 6000-Produktfamilie kann die ToS-Funktionen manipulieren. Dies kann sowohl über die PFC als auch über die MSFC erreicht werden. Wenn ein Frame in den Switch eingeht, wird ihm ein DSCP-Wert zugewiesen. Dieser DSCP-Wert wird intern im Switch verwendet, um vom Administrator definierte Servicelevel (QoS-Richtlinien) zuzuweisen. Das DSCP kann bereits in einem Frame vorhanden und verwendet werden, oder das DSCP kann von der vorhandenen CoS-, IP-Rangfolge oder DSCP im Frame abgeleitet werden (sollte der Port vertrauenswürdig sein). Eine Zuordnung wird im Switch intern verwendet, um das DSCP abzuleiten. Mit acht möglichen CoS/IP-Prioritätswerten und 64 möglichen DSCP-Werten ordnet die Standardzuordnung CoS/IPPrec 0 DSCP 0, CoS/IPPrec 1 zu DSCP 7, CoS/IPPrec 2 zu DSCP 15 usw. zu. Diese Standardzuordnungen können vom Administrator überschrieben werden. Wenn der Frame für einen ausgehenden Port geplant ist, kann die CoS neu geschrieben und der DSCP-Wert zum Ableiten der neuen CoS verwendet werden.

CoS

CoS bezieht sich auf drei Bit in einem ISL-Header oder einem 802.1Q-Header, die verwendet werden, um die Priorität des Ethernet-Frames anzugeben, während dieser durch ein Switch-Netzwerk geleitet wird. Für die Zwecke dieses Dokuments wird nur die Verwendung des 802.1Q-Headers verwendet. Die CoS-Bits im 802.1Q-Header werden allgemein als 802.1p-Bits bezeichnet. Es überrascht nicht, dass es drei CoS-Bits gibt, die der Anzahl der für die IP-Rangfolge verwendeten Bits entsprechen. In vielen Netzwerken kann ein Paket sowohl L2- als auch L3-Domänen durchlaufen, um die QoS durchgängig zu halten. Um QoS beizubehalten, können die ToS CoS zugeordnet und CoS ToS zugeordnet werden.

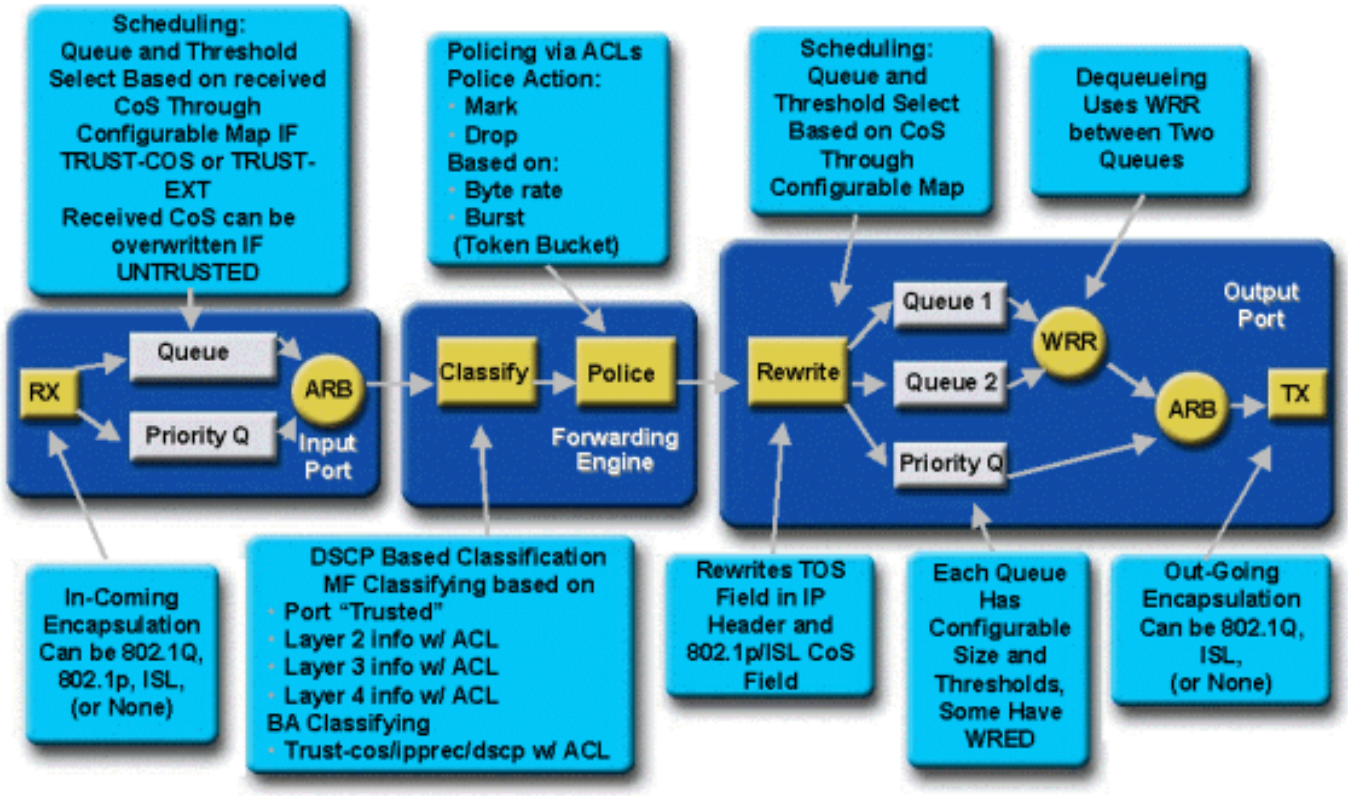
Das nachfolgende Diagramm ist ein Ethernet-Frame, der mit einem 802.1Q-Feld markiert ist und aus einem 2-Byte-Ethertype und einem 2-Byte-Tag besteht. Innerhalb des 2-Byte-Tags befinden sich die Prioritätsbits des Benutzers (bekannt als 802.1p).



QoS-Fluss in der Catalyst 6000-Familie

QoS in der Catalyst 6000-Familie ist die umfassendste Implementierung von QoS in allen aktuellen Cisco Catalyst-Switches. In den folgenden Abschnitten wird beschrieben, wie die verschiedenen QoS-Prozesse auf einen Frame angewendet werden, während dieser den Switch durchläuft.

In diesem Dokument wurde bereits darauf hingewiesen, dass viele L2- und L3-Switches eine Reihe von QoS-Elementen anbieten können. Diese Elemente sind Klassifizierung, Warteschlangenplanung für Eingabefelder, Richtlinienvergabe, Neuschreibung und Planung von Ausgabewarteschlangen. Der Unterschied zur Catalyst 6000-Familie besteht darin, dass diese QoS-Elemente von einer L2-Engine angewendet werden, die Einblicke in L3- und L4-Details sowie lediglich Informationen über L2-Header bietet. Im folgenden Diagramm wird zusammengefasst, wie die Catalyst 6000-Familie diese Elemente implementiert.



Ein Frame gelangt in den Switch und wird zunächst von dem Port-ASIC verarbeitet, der den Frame empfangen hat. Der Frame wird in eine Rx-Warteschlange gestellt. Je nach Line Card der Catalyst 6000-Familie gibt es ein oder zwei Rx-Warteschlangen.

Der Port-ASIC verwendet die CoS-Bits als Indikator für die Warteschlange, in der der Frame platziert werden soll (wenn mehrere Eingangswarteschlangen vorhanden sind). Wenn der Port als nicht vertrauenswürdig eingestuft wird, kann der Port-ASIC die vorhandenen CoS-Bits auf der Grundlage eines vordefinierten Werts überschreiben.

Der Frame wird dann an die L2/L3 Forwarding Engine (PFC) weitergeleitet, die den Frame klassifiziert und optional regelt (Ratenlimit). Bei der Klassifizierung wird dem Frame ein DSCP-Wert zugewiesen, der vom Switch intern zur Verarbeitung des Frames verwendet wird. Das DSCP wird aus einem der folgenden Komponenten abgeleitet:

1. Ein vorhandener DSCP-Wert wird vor der Eingabe des Frames in den Switch festgelegt.
2. Die empfangenen IP-Prioritätsbits sind bereits im IPV4-Header festgelegt. Da es 64 DSCP-Werte und nur acht IP-Rangfolgewerte gibt, konfiguriert der Administrator eine vom Switch verwendete Zuordnung, um das DSCP abzuleiten. Wenn der Administrator die Karten nicht konfiguriert, sind Standardzuordnungen vorhanden.
3. Die empfangenen CoS-Bits wurden bereits vor der Eingabe des Frames in den Switch festgelegt. Ähnlich wie die IP-Rangfolge gibt es maximal acht CoS-Werte, die jeweils einem von 64 DSCP-Werten zugeordnet werden müssen. Diese Zuordnung kann konfiguriert werden, oder der Switch kann die Standardzuordnung verwenden.
4. Legen Sie für den Frame einen DSCP-Standardwert fest, der normalerweise über einen ACL-Eintrag (Access Control List) zugewiesen wird.

Nachdem dem Frame ein DSCP-Wert zugewiesen wurde, wird die Richtlinie (Ratenbegrenzung) angewendet, falls eine Richtlinienkonfiguration vorhanden ist. Die Richtlinienvergabe beschränkt den Datenfluss durch die PFC, indem Datenverkehr, der nicht im Profil enthalten ist, verworfen oder markiert wird. Der Begriff "Out-of-Profile" (Out-of-Profile) wird verwendet, um anzugeben,

dass der Datenverkehr eine vom Administrator definierte Grenze überschritten hat, die die von der PFC gesendete Bitmenge pro Sekunde entspricht. Out-of-Profile-Datenverkehr kann verworfen oder der CoS-Wert kann deaktiviert werden. PFC1 und PFC2 unterstützen derzeit nur die Eingabe-Policing (Ratenbegrenzung). Mit der Einführung einer neuen PFC wird Unterstützung für Eingabe- und Ausgaberichtlinien angeboten.

Die PFC leitet den Frame zur Verarbeitung an den Ausgangsport weiter. An diesem Punkt wird ein Umschreibprozess aufgerufen, um die CoS-Werte im Frame und den ToS-Wert im IPV4-Header zu ändern. Dies wird vom internen DSCP abgeleitet. Der Frame wird dann auf Basis seines CoS-Werts in eine Übertragungswarteschlange gestellt, die für die Übertragung bereit ist. Während sich der Frame in der Warteschlange befindet, überwacht der Port-ASIC die Puffer und implementiert WRED, um ein Überlaufen der Puffer zu verhindern. Anschließend wird ein WRR-Planungsalgorithmus zum Planen und Übertragen von Frames vom Ausgangsport verwendet.

In jedem der folgenden Abschnitte wird dieser Ablauf genauer beschrieben. Es werden Konfigurationsbeispiele für die oben beschriebenen Schritte bereitgestellt.

Warteschlangen, Puffer, Schwellenwerte und Zuordnungen

Bevor die QoS-Konfiguration detailliert beschrieben wird, müssen bestimmte Begriffe genauer erläutert werden, um sicherzustellen, dass Sie die QoS-Konfigurationsfunktionen des Switches vollständig verstehen.

Warteschlangen

Jeder Port des Switches verfügt über eine Reihe von Eingangs- und Ausgangswarteschlangen, die als temporäre Speicherbereiche für Daten verwendet werden. Die Line Cards der Catalyst 6000-Familie implementieren für jeden Port eine unterschiedliche Anzahl von Warteschlangen. Die Warteschlangen werden normalerweise in Hardware-ASICs für jeden Port implementiert. Bei den Line Cards der Catalyst 6000-Familie der ersten Generation wurden normalerweise eine Eingangs- und zwei Ausgabewarteschlangen konfiguriert. Auf neueren Linecards (10/100 und GE) implementiert der ASIC eine zusätzliche Gruppe von zwei Warteschlangen (ein Eingang und ein Ausgang), die zwei Eingangs- und drei Ausgabewarteschlangen ergeben. Diese beiden zusätzlichen Warteschlangen sind spezielle SP-Warteschlangen, die für latenzempfindlichen Datenverkehr wie VoIP verwendet werden. Sie werden auf SP-Art gewartet. Wenn also ein Frame in der SP-Warteschlange eintrifft, wird das Planen von Frames aus den unteren Warteschlangen beendet, um den Frame in der SP-Warteschlange zu verarbeiten. Nur wenn die SP-Warteschlange leer ist, wird die Planung von Paketen aus der (den) unteren Warteschlange(n) wieder aufgenommen.

Wenn ein Frame zu Zeiten der Überlastung an einem Port (für Eingabe oder Ausgabe) ankommt, wird er in eine Warteschlange gestellt. Die Entscheidung, hinter der Warteschlange der Frame platziert wird, wird normalerweise anhand des CoS-Werts im Ethernet-Header des eingehenden Frames getroffen.

Beim Ausgang wird ein Scheduling-Algorithmus verwendet, um die TX-Warteschlange (Ausgabe) zu leeren. WRR ist die Technik, um dies zu erreichen. Für jede Warteschlange wird eine Gewichtung verwendet, um festzulegen, wie viele Daten aus der Warteschlange entfernt werden, bevor sie in die nächste Warteschlange verschoben werden. Die vom Administrator zugewiesene Gewichtung liegt zwischen 1 und 255, die jeder TX-Warteschlange zugewiesen wird.

Puffer

Jeder Warteschlange wird eine bestimmte Menge an Pufferspeicher zugewiesen, um Transit-Daten zu speichern. Auf dem Port-ASIC befindet sich der Speicher, der aufgeteilt und pro Port zugewiesen wird. Für jeden GE-Port weist der GE ASIC 512 K Pufferkapazität zu. Für 10/100-Ports reserviert der Port-ASIC eine Pufferung von 64.000 oder 128.000 Ports (je nach Linecard) pro Port. Dieser Pufferspeicher wird dann zwischen der Rx-Warteschlange (Eingang) und der TX-Warteschlange (Ausgang) aufgeteilt.

Schwellenwerte

Ein Aspekt der normalen Datenübertragung besteht darin, dass bei einem Paketverlust das Paket erneut übertragen wird (TCP-Flows). In Zeiten von Überlastungen kann dies die Netzwerkbelastung erhöhen und möglicherweise dazu führen, dass Puffer noch mehr überlastet werden. Um sicherzustellen, dass Puffer nicht überlaufen, setzt der Catalyst Switch der Serie 6000 eine Reihe von Techniken ein, um dies zu vermeiden.

Schwellenwerte sind imaginäre Werte, die vom Switch (oder vom Administrator) zugewiesen werden und die Nutzungspunkte definieren, an denen der Überlastungsmanagementalgorithmus beginnt, Daten aus der Warteschlange zu verwerfen. Auf den Ports der Catalyst 6000-Produktfamilie gibt es in der Regel vier Schwellenwerte, die mit Eingangswarteschlangen verknüpft sind. Ausgabewarteschlangen sind in der Regel zwei Schwellenwerte zugeordnet.

Diese Schwellenwerte werden auch im Kontext von QoS bereitgestellt, um diesen Schwellenwerten Frames mit unterschiedlichen Prioritäten zuzuweisen. Wenn sich der Puffer füllt und Schwellenwerte überschritten werden, kann der Administrator den verschiedenen Schwellenwerten unterschiedliche Prioritäten zuordnen und dem Switch mitteilen, welche Frames bei Überschreitung eines Schwellenwerts verworfen werden sollen.

Zuordnungen

In den Warteschlangen- und Schwellenabschnitten oben wurde erwähnt, dass der CoS-Wert im Ethernet-Frame verwendet wird, um zu bestimmen, in welche Warteschlange der Frame platziert werden soll und an welchem Punkt der Pufferbelegung ein Frame fallen gelassen werden kann. Dies ist der Zweck von Zuordnungen.

Wenn QoS auf der Catalyst 6000-Familie konfiguriert ist, werden Standardzuordnungen aktiviert, die Folgendes definieren:

- bei welchen Schwellenwerten Frames mit bestimmten CoS-Werten verworfen werden dürfen
- in welche Warteschlange ein Frame platziert wird (basierend auf seinem CoS-Wert)

Obwohl die Standardzuordnungen vorhanden sind, können diese Standardzuordnungen vom Administrator überschrieben werden. Zuordnung ist für Folgendes vorhanden:

- CoS-Werte eines eingehenden Frames zu einem DSCP-Wert
- IP-Rangfolgewerte eines eingehenden Frames zu einem DSCP-Wert
- DSCP-Werte zu einem CoS-Wert für einen ausgehenden Frame
- CoS-Werte zu Drop-Schwellenwerten für Empfangswarteschlangen
- CoS-Werte zu Drop-Schwellenwerten für Übertragungswarteschlangen
- DSCP-Markdown-Werte für Frames, die Richtlinienanweisungen überschreiten
- CoS-Werte zu einem Frame mit einer bestimmten MAC-Zieladresse

WRED und WRR

WRED und WRR sind zwei extrem leistungsfähige Algorithmen, die in der Catalyst 6000-Familie eingesetzt werden. Sowohl WRED als auch WRR verwenden das Priority Tag (CoS) innerhalb eines Ethernet-Frames, um eine verbesserte Puffer-Verwaltung und die Planung ausgehender Anrufe zu ermöglichen. B

WURDE

WRED ist ein von der Catalyst 6000-Produktfamilie verwendeter Puffermanagementalgorithmus, mit dem die Auswirkungen von Verkehrsstaus mit hoher Priorität in Zeiten von Überlastungen auf ein Minimum reduziert werden sollen. WRED basiert auf dem ROT-Algorithmus.

Um ROT und WRED besser zu verstehen, sollten Sie das Konzept des TCP-Flussmanagements erneut durchgehen. Flow Management stellt sicher, dass der TCP-Sender das Netzwerk nicht überlastet. Der TCP-Langstart-Algorithmus ist Teil der Lösung, um diesem Problem zu begegnen. Es schreibt vor, dass beim Start eines Datenflusses ein einzelnes Paket gesendet wird, bevor es auf eine Bestätigung wartet. Zwei Pakete werden dann gesendet, bevor ein ACK empfangen wird, wodurch sich die Anzahl der Pakete, die gesendet werden, schrittweise erhöht, bevor jedes ACK empfangen wird. Dies wird so lange fortgesetzt, bis der Datenfluss eine Übertragungsebene erreicht (d. h. eine *x* Anzahl von Paketen), die das Netzwerk ohne die Belastung bewältigen kann, die eine Überlastung verursacht. Wenn eine Überlastung auftritt, drosselt der Langsamstart-Algorithmus die Fenstergröße (d. h. die Anzahl der Pakete, die vor dem Warten auf eine Bestätigung versendet wurden) zurück und reduziert so die Gesamtleistung für diese TCP-Sitzung (Flow).

ROT überwacht beim Auffüllen eine Warteschlange. Wenn ein bestimmter Grenzwert überschritten wurde, werden Pakete nach dem Zufallsprinzip verworfen. Bestimmte Ströme werden nicht berücksichtigt. Stattdessen werden zufällige Pakete verworfen. Diese Pakete können aus Datenflüssen mit hoher oder niedriger Priorität stammen. Verworfene Pakete können Teil eines einzigen Datenflusses oder mehrerer TCP-Flüsse sein. Wenn mehrere Datenflüsse betroffen sind (wie oben beschrieben), kann dies erhebliche Auswirkungen auf die Fenstergröße der Datenflüsse haben.

Im Gegensatz zu ROT ist WRED beim Verwerfen von Frames nicht so zufällig. WRED berücksichtigt die Priorität der Frames (im Fall der Catalyst 6000-Familie verwendet es den CoS-Wert). Mit WRED weist der Administrator Frames mit bestimmten CoS-Werten bestimmten Schwellenwerten zu. Wenn diese Schwellenwerte überschritten werden, können Frames mit CoS-Werten, die diesen Schwellenwerten zugeordnet sind, verworfen werden. Andere Frames mit CoS-Werten, die den höheren Schwellenwerten zugewiesen sind, werden in der Warteschlange beibehalten. Dieser Prozess ermöglicht es, Datenflüsse mit höherer Priorität intakt zu halten, wodurch die größeren Fenster intakt bleiben und die Latenz beim Abruf der Pakete vom Sender zum Empfänger minimiert wird.

Woher wissen Sie, ob Ihre Linecard WRED unterstützt? Geben Sie den folgenden Befehl ein. Überprüfen Sie in der Ausgabe den Abschnitt, der die Unterstützung für WRED an diesem Port angibt.

```
Console> show qos info config 2/1
QoS setting in NVRAM:
QoS is enabled
```

```
Port 2/1 has 2 transmit queue with 2 drop thresholds (2q2t).
Port 2/1 has 1 receive queue with 4 drop thresholds (1q4t).
Interface type:vlan-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping:
Queue Threshold CoS
----- --------- ---------------
1     1         0 1
1     2         2 3
2     1         4 5
2     2         6 7
Rx drop thresholds:
Rx drop thresholds are disabled for untrusted ports.
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------
1        50% 60% 80% 100%
TX drop thresholds:
Queue #  Thresholds - percentage (abs values)
-------  ---------------------------------
1        40% 100%
2        40% 100%
TX WRED thresholds:
WRED feature is not supported for this port_type.
!-- Look for this. Queue Sizes: Queue # Sizes - percentage (abs values) ------- ----------------
-------------------- 1 80% 2 20% WRR Configuration of ports with speed 1000MBPS: Queue # Ratios
(abs values) ------- ----------------------------------- 1 100 2 255 Console> (enable)
```

Falls WRED auf einem Port nicht verfügbar ist, verwendet der Port eine Tail-Drop-Methode zur Puffer-Verwaltung. Tail Drop verwirft, wie der Name schon andeutet, einfach eingehende Frames, sobald die Puffer voll ausgelastet sind.

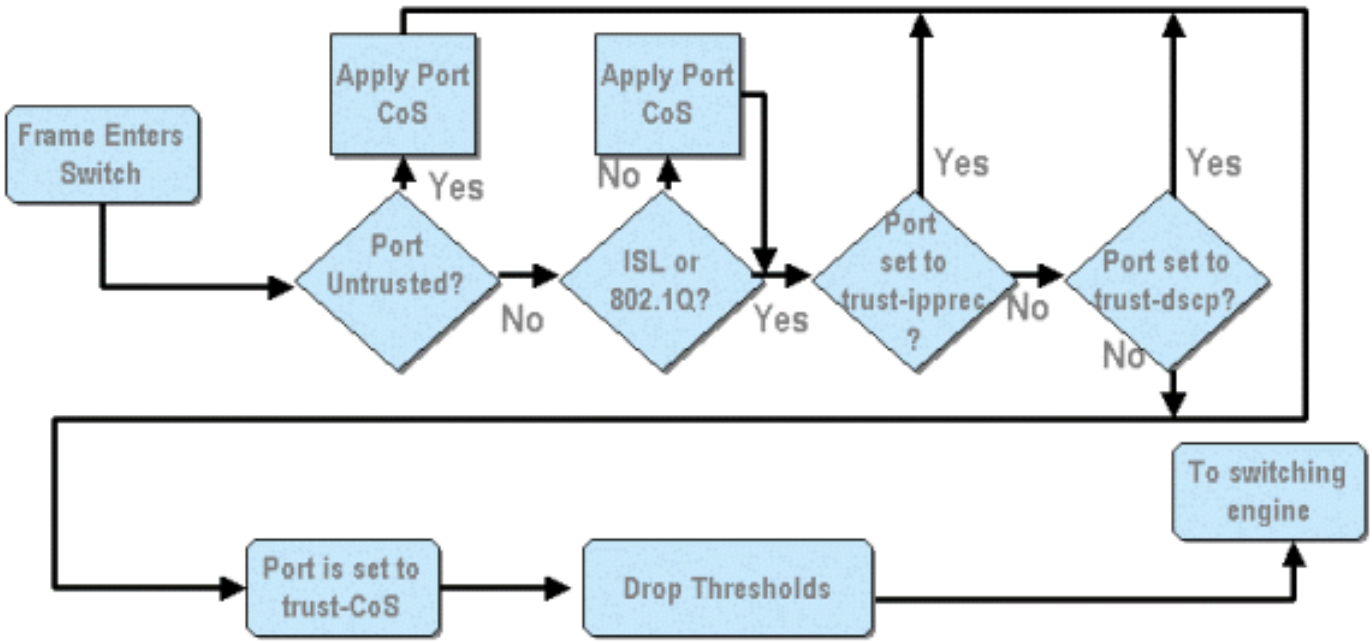
WRR

WRR wird zum Planen des ausgehenden Datenverkehrs aus TX-Warteschlangen verwendet. Ein normaler Round-Robin-Algorithmus wechselt zwischen TX-Warteschlangen, die dieselbe Anzahl von Paketen aus jeder Warteschlange senden, bevor sie zur nächsten Warteschlange wechselt. Der gewichtete Aspekt von WRR ermöglicht es dem Planungsalgorithmus, eine Gewichtung zu überprüfen, die der Warteschlange zugewiesen wurde. Dies ermöglicht definierten Warteschlangen den Zugriff auf mehr Bandbreite. Der WRR-Scheduling-Algorithmus löscht mehr Daten aus identifizierten Warteschlangen als andere Warteschlangen und stellt somit eine Voreinstellung für designierte Warteschlangen bereit.

Die Konfiguration für WRR und die anderen oben beschriebenen Aspekte werden in den folgenden Abschnitten erläutert.

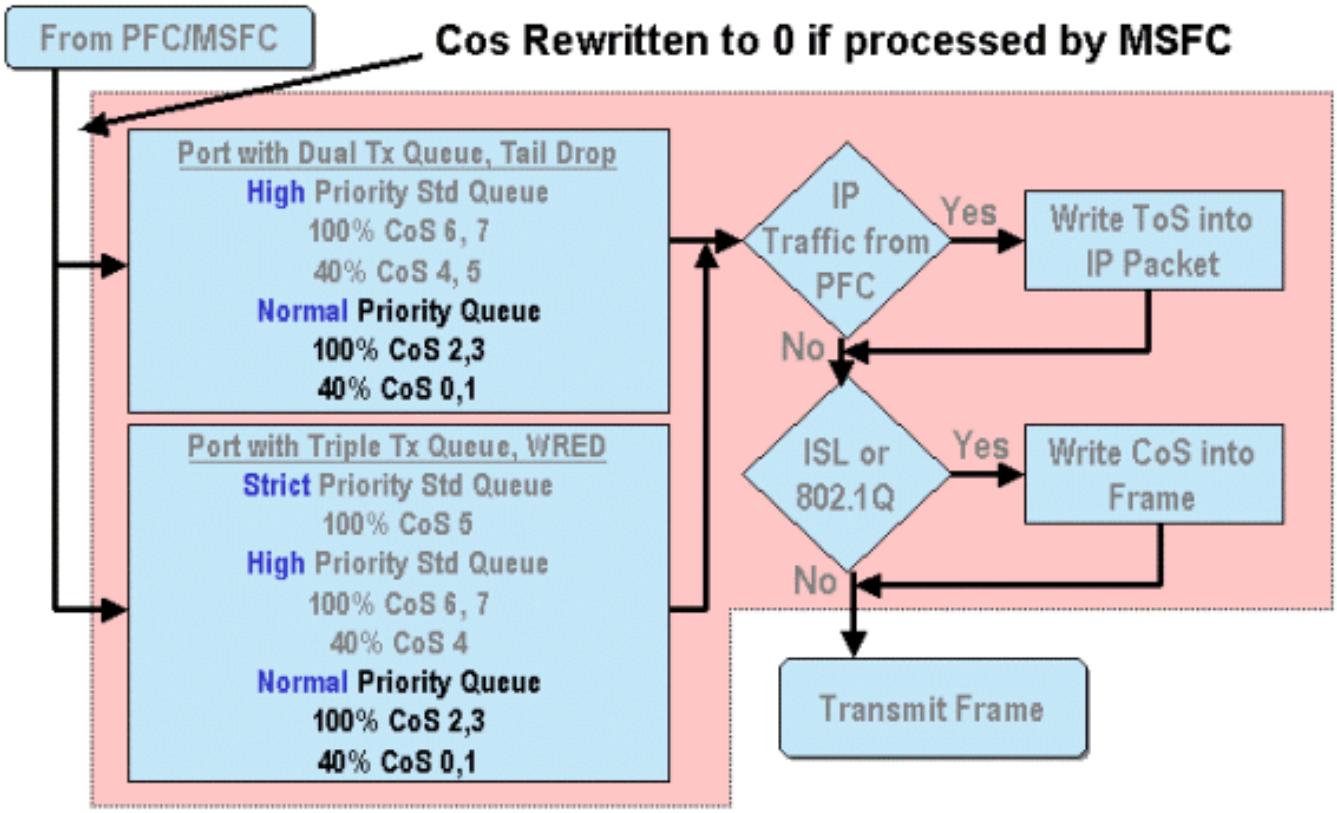
Konfigurieren von Port ASIC-basierter QoS auf der Catalyst 6000-Produktfamilie

Die QoS-Konfiguration weist entweder den Port-ASIC oder den PFC an, eine QoS-Aktion auszuführen. In den folgenden Abschnitten wird die QoS-Konfiguration für beide Prozesse behandelt. Auf dem Port-ASIC wirkt sich die QoS-Konfiguration auf den ein- und ausgehenden Datenverkehr aus.



Aus dem obigen Diagramm kann ersichtlich werden, dass die folgenden QoS-Konfigurationsprozesse zutreffen:

1. Vertrauensstatus der Ports
2. Anwendung portbasierter CoS
3. Rx Drop Schwellenwert-Zuweisung
4 Zuordnung von CoS zu Rx-Drop-Schwellenwerten



Wenn ein Frame entweder von der MSFC oder von der PFC verarbeitet wird, wird er zur weiteren Verarbeitung an den ausgehenden Port-ASIC übergeben. Bei allen von der MSFC verarbeiteten Frames werden die CoS-Werte auf Null zurückgesetzt. Dies muss bei der QoS-Verarbeitung an

ausgehenden Ports berücksichtigt werden.

Das obige Diagramm zeigt die QoS-Verarbeitung, die vom Port-ASIC für ausgehenden Datenverkehr durchgeführt wird. Bei der ausgehenden QoS-Verarbeitung werden u. a. folgende Prozesse aufgerufen:

1. TX Tail Drop und WRED-Schwellenwertzuweisungen
2. CoS to TX Tail Drop und WRED-Karten

Außerdem wird im obigen Diagramm nicht dargestellt, wie die CoS mithilfe einer DSCP-CoS-Zuordnung dem ausgehenden Frame zugewiesen wird.

In den folgenden Abschnitten werden die QoS-Konfigurationsfunktionen der Port-basierten ASICs genauer untersucht.

Hinweis: Ein wichtiger Punkt ist, dass QoS-Befehle, die mit CatOS aufgerufen werden, in der Regel für alle Ports mit dem angegebenen Warteschlangentyp gelten. Wenn beispielsweise ein WRED-Drop-Schwellenwert auf Ports mit dem Warteschlangentyp 1p2q2t angewendet wird, wird dieser WRED-Drop-Schwellenwert auf alle Ports auf allen Linecards angewendet, die diesen Warteschlangentyp unterstützen. Bei Cat IOS werden QoS-Befehle in der Regel auf Schnittstellenebene angewendet.

Aktivieren von QoS

Bevor eine QoS-Konfiguration für die Catalyst 6000-Familie vorgenommen werden kann, muss QoS auf dem Switch aktiviert werden. Hierzu wird der folgende Befehl ausgegeben:

CatOS

```
Console> (enable) set qos enable
!-- QoS is enabled. Console> (enable)
```

Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config)# mls qos
```

Wenn QoS in der Catalyst 6000-Familie aktiviert ist, legt der Switch eine Reihe von QoS-Standardwerten für den Switch fest. Diese Standardeinstellungen sind wie folgt:

QoS Feature	Default setting
Trust state of each port	Un-trusted
Receive Queue drop threshold percentages	Threshold 1 – 50% Threshold 2 – 60% Threshold 3 – 80% Threshold 4 – 100%
Transmit Queue drop threshold percentages	Low priority queue threshold 1 – 80% Low priority queue threshold 2 – 100% High priority queue threshold 1 – 80% High priority queue threshold 2 – 100%
CoS value to Drop threshold mapping	Receive queue 1/drop threshold 1: CoS 0 and 1 Transmit queue 1/drop threshold 1: CoS 0 and 1 Receive queue 1/drop threshold 2: CoS 2 and 3 Transmit queue 1/drop threshold 2: CoS 2 and 3 Receive queue 1/drop threshold 3: CoS 4 and 5 Transmit queue 2/drop threshold 1: CoS 4 and 5 Receive queue 1/drop threshold 4: CoS 6 and 7
	Transmit queue 2/drop threshold 2: CoS 6 and 7
CoS to DSCP Mapping (DSCP set from CoS value)	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
IP Precedence to DSCP Map (DSCP set from IP Precedence value)	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
DSCP to CoS map (CoS set from DSCP values)	DSCP 0-7 = CoS 0 DSCP 8-15 = CoS 1 DSCP 16-23 = CoS 2 DSCP 24-31 = CoS 3 DSCP 32-39 = CoS 4 DSCP 40-47 = CoS 5 DSCP 48-55 = CoS 6 DSCP 56-63 = CoS 7

Vertrauenswürdige und nicht vertrauenswürdige Ports

Jeder Port der Catalyst 6000-Familie kann als vertrauenswürdig oder UN-vertrauenswürdig konfiguriert werden. Der Vertrauensstatus des Ports legt fest, wie er den Frame während der Übertragung über den Switch kennzeichnet, klassifiziert und plant. Standardmäßig befinden sich alle Ports im nicht vertrauenswürdigen Zustand.

Nicht vertrauenswürdige Ports (Standardeinstellung für Ports)

Wenn der Port als nicht vertrauenswürdiger Port konfiguriert wird, werden die CoS- und ToS-Werte für einen Frame beim erstmaligen Eingeben des Ports vom Port-ASIC auf Null zurückgesetzt. Das bedeutet, dass der Frame den Service mit der niedrigsten Priorität auf seinem Pfad über den Switch erhält.

Alternativ kann der Administrator den CoS-Wert jedes Ethernet-Frames zurücksetzen, der einen nicht vertrauenswürdigen Port auf einen vorher festgelegten Wert setzt. Die Konfiguration wird in einem späteren Abschnitt erläutert.

Wenn Sie den Port als nicht vertrauenswürdig festlegen, wird der Switch angewiesen, keine Überlastungsvermeidung auszuführen. Die Überlastungsvermeidung ist die Methode zum Verwerfen von Frames anhand ihrer CoS-Werte, sobald diese die für diese Warteschlange definierten Schwellenwerte überschreiten. Alle Frames, die diesen Port betreten, können ebenfalls verworfen werden, sobald die Puffer 100 % erreichen.

In CatOS kann ein 10/100- oder GE-Port durch folgenden Befehl als nicht vertrauenswürdig konfiguriert werden:

CatOS

```
Console> (enable) set port qos 3/16 trust untrusted
!-- Port 3/16 qos set to untrusted. Console> (enable)
```

Mit diesem Befehl wird Port 16 auf Modul 3 in den Zustand nicht vertrauenswürdig eingestellt.

Hinweis: Für den integrierten Cisco IOS-Modus (Native Mode) unterstützt die Software derzeit nur die Einstellung von Vertrauenswürdigkeit für GE-Ports.

Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config)# interface gigabitethernet 1/1
Cat6500(config-if)# no mls qos trust
```

Im obigen Beispiel geben wir die Schnittstellenkonfiguration ein und wenden die **no**-Form des Befehls an, um den Port als nicht vertrauenswürdig festzulegen, da es sich um IOS handelt.

Vertrauenswürdige Ports

In manchen Fällen werden Ethernet-Frames, die in einen Switch eingegeben werden, entweder über eine CoS- oder eine ToS-Einstellung verfügen, die der Administrator beim Durchlaufen des Frames durch den Switch beibehalten möchte. Für diesen Datenverkehr kann der Administrator den Vertrauensstatus eines Ports festlegen, bei dem dieser Datenverkehr zum Switch gelangt.

Wie bereits erwähnt, verwendet der Switch intern einen DSCP-Wert, um diesem Frame eine vordefinierte Servicestufe zuzuweisen. Wenn ein Frame in einen vertrauenswürdigen Port eingeht, kann der Administrator den Port so konfigurieren, dass er entweder den vorhandenen CoS-, IP-Rangfolge- oder DSCP-Wert überprüft, um den internen DSCP-Wert festzulegen. Alternativ kann der Administrator für jedes Paket, das den Port betritt, ein vordefiniertes DSCP festlegen.

Das Festlegen des Vertrauensstatus eines Ports auf vertrauenswürdig kann mithilfe des folgenden Befehls erreicht werden:

CatOS

```
Console> (enable) set port qos 3/16 trust trust-cos
!-- Port 3/16 qos set to trust-COs Console> (enable)
```

Dieser Befehl gilt für die Linecard WS-X6548-RJ45 und legt den Vertrauensstatus von Port 3/16 auf "Trusted" fest. Der Switch verwendet den im eingehenden Frame festgelegten CoS-Wert, um das interne DSCP festzulegen. Das DSCP wird entweder von einer Standardzuordnung abgeleitet, die bei Aktivierung von QoS auf dem Switch erstellt wurde, oder von einer vom Administrator definierten Zuordnung. Anstelle des trust-COs-Schlüsselworts kann der Administrator auch die Schlüsselwörter trust-dscp oder trust-ipprec verwenden.

Bei früheren 10/100-Linecards (WS-X6348-RJ45 und WS-X6248-RJ45) muss die Port-Vertrauenswürdigkeit durch Ausgabe des Befehls **set qos acl** festgelegt werden. In diesem Befehl kann ein Vertrauenszustand durch einen Unterparameter des Befehls **set qos acl** zugewiesen werden. Das Festlegen von trust CoS auf Ports dieser Linecards wird nicht unterstützt (siehe unten).

```
Console> (enable) set port qos 4/1 trust trust-COs
Trust type trust-COs not supported on this port.
!-- Trust-COs not supported, use acl instead. Rx thresholds are enabled on port 4/1. !-- Need to turn on input queue scheduling. Port 4/1 qos set to untrusted. !-- Trust-COs not supported, so port is set to untrusted.
```

Der obige Befehl gibt an, dass die Planung von Eingabewarteschlangen aktiviert werden muss. Daher muss für 10/100-Ports auf den Linecards WS-X6248-RJ45 und WS-X6348-RJ45 der Befehl **set port qos x/y trust-COs** konfiguriert werden. Um Vertrauenswürdigkeit festzulegen, muss die ACL verwendet werden.

Mit dem integrierten Cisco IOS (Nativer Modus) kann die Einstellung der Vertrauenswürdigkeit auf einer GE-Schnittstelle und 10/100-Ports auf der neuen WS-X6548-RJ45-Linecard vorgenommen werden.

Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config)# interface gigabitethernet 5/4
Cat6500(config-if)# mls qos trust ip-precedence
Cat6500(config-if)#
```

In diesem Beispiel wird der Vertrauensstatus von GE-Port 5/4 als vertrauenswürdig festgelegt. Der IP-Rangfolgewert des Frames wird zum Ableiten des DSCP-Werts verwendet.

Eingangsklassifizierung und Festlegen Port-basierter CoS

Beim Eingang an einen Switch-Port kann die CoS eines Ethernet-Frames geändert werden, wenn eines der folgenden beiden Kriterien erfüllt ist:

1. Port als nicht vertrauenswürdig konfiguriert ist oder
2. der Ethernet-Frame hat keinen vorhandenen CoS-Wert bereits festgelegt.

Wenn Sie die CoS eines eingehenden Ethernet-Frames neu konfigurieren möchten, müssen Sie den folgenden Befehl ausführen:

CatOS

```
Console> (enable) set port qos 3/16 cos 3
!-- Port 3/16 qos set to 3. Console> (enable)
```

Mit diesem Befehl werden die COs eingehender Ethernet-Frames auf Port 16 auf Modul 3 auf den Wert 3 festgelegt, wenn ein nicht markierter Frame eintrifft oder wenn der Port auf nicht vertrauenswürdig eingestellt ist.

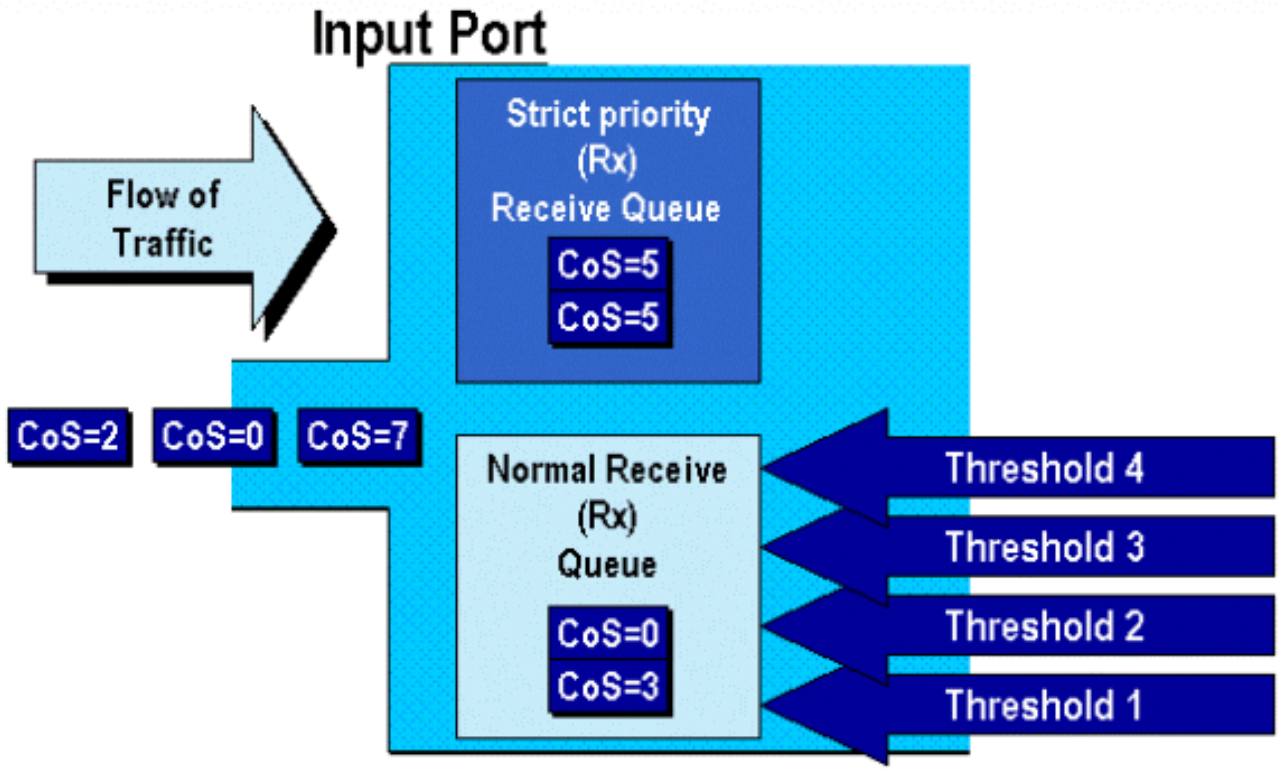
Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config)# interface fastethernet 5/13
Cat6500(config-if)# mls qos COs 4
Cat6500(config-if)#
```

Mit diesem Befehl werden die COs eingehender Ethernet-Frames auf Port 13 des Moduls 5 auf den Wert 4 festgelegt, wenn ein nicht markierter Frame eintrifft oder der Port auf nicht vertrauenswürdig eingestellt ist.

Rx-Drop-Grenzwerte konfigurieren

Beim Eingang am Switch-Port wird der Frame in eine Rx-Warteschlange gestellt. Um Pufferüberläufe zu vermeiden, implementiert der Port-ASIC vier Schwellenwerte für jede Rx-Warteschlange und verwendet diese Schwellenwerte, um Frames zu identifizieren, die nach Überschreiten dieser Schwellenwerte verworfen werden können. Der Port-ASIC verwendet den Wert der über Frames gesetzten COs, um zu ermitteln, welche Frames bei Überschreitung eines Schwellenwerts verworfen werden können. Diese Funktion ermöglicht es Frames mit höherer Priorität, im Puffer für längere Zeit zu bleiben, wenn eine Überlastung auftritt.



Wie im obigen Diagramm gezeigt, werden Frames in die Warteschlange gestellt. Wenn die Warteschlange zu füllen beginnt, werden die Schwellenwerte vom Port-ASIC überwacht. Bei Überschreitung eines Schwellenwerts werden Frames mit vom Administrator identifizierten CO-Werten willkürlich aus der Warteschlange entfernt. Die Standard-Schwellenwertzuordnungen für eine 1q4t-Warteschlange (gefunden auf den Linecards WS-X6248-RJ45 und WS-X6348-RJ45) sind wie folgt:

- Schwellenwert 1 ist auf 50 % festgelegt, und die CO-Werte 0 und 1 werden diesem Schwellenwert zugeordnet.
- Schwellenwert 2 ist auf 60 % festgelegt, und die CO-Werte 2 und 3 werden diesem Schwellenwert zugeordnet.
- Schwellenwert 3 ist auf 80 % festgelegt, und die CO-Werte 4 und 5 werden diesem Schwellenwert zugeordnet.
- Schwellenwert 4 ist auf 100 % festgelegt, und die CO-Werte 6 und 7 werden diesem Schwellenwert zugeordnet.

Für eine 1P1q4t-Warteschlange (die an GE-Ports zu finden ist) sind die Standardzuordnungen wie folgt:

- Schwellenwert 1 ist auf 50 % festgelegt, und die CO-Werte 0 und 1 werden diesem Schwellenwert zugeordnet.
- Schwellenwert 2 ist auf 60 % festgelegt, und die CO-Werte 2 und 3 werden diesem Schwellenwert zugeordnet.
- Schwellenwert 3 ist auf 80 % festgelegt, und die CO-Werte 4 werden diesem Grenzwert zugeordnet.
- Schwellenwert 4 ist auf 100 % festgelegt, und die CO-Werte 6 und 7 werden diesem Schwellenwert zugeordnet.
- COs-Wert von 5 wird der Warteschlange mit höchster Priorität zugeordnet

Für einen 1p1q0t (gefunden auf 10/100-Ports der WS-X6548-RJ45-Linecard) sind die

Standardzuordnungen wie folgt:

- Frames mit COs 5 werden in die SP-Rx-Warteschlange (Warteschlange 2) gestellt, in der der Switch eingehende Frames nur dann verwirft, wenn der SP-Empfangs-Warteschlangen-Puffer zu 100 Prozent voll ist.
- Frames mit den COs 0, 1, 2, 3, 4, 6 oder 7 werden in die Standard-Rx-Warteschlange gestellt. Der Switch verwirft eingehende Frames, wenn der Puffer der Rx-Queue zu 100 Prozent voll ist.

Diese Drop-Schwellenwerte können vom Administrator geändert werden. Außerdem können die CO-Standardwerte, die jedem Schwellenwert zugeordnet sind, geändert werden. Verschiedene Linecards implementieren unterschiedliche Rx Queue-Implementierungen. Nachfolgend finden Sie eine Zusammenfassung der Warteschlangentypen.

CatOS

```
Console> (enable) set qos drop-threshold 1q4t rx queue 1 20 40 75 100
!-- Rx drop thresholds for queue 1 set at 20%, 40%, 75%, and 100%. Console> (enable)
```

Mit diesem Befehl werden die Empfangs-Drop-Schwellenwerte für alle Eingangsports mit einer Warteschlange und vier Schwellenwerten (kennzeichnet 1q4t) auf 20 %, 40 %, 75 % und 100 % festgelegt.

Der Befehl im integrierten Cisco IOS-Modus (nativer Modus) wird unten angezeigt.

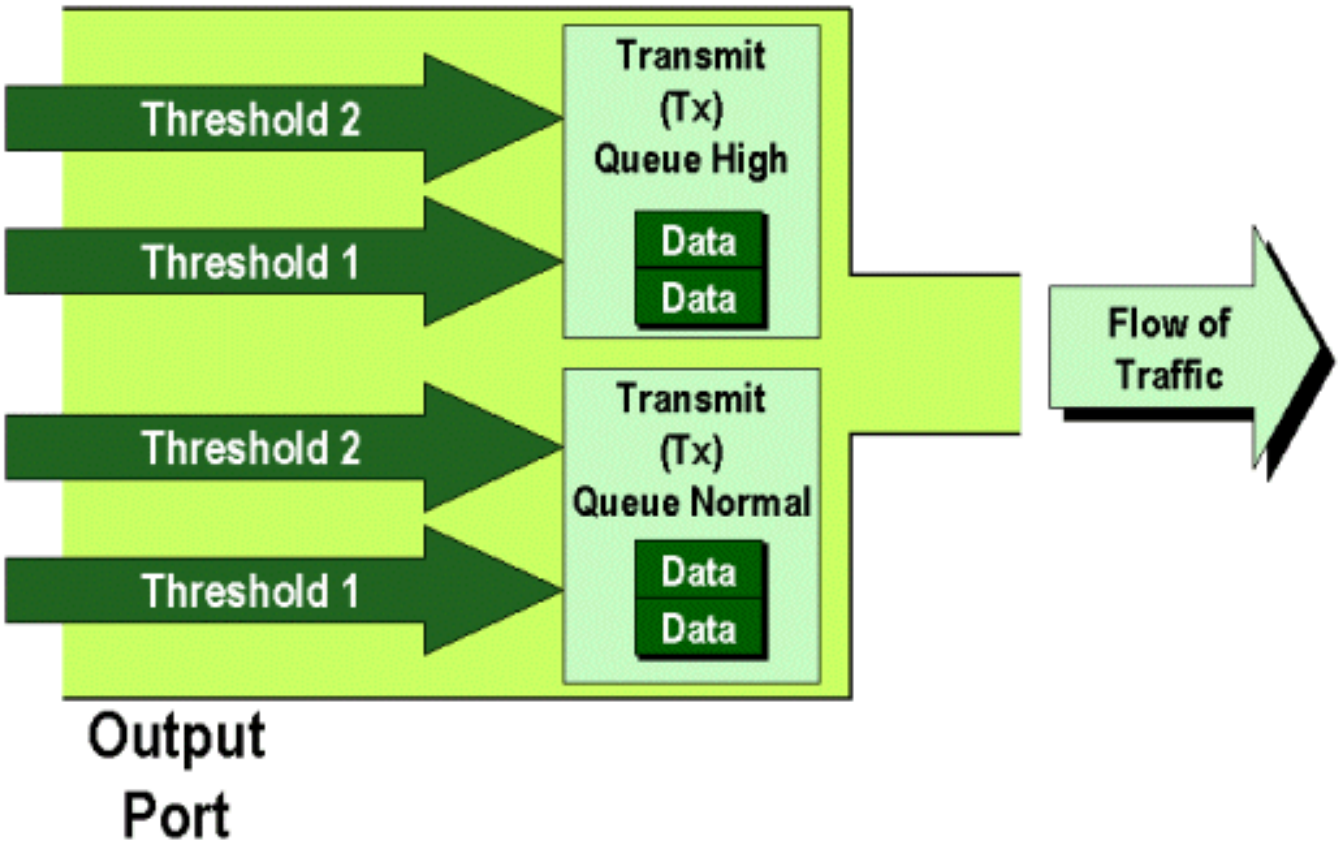
Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config-if)# wrr-queue threshold 1 40 50
Cat6500(config-if)# wrr-queue threshold 2 60 100

!-- Configures the 4 thresholds for a 1q4t rx queue and. Cat6500(config-if)# rcv-queue threshold
1 60 75 85 100

!-- Configures for a 1p1q4t rx queue, which applies to !-- the new WS-X6548-RJ45 10/100 line
card.
```

Rx-Drop-Schwellenwerte müssen vom Administrator aktiviert werden. Derzeit sollte der Befehl **set port qos x/y trust-COs** zum Aktivieren der Rx-Drop-Schwellenwerte verwendet werden (wobei *x* die Modulnummer und *y* der Port dieses Moduls ist).

Konfigurieren von TX-Drop-Schwellenwerten

An einem Ausgangsport verfügt der Port über zwei TX-Schwellenwerte, die als Teil des Überlastungsvermeidungsmechanismus verwendet werden: Warteschlange 1 und Warteschlange 2. Warteschlange 1 wird als Standard-Warteschlange mit niedriger Priorität und Warteschlange 2 als Standard-Warteschlange mit hoher Priorität bezeichnet. Abhängig von den verwendeten Linecards wird entweder ein Tail Drop oder ein WRED-Schwellenwert-Managementalgorithmus verwendet. Beide Algorithmen verwenden für jede TX-Warteschlange zwei Schwellenwerte.



Der Administrator kann diese Grenzwerte manuell wie folgt festlegen:

CatOS

```
Console> (enable) set qos drop-threshold 2q2t TX queue 1 40 100
!-- TX drop thresholds for queue 1 set at 40% and 100%. Console> (enable)
```

Mit diesem Befehl werden die TX-Drop-Schwellenwerte für die Warteschlange 1 für alle Ausgabeports mit zwei Warteschlangen und zwei Schwellenwerten (benennen 2q2t) auf 40 % und 100 % festgelegt.

```
Console> (enable) set qos wred 1p2q2t TX queue 1  60 100
!-- WRED thresholds for queue 1 set at 60% 100% on all WRED-capable 1p2q2t ports. Console>
(enable)
```

Mit diesem Befehl werden die WRED-Drop-Schwellenwerte für die Warteschlange 1 für alle Ausgabeports mit einer SP-Warteschlange, zwei normalen Warteschlangen und zwei Schwellenwerten (kennzeichnet 1p2q2t) auf 60 % und 100 % festgelegt. Warteschlange 1 ist als normale Warteschlange mit niedriger Priorität definiert und hat die niedrigste Priorität. Warteschlange 2 ist die normale Warteschlange mit hoher Priorität und hat eine höhere Priorität als Warteschlange 1. Warteschlange 3 ist die SP-Warteschlange und wird vor allen anderen Warteschlangen an diesem Port gewartet.

Der entsprechende Befehl, der im integrierten Cisco IOS-Modus (Native Mode) ausgegeben wird, ist unten dargestellt.

Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config-if)# wrr-queue random-detect max-threshold  1 40 100
Cat6500(config-if)#
```

Dadurch werden die WRED-Drop-Schwellenwerte für einen 1p2q2t-Port so festgelegt, dass die Warteschlange 1 bis 40 % für Schwellenwert 1 (TX) und 100 % für Grenzwert 2 (TX) beträgt.

WRED kann bei Bedarf auch in Integrated Cisco IOS (Nativer Modus) deaktiviert werden. Die dafür verwendete Methode ist die Verwendung der **n"**-Form des Befehls. Ein Beispiel für die Deaktivierung von WRED ist wie folgt:

Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config-if)# no wrr-queue random-detect queue_id
```

Zuordnen der MAC-Adresse zu COs-Werten

Neben der Festlegung von COs auf der Grundlage einer globalen Portdefinition kann der Administrator auch COs-Werte basierend auf der MAC-Zieladresse und der VLAN-ID festlegen. Dadurch können Frames, die für bestimmte Ziele bestimmt sind, mit einem vordefinierten CO-Wert gekennzeichnet werden. Diese Konfiguration kann mithilfe des folgenden Befehls erreicht werden:

CatOS

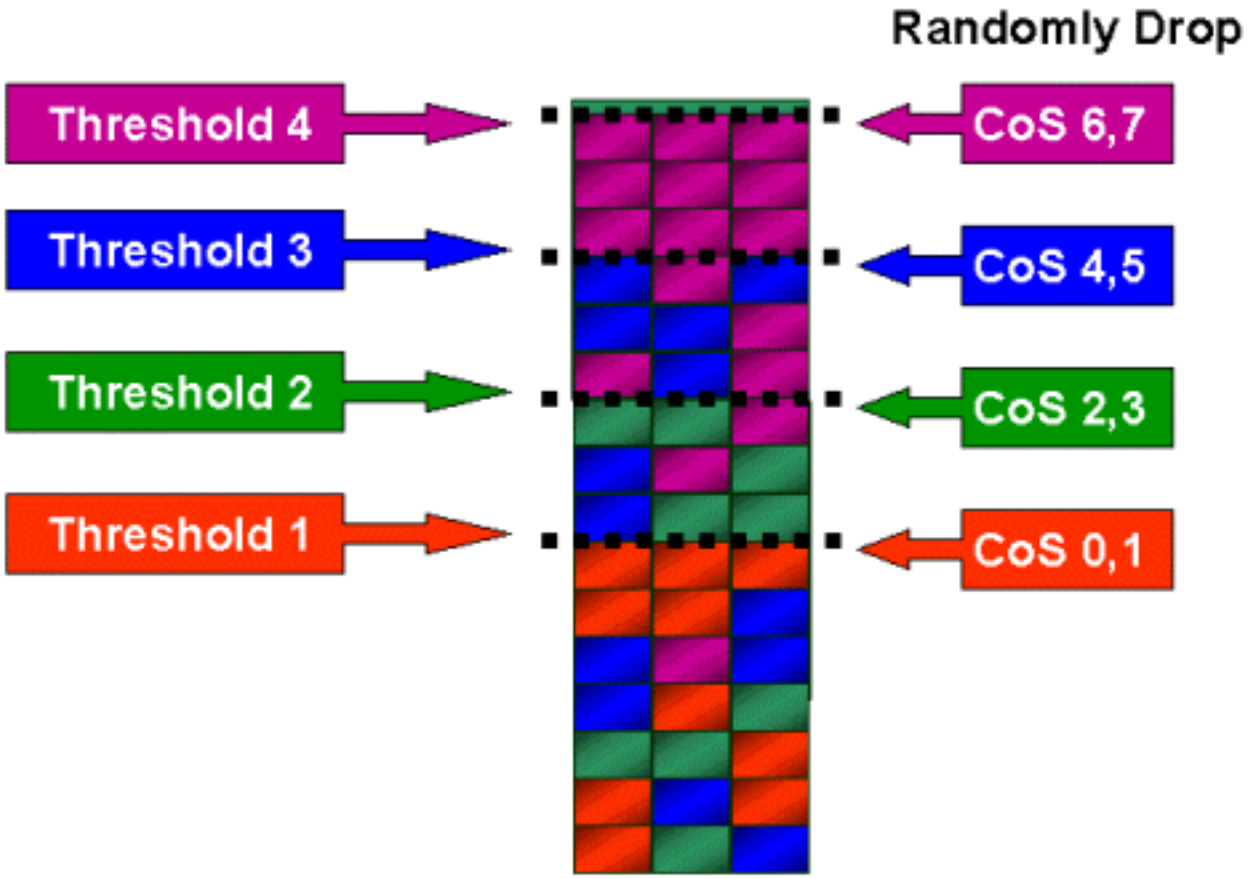
```
Console> (enable) set qos Mac-COs 00-00-0c-33-2a-4e 200 5
!-- COs 5 is assigned to 00-00-0c-33-2a-4e VLAN 200. Console> (enable)
```

Mit diesem Befehl werden für jeden Frame, dessen MAC-Zieladresse 00-00-0c-33-2a-4e ist, die vom VLAN 200 stammt, die COs 5 festgelegt.

Im integrierten Cisco IOS-Modus (nativer Modus) gibt es keinen entsprechenden Befehl. Dies liegt daran, dass dieser Befehl nur unterstützt wird, wenn kein PFC vorhanden ist und für die Funktion des integrierten Cisco IOS (Native Mode) eine PFC erforderlich ist.

Zuordnung von COs zu Schwellenwerten

Nach der Konfiguration der Schwellenwerte kann der Administrator diesen Schwellenwerten CO-Werte zuweisen, sodass Frames mit bestimmten CO-Werten verworfen werden können, wenn der Schwellenwert überschritten wurde. In der Regel weist der Administrator den unteren Schwellenwerten Frames mit niedrigerer Priorität zu, sodass der Datenverkehr mit höherer Priorität in der Warteschlange aufrechterhalten wird, wenn eine Überlastung auftritt.



Die obige Abbildung zeigt eine Eingangswarteschlange mit vier Schwellenwerten und wie CO-Werte jedem Schwellenwert zugewiesen wurden.

Die folgende Ausgabe zeigt, wie CO-Werte Schwellenwerten zugeordnet werden können:

CatOS

```
Console> (enable) set qos map 2q2t 1 1 COs 0 1
!-- QoS TX priority queue and threshold mapped to COs successfully. Console> (enable)
```

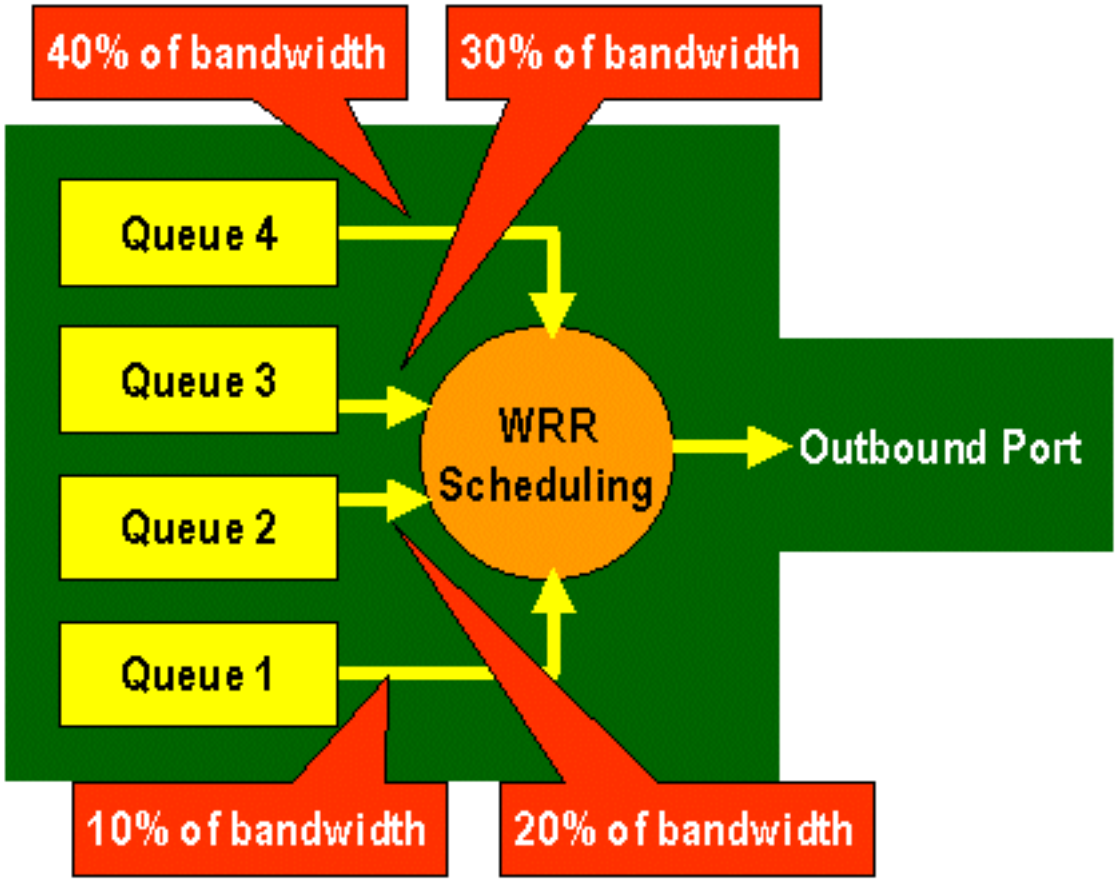
Mit diesem Befehl werden der Warteschlange 1, Schwellenwert 1, die CO-Werte 0 und 1 zugewiesen. Der entsprechende Befehl in Integrated Cisco IOS (Native Mode) wird unten angezeigt.

Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config-if)# wrr-queue COs-map  1  1  0  1
Cat6500(config-if)#
```

Konfigurieren der Bandbreite für TX-Warteschlangen

Wenn ein Frame in eine Ausgabewarteschlange gestellt wird, wird er mithilfe eines Ausgabeplanungs-Algorithmus übertragen. Der Ausgabeplaner-Prozess verwendet WRR, um Frames aus den Ausgabewarteschlangen zu übertragen. Je nach verwendeter Linecard-Hardware gibt es zwei, drei oder vier Übertragungswarteschlangen pro Port.



Auf den Linecards WS-X6248 und WS-X6348 (mit 2q2t-Warteschlangenstrukturen) werden zwei TX-Warteschlangen vom WRR-Mechanismus für die Planung verwendet. Auf den WS-X6548-Linecards (mit einer 1p3q1t-Warteschlangenstruktur) gibt es vier TX-Warteschlangen. Von diesen vier TX-Warteschlangen werden drei TX-Warteschlangen vom WRR-Algorithmus bedient (die letzte TX-Warteschlange ist eine SP-Warteschlange). Auf GE-Linecards gibt es drei TX-Warteschlangen (unter Verwendung einer 1p2q2t-Warteschlangenstruktur). Eine dieser Warteschlangen ist eine SP-Warteschlange, sodass der WRR-Algorithmus nur zwei TX-Warteschlangen unterstützt.

In der Regel weist der Administrator der TX-Warteschlange eine Gewichtung zu. WRR verwendet die Gewichtung der Portwarteschlange, die vom Switch intern verwendet wird, um zu bestimmen, wie viel Datenverkehr übertragen wird, bevor er in die nächste Warteschlange verschoben wird. Jeder Port-Warteschlange kann ein Gewichtungswert zwischen 1 und 255 zugewiesen werden.

CatOS

```
Console> (enable) set qos wrr 2q2t 40 80
!-- QoS wrr ratio set successfully. Console> (enable)
```

Dieser Befehl weist der Warteschlange 1 eine Gewichtung von 40 und der Warteschlange 2 eine Gewichtung von 80 zu. Dies bedeutet im Grunde ein Verhältnis von zwei zu einem (80 zu 40 = 2 zu 1) der Bandbreite, die zwischen den beiden Warteschlangen zugewiesen wird. Dieser Befehl wird auf allen Ports mit zwei Warteschlangen und zwei Schwellenwerten für Ports ausgeführt.

Der entsprechende Befehl, der im integrierten Cisco IOS-Modus (Native Mode) ausgegeben wird, ist unten dargestellt.

Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config-if)# wrr-queue bandwidth 1 3
Cat6500(config-if)#
```

Die obige Darstellung stellt ein Verhältnis von drei zu einem Verhältnis zwischen den beiden Warteschlangen dar. Sie werden feststellen, dass die Cat IOS-Version dieses Befehls nur für eine bestimmte Schnittstelle gilt.

Zuordnung von DSCP zu COs

Wenn der Frame in den Ausgangsport verschoben wurde, verwendet der Port-ASIC die zugewiesenen COs, um eine Überlastungsvermeidung (d. h. WRED) durchzuführen, und verwendet die COs, um die Planung des Frames (d. h. die Übertragung des Frames) zu bestimmen. An diesem Punkt verwendet der Switch eine Standardzuordnung, um das zugewiesene DSCP zu übernehmen und einem CO-Wert zuzuordnen. Diese Standardzuordnung wird in dieser Tabelle angezeigt.

Alternativ kann der Administrator eine Karte erstellen, die vom Switch verwendet wird, um den zugewiesenen internen DSCP-Wert zu verwenden und einen neuen CO-Wert für den Frame zu erstellen. Nachfolgend finden Sie Beispiele dafür, wie Sie CatOS und das integrierte Cisco IOS (Native Mode) nutzen würden, um dies zu erreichen.

CatOS

```
Console> (enable) set qos dscp-cos--map 20-30:5 10-15:3 45-52:7
!-- QoS dscp-cos-map set successfully. Console> (enable)
```

Der obige Befehl ordnet die DSCP-Werte 20 bis 30 einem COs-Wert von 5 zu, die DSCP-Werte 10 bis 15 einem COs von 3 und die DSCP-Werte 45 bis 52 einem COs-Wert von 7. Alle anderen DSCP-Werte verwenden die Standardzuordnung, die bei Aktivierung von QoS auf dem Switch erstellt wurde.

Der entsprechende Befehl, der im integrierten Cisco IOS-Modus (Native Mode) ausgegeben wird, ist unten dargestellt.

Integriertes Cisco IOS (nativer Modus)

```
Cat6500(config)# mls qos map dscp-cos 20 30 40 50 52 10 1 to 3
Cat6500(config)#
```

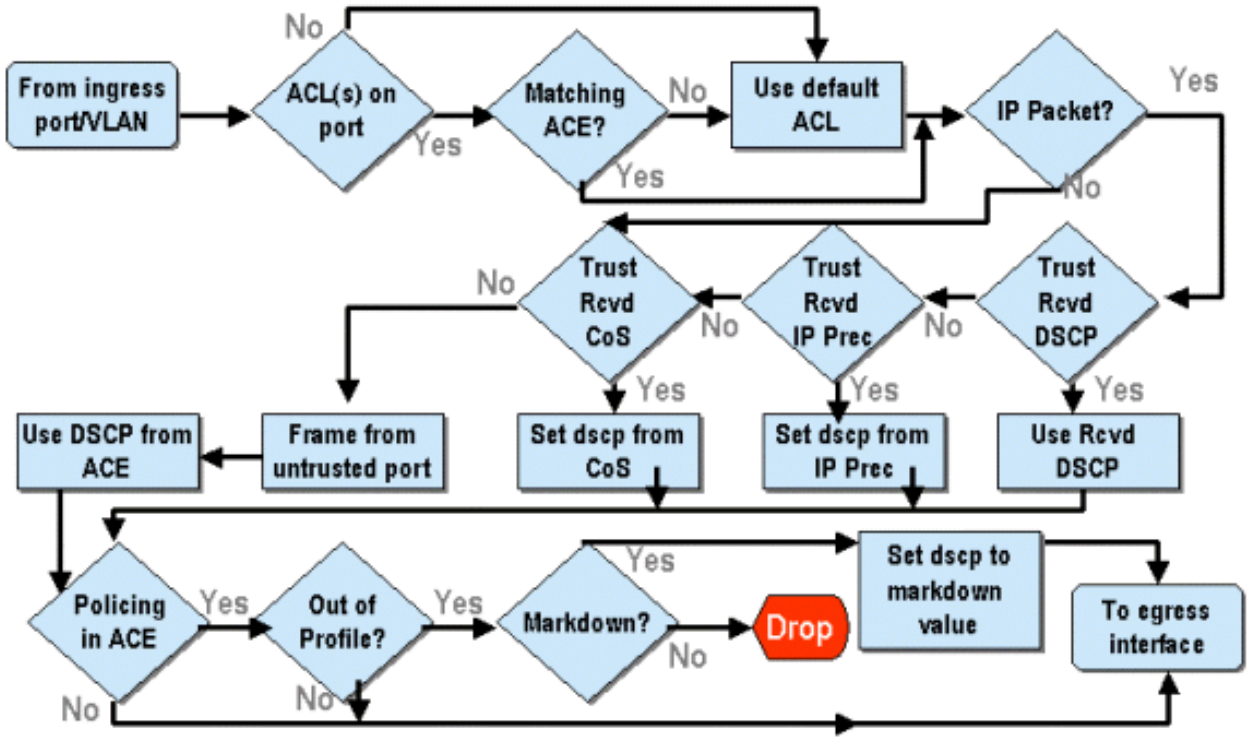
Damit werden die DSCP-Werte 20, 30, 40, 50, 52, 10 und 1 auf einen COs-Wert von 3 festgelegt.

Klassifizierung und Richtlinienvergabe mit PFC

Die PFC unterstützt die Klassifizierung und Richtlinienvergabe von Frames. Bei der Klassifizierung kann eine ACL verwendet werden, um einen eingehenden Frame mit einer Priorität (DSCP) zuzuweisen (zu markieren). Durch die Richtlinienvergabe kann ein Datenstrom auf eine bestimmte Bandbreite beschränkt werden.

In den folgenden Abschnitten werden diese Funktionen für die PFC sowohl aus der Perspektive

der CatOS- als auch der Integrated Cisco IOS (Native Mode) OS-Plattformen beschrieben. Die von der PFC angewendeten Prozesse sind im folgenden Diagramm dargestellt:



Konfigurieren von Richtlinien für die Catalyst 6000-Familie mit CatOS

Die Richtlinienfunktion ist in zwei Abschnitte unterteilt: einen für CatOS und einen für Integrated Cisco IOS (Native Mode). Beide erreichen dasselbe Endergebnis, werden jedoch auf unterschiedliche Weise konfiguriert und implementiert.

Richtlinienvergabe

Die PFC unterstützt die Möglichkeit, eingehenden Datenverkehr an den Switch zu begrenzen (oder zu überwachen) und den Datenverkehrsfluss auf ein vordefiniertes Limit zu reduzieren. Datenverkehr, der diesen Grenzwert überschreitet, kann verworfen werden oder der DSCP-Wert im Frame wird auf einen niedrigeren Wert markiert.

Die Beschränkung der Ausgangsrate (Ausgang) wird derzeit weder von PFC1 noch von PFC2 unterstützt. Dies wird in eine neue Version der PFC eingefügt, die für das zweite Halbjahr 2002 geplant ist und die Output- (oder Egress-) Policing unterstützt.

Das Policing wird sowohl im CatOS als auch im neuen integrierten Cisco IOS (Native Mode) unterstützt, obwohl die Konfiguration dieser Funktionen sehr unterschiedlich ist. In den folgenden Abschnitten wird die Konfiguration der Richtlinien in beiden Betriebssystemplattformen beschrieben.

Aggregate und Mikroflows (CatOS)

Aggregate und Microflows sind Begriffe, mit denen der Umfang der vom PFC durchgeführten Richtlinien definiert wird.

Ein Mikroflow definiert die Richtlinienvergabe für einen einzelnen Fluss. Ein Datenfluss wird durch eine Sitzung mit einer eindeutigen SA/DA-MAC-Adresse, SA/DA-IP-Adresse und TCP/UDP-Portnummern definiert. Für jeden neuen Datenfluss, der über einen VLAN-Port initiiert wird, kann

der Microflow verwendet werden, um die Datenmenge zu begrenzen, die der Switch für diesen Datenfluss empfängt. In der Mikroflow-Definition können Pakete, die die vorgeschriebene Ratengrenze überschreiten, entweder verworfen werden oder ihr DSCP-Wert wird deaktiviert.

Ähnlich wie bei einem Mikroflow kann ein Aggregat verwendet werden, um den Datenverkehr zu begrenzen. Die Aggregatrate gilt jedoch für den gesamten eingehenden Datenverkehr an einem Port oder VLAN, der mit einer angegebenen QoS-ACL übereinstimmt. Sie können das Aggregat als Richtlinie für den kumulativen Datenverkehr anzeigen, der mit dem Profil in der Zugriffssteuerungseingabe (ACE) übereinstimmt.

Sowohl Aggregat als auch Microflow definieren die Menge an Datenverkehr, der in den Switch aufgenommen werden kann. Ein Aggregat und ein Microflow können gleichzeitig einem Port oder einem VLAN zugewiesen werden.

Bei der Definition von Mikroströmen können bis zu 63 davon definiert und bis zu 1023 Aggregate definiert werden.

Zugriffskontrolleinträge und QoS-ACLs (CatOS)

Eine QoS-ACL besteht aus einer Liste von ACEs, die eine Reihe von QoS-Regeln definieren, die die PFC zur Verarbeitung eingehender Frames verwendet. ACEs ähneln einer RACL (Router Access Control List). Der ACE definiert Klassifizierungs-, Marking- und Richtlinienkriterien für einen eingehenden Frame. Wenn ein eingehender Frame die im ACE festgelegten Kriterien erfüllt, verarbeitet die QoS-Engine den Frame (wie vom ACE als angenommen).

Die gesamte QoS-Verarbeitung erfolgt in der Hardware, sodass die Aktivierung der QoS-Richtlinienvergabe die Leistung des Switches nicht beeinträchtigt.

Die PFC2 unterstützt derzeit bis zu 500 ACLs, und diese ACLs können aus bis zu 32.000 Aces bestehen (insgesamt). Die tatsächlichen ACE-Nummern hängen von anderen Services ab, die im PFC definiert sind und über die verfügbarer Speicher verfügt.

Es gibt drei Arten von Asse, die definiert werden können. Dabei handelt es sich um IP-, IPX- und MAC-Adressen. Sowohl IP- als auch IPX-Asse überprüfen L3-Headerinformationen, während MAC-basierte Asse nur L2-Headerinformationen prüfen. Es ist zu beachten, dass MAC-Asse nur auf Nicht-IP- und Nicht-IPX-Datenverkehr angewendet werden können.

Erstellen von Policing-Regeln

Beim Erstellen einer Regelrichtlinienregel wird ein Aggregat (oder Microflow) erstellt und dieser dann einem ACE zugeordnet.

Wenn beispielsweise der gesamte eingehende IP-Datenverkehr an Port 5/3 auf maximal 20 MB beschränkt werden sollte, müssen die beiden oben genannten Schritte konfiguriert werden.

Zunächst wird im Beispiel gefordert, dass der gesamte eingehende IP-Datenverkehr beschränkt wird. Dies impliziert, dass eine Gesamtüberwachung definiert werden muss. Ein Beispiel hierfür ist:

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13 policed-dscp
!-- Hardware programming in progress !-- QoS policer for aggregate test-flow created
successfully. Console> (enable)
```

Wir haben ein Aggregat namens "Testfluss" erstellt. Sie definiert eine Rate von 20.000 KBPS (20

MBIT/S) und eine Burst von 13 Punkten. Das Schlüsselwort "policed-dscp" gibt an, dass für alle Daten, die diese Richtlinie überschreiten, der DSCP-Wert wie in einer DSCP-Markdown-Karte angegeben deklariert ist (eine Standard-Zuordnung ist vorhanden oder kann vom Administrator geändert werden). Eine Alternative zur Verwendung des policed-dscp-Schlüsselworts ist die Verwendung des drop-Schlüsselworts. Das drop-Schlüsselwort verwirft einfach den gesamten Out-of-Profile-Datenverkehr (Datenverkehr, der über den zugewiesenen Burst-Wert hinausgeht).

Die Überwachungseinrichtung arbeitet mit einem undichten Token-Ecket-Schema, indem Sie einen Burst definieren (d. h. die Datenmenge in Bits pro Sekunde, die Sie in einem bestimmten (festen) Zeitintervall akzeptieren), und dann die Rate (die als die Datenmenge definiert ist, die Sie in einer Sekunde aus diesem Eimer leeren werden). Alle Daten, die diese Gruppe überfluten, werden entweder verworfen oder ihr DSCP ist deaktiviert. Der oben angegebene Zeitraum (oder das oben angegebene Intervall) beträgt 0,00025 Sekunden (bzw. 1/4000 Sekunden) und ist fest (Sie können also keine Konfigurationsbefehle verwenden, um diese Zahl zu ändern).

Die Zahl 13 aus dem obigen Beispiel stellt einen Eimer dar, der bis zu 13.000 Bit Daten pro 1/4.000 Sekunde aufnehmen kann. Dies bezieht sich auf 52 MB pro Sekunde (13K * (1 / 0,00025) oder 13K * 4000). Sie müssen immer sicherstellen, dass Ihr Burst so konfiguriert ist, dass er gleich oder größer als die Geschwindigkeit ist, mit der Daten gesendet werden sollen. Anders ausgedrückt: Der Burst sollte größer oder gleich der minimalen Datenmenge sein, die Sie für einen bestimmten Zeitraum übertragen möchten. Wenn der Burst eine niedrigere Zahl ergibt als die von Ihnen angegebene Rate, entspricht die Ratenbeschränkung dem Burst. Mit anderen Worten: Wenn Sie eine Rate von 20 MBIT/S und einen Burst von 15 MBIT/S definieren, wird Ihre Rate nur auf 15 MBPS steigen. Die nächste Frage, die Sie stellen könnten, ist warum 13? Denken Sie daran, dass der Burst die Tiefe des Tokenbuckets definiert, also die Tiefe des Eckels, der für den Empfang eingehender Daten alle 1/400 Sekunden verwendet wird. Der Burst kann also eine beliebige Zahl sein, die bei einer Ankunftsdatenrate von mindestens 20 MB pro Sekunde unterstützt wird. Der minimale Burst, den man für eine Durchsatzgrenze von 20 MB verwenden könnte, ist 2000/4000 = 5.

Beim Verarbeiten der Richtlinie beginnt der Regelungsalgorithmus, indem er die Tokenbuchse mit einer vollständigen Ergänzung von Token füllt. Die Anzahl der Token entspricht dem Burst-Wert. Wenn der Burst-Wert also 13 beträgt, beträgt die Anzahl der Token in der Eimer 13.000. Für jede 1/4000. Sekunde sendet der Regelungsalgorithmus eine Datenmenge, die der durch 4000 dividierten definierten Rate entspricht. Für jedes Bit (Binärziffer) der gesendeten Daten wird ein Token aus dem Eimer verwendet. Am Ende des Intervalls wird der Eimer mit einem neuen Satz von Token aufgefüllt. Die Anzahl der Token, die es ersetzt wird, wird durch die Rate / 4000 definiert. Betrachten Sie das obige Beispiel, um Folgendes zu verstehen:

```
Console> (enable) set qos policer aggregate test-flow rate 20000 burst 13
```

Angenommen, es handelt sich um einen 100-MBPS-Port, den wir in einem konstanten Stream von 100 MBPS an den Port senden. Wir wissen, dass dies einer eingehenden Rate von 100.000.000 Bit pro Sekunde entspricht. Die Parameter hier sind eine Rate von 20000 und Burst von 13. Im Zeitintervall t0 befindet sich eine vollständige Ergänzung von Token im Eimer (13.000). Im Zeitintervall t0 werden die ersten Daten in den Port eingegeben. In diesem Zeitintervall beträgt die Ankunftsrate 100.000.000 / 4000 = 25.000 Bit pro Sekunde. Da unsere Token-Eimer nur eine Tiefe von 13.000 Token hat, sind nur 13.000 Bit der 25.000 Bits, die in diesem Intervall in den Port gelangen, für das Senden zulässig und 12.000 Bit werden verworfen.

Die angegebene Rate definiert eine Weiterleitungsrate von 20.000.000 Bit pro Sekunde, was 5.000 Bit entspricht, die pro 1/4000-igem Intervall gesendet werden. Für jede gesendete 5.000 Bit werden 5.000 Token verbraucht. Im Zeitintervall T1 kommen weitere 25.000 Bit an Daten ein, aber der Eimer verliert 12.000 Bit. Der Eimer wird mit Token aufgefüllt, die als Rate / 4000 definiert sind

(was 5.000 neue Token entspricht). Der Algorithmus sendet dann die nächste Ergänzung von Daten, die weitere 5.000 Bit an Daten entspricht (dies erfordert weitere 5.000 Token) und so weiter für jedes Intervall.

Im Wesentlichen werden alle Daten, die über die Eckettiefe (definierter Burst) hinausgehen, verworfen. Die Daten, die nach dem Versenden der Daten noch übrig geblieben sind (entsprechend der angegebenen Rate), werden ebenfalls verworfen, und der nächste Datensatz wird ersetzt. Ein unvollständiges Paket ist ein Paket, das nicht vollständig innerhalb des Zeitintervalls empfangen wurde, aber nicht verworfen wird, bis es vollständig in den Port empfangen wurde.

Diese Burst-Zahl geht von einem konstanten Datenverkehrsfluss aus. In realen Netzwerken sind die Daten jedoch nicht konstant und ihr Datenfluss wird durch TCP-Fenstergrößen bestimmt, die TCP-Bestätigungen in die Übertragungssequenz einbeziehen. Um die Probleme mit TCP-Fenstergrößen zu berücksichtigen, wird empfohlen, den Burst-Wert zu verdoppeln. Im obigen Beispiel wird der empfohlene Wert von 13 als 26 konfiguriert.

Ein weiterer wichtiger Punkt ist, dass im Zeitintervall 0 (d. h. am Anfang eines Regelungszyklus) die Token-Eimer voll von Token ist.

Diese Gesamtrichtlinie muss nun in einen QoS-ACE integriert werden. Der ACE ist der Ort, an dem die Spezifikation erstellt wird, um einem eingehenden Frame eine Reihe von Kriterien zuzuordnen. Betrachten Sie das folgende Beispiel. Sie möchten die oben definierte Aggregation auf den gesamten IP-Datenverkehr anwenden, jedoch speziell für Datenverkehr, der von Subnetz 10.5.x.x stammt und für Subnetz 203.100.45.x bestimmt ist. Der ACE sieht wie folgt aus:

```
Console> (enable) set qos acl ip test-acl trust-dscp aggregate test-flow tcp 10.5.0.0
203.100.45.0
!-- Test-acl editbuffer modified. Issue the commit command to apply changes.
Console> (enable)
```

Der obige Befehl hat einen IP-ACE erstellt (durch die Verwendung des Befehls **set qos acl ip**), der nun einer QoS-ACL mit der Bezeichnung test-acl zugeordnet ist. Nachfolgende Aces, die erstellt wurden und der ACL-Test-ACL zugeordnet sind, werden am Ende der ACE-Liste angehängt. Dem ACE-Eintrag ist der aggregierte Testfluss zugeordnet. Bei allen TCP-Flüssen mit dem Quell-Subnetz 10.5.0.0 und dem Ziel-Subnetz 203.100.45.0 wird diese Richtlinie auf sie angewendet.

ACLs (und die zugehörigen ACLs) bieten ein sehr hohes Maß an Konfigurationsflexibilität, das Administratoren verwenden können. Eine ACL kann aus einem oder mehreren Asse bestehen, und es können Quell- und/oder Zieladressen sowie L4-Port-Werte verwendet werden, um bestimmte Flüsse zu identifizieren, die überwacht werden müssen.

Bevor eine Richtlinie tatsächlich erfolgt, muss die ACL jedoch entweder einem physischen Port oder einem VLAN zugeordnet werden.

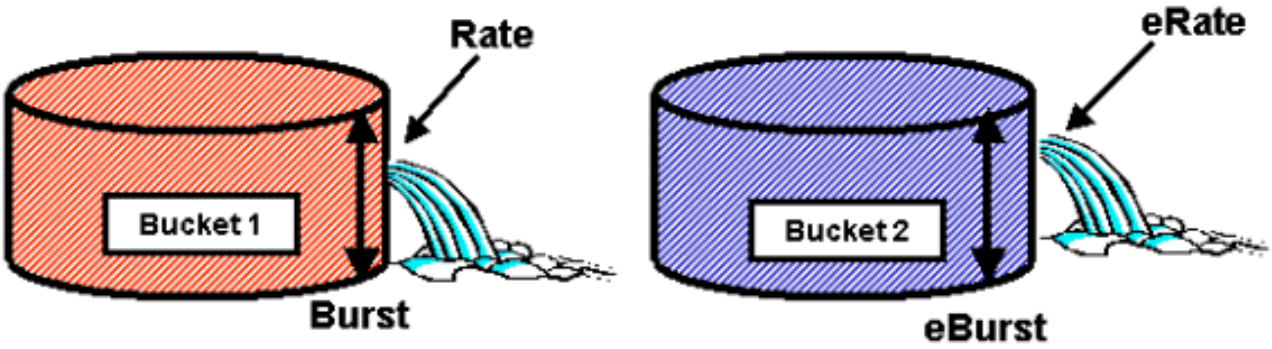
PFC2-Richtlinienentscheidungen

Für PFC2 wurde in CatOS 7.1 und CatOS 7.2 eine Änderung vorgenommen, mit der ein doppelter Schlitzkabelalgorithmus für die Richtlinienvergabe eingeführt wurde. Mit diesem neuen Algorithmus werden die folgenden zwei neuen Ebenen hinzugefügt:

1. **Normale Policing-Ebene:** Dies entspricht dem ersten Eimer und definiert Parameter, die die Tiefe des Eckets (Burst) und die Geschwindigkeit angeben, mit der Daten aus dem

Eimer gesendet werden sollen (Rate).

2. **Übermäßige Richtlinienvergabe:** Dies entspricht einem zweiten Eimer und definiert Parameter, die die Tiefe des Eckels (Esel) und die Geschwindigkeit angeben, mit der Daten aus dem Eimer gesendet werden sollen (Erate).



Dieser Prozess funktioniert so, dass Daten das erste Eimer ausfüllen. Der PFC2 akzeptiert einen eingehenden Datenstrom, der kleiner oder gleich der Tiefe (Burst-Wert) der ersten Bucket ist. Daten, die aus dem ersten Eimer überlaufen, können markiert und an den zweiten Eimer übergeben werden. Der zweite Eimer kann eine eingehende Rate von Daten akzeptieren, die von der ersten Gruppe übertragen werden, und zwar zu einem Wert, der kleiner oder gleich dem höchsten Wert ist. Die Daten aus der zweiten Eimer werden mit einer Geschwindigkeit gesendet, die durch den erateten Parameter abzüglich des Ratenparameters definiert ist. Daten, die aus dem zweiten Eimer überlaufen, können ebenfalls markiert oder verworfen werden.

Ein Beispiel für eine doppelte Schlitzverschlussprüfung ist:

```
Console> (enable) set qos policer aggregate AGG1 rate 10000 policed-dscp erate 12000 drop burst
13 eburst 13
```

In diesem Beispiel wird ein Aggregat mit dem Namen AGG1 mit einer Datenverkehrsrate von mehr als 10 MBPS eingerichtet und entsprechend der bereitgestellten DSCP-Zuordnung gekennzeichnet. Datenverkehr, der den ursprünglichen Wert übersteigt (auf 12 MBPS festgelegt), wird entsprechend dem Drop-Schlüsselwort verworfen.

Anwenden von Aggregate Policers auf DFC-fähige Module

Es ist zu beachten, dass die Anwendung von Aggregat-Policers auf Line Cards ohne DFC möglich ist, da der 6000 eine zentrale Weiterleitungs-Engine (PFC) für die Weiterleitung von Datenverkehr verwendet. Durch die Implementierung einer zentralen Weiterleitungs-Engine kann die Engine die Datenverkehrsstatistiken für ein bestimmtes VLAN verfolgen. Dieser Prozess kann verwendet werden, um eine aggregierte Policer auf ein VLAN anzuwenden.

Auf einer DFC-fähigen Linecard werden Weiterleitungsentscheidungen jedoch an diese Linecard verteilt. Die DFC kennt nur die Ports ihrer direkten Linecard und kennt keine Datenverkehrsbewegungen auf anderen Linecards. Aus diesem Grund kann die Richtlinie inkonsistente Ergebnisse hervorrufen, wenn eine aggregierte Richtlinie auf ein VLAN angewendet wird, das über Mitgliedsports für mehrere DFC-Module verfügt. Der Grund hierfür ist, dass die DFC nur die lokalen Port-Statistiken verfolgen kann und keine Port-Statistiken für andere Line Cards berücksichtigt. Aus diesem Grund führt eine auf ein VLAN angewendete aggregierte Policer mit Mitglieds-Ports auf einer DFC-fähigen Linecard zu einem DFC-Richtlinienverkehr bis zum Nominallimit für VLAN-Ports, die nur auf der DFC-Linecard vorhanden sind.

DSCP-Markdown-Karten (CatOS)

DSCP-Markdown-Karten werden verwendet, wenn die Richtlinie so definiert ist, dass der Out-of-Profile-Datenverkehr markiert wird, anstatt ihn zu verwerfen. Der Out-of-Profile-Datenverkehr wird definiert als Datenverkehr, der die definierte Burst-Einstellung überschreitet.

Wenn QoS aktiviert ist, wird eine Standard-DSCP-Markdown-Zuordnung eingerichtet. Diese Standard-Markdown-Zuordnung ist in dieser Tabelle weiter oben im Dokument aufgeführt. Mit der Befehlszeilenschnittstelle (CLI) kann ein Administrator die Standard-Markdown-Zuordnung ändern, indem er den Befehl **set qos policed-dscp-map** ausgibt. Ein Beispiel hierfür ist unten dargestellt.

```
Cat6500(config)# set qos policed-dscp-map 20-25:7 33-38:3
```

In diesem Beispiel wird die überwachte DSCP-Zuordnung so geändert, dass die DSCP-Werte 20 bis 25 nach unten auf einen DSCP-Wert 7 markiert werden und die DSCP-Werte 33 bis 38 nach unten auf einen DSCP-Wert 3 markiert werden.

Zuordnen von Richtlinien zu VLANs und Ports (CatOS)

Nachdem eine ACL erstellt wurde, muss sie entweder einem Port oder einem VLAN zugeordnet werden, damit diese ACL wirksam wird.

Ein interessanter Befehl, der viele unbewusst ist, ist die Standard-QoS-Einstellung, die alle QoS-Ports basiert. Wenn Sie ein Aggregat (oder einen Microflow) auf ein VLAN anwenden, wird es nur dann auf einen Port angewendet, wenn dieser Port für VLAN-basierte QoS konfiguriert wurde.

```
Console> (enable) set port qos 2/5-10 vlan-based
!-- Hardware programming in progress  !-- QoS interface is set to vlan-based for ports 2/5-10.
Console> (enable)
```

Durch die Änderung der portbasierten QoS in VLAN-basierte QoS werden sofort alle diesem Port zugewiesenen ACLs entfernt und diesem Port alle VLAN-basierten ACLs zugewiesen.

Die Zuordnung der ACL zu einem Port (oder VLAN) erfolgt über den folgenden Befehl:

```
Console> (enable) set qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is attached to port 3/5. Console>
(enable) Console> (enable) set qos acl map test-acl 18
!-- Hardware programming in progress  !-- ACL test-acl is attached to VLAN 18. Console> (enable)
```

Selbst nach der Zuordnung der ACL zu einem Port (oder VLAN) wird die ACL erst wirksam, wenn die ACL der Hardware zugewiesen wurde. Dies wird im folgenden Abschnitt beschrieben. An diesem Punkt befindet sich die ACL im temporären Editierpuffer im Speicher. In diesem Puffer kann die ACL geändert werden.

Wenn Sie nicht bestätigte ACLs entfernen möchten, die sich im Editbuffer befinden, wird der **Rollback-**Befehl ausgegeben. Dieser Befehl löscht im Wesentlichen die ACL aus dem Bearbeitungspuffer.

```
Console> (enable) rollback qos acl test-acl
!-- Rollback for QoS ACL test-acl is successful. Console> (enable)
```

Übergeben von ACLs (CatOS)

Um die von Ihnen definierte QoS-ACL anzuwenden (siehe oben), muss die ACL Hardware zugewiesen werden. Das Commit-Verfahren kopiert die ACL aus dem temporären Puffer auf die PFC-Hardware. Sobald sie sich im PFC-Speicher befinden, kann die in der QoS-ACL definierte Richtlinie auf den gesamten Datenverkehr angewendet werden, der mit den Aces übereinstimmt.

Um die Konfiguration zu vereinfachen, geben die meisten Administratoren einen **Commit All-**Befehl aus. Sie können jedoch eine bestimmte Zugriffskontrollliste (eine von vielen) festlegen, die sich derzeit im Bearbeitungspuffer befindet. Ein Beispiel für den Commit-Befehl ist unten dargestellt.

```
Console> (enable) commit qos acl test-acl
!-- Hardware programming in progress  !-- ACL test-acl is committed to hardware. Console>
(enable)
```

Wenn Sie eine ACL von einem Port (oder einem VLAN) entfernen möchten, müssen Sie die Zuordnung, die diese ACL mit diesem Port (oder VLAN) verknüpft, löschen, indem Sie den folgenden Befehl eingeben:

```
Console> (enable) clear qos acl map test-acl 3/5
!-- Hardware programming in progress  !-- ACL test-acl is detached from port 3/5.
Console>(enable)
```

Konfigurieren der Richtlinienüberwachung auf der Catalyst 6000-Familie mit integriertem Cisco IOS (nativer Modus)

Die Richtlinienvergabe wird mit dem integrierten Cisco IOS (Native Mode) unterstützt. Die Konfiguration und Implementierung der Richtlinienfunktion erfolgt jedoch mithilfe von Richtlinienzuordnungen. Jede Richtlinienzuordnung verwendet mehrere Richtlinienklassen, um eine Richtlinienzuordnung zu erstellen. Diese Richtlinienklassen können für verschiedene Arten von Datenverkehrsflüssen definiert werden.

Bei der Filterung verwenden Richtlinienzuordnungsklassen IOS-basierte ACLs und Class Match Statements, um den zu überwachenden Datenverkehr zu identifizieren. Nachdem der Datenverkehr identifiziert wurde, können die Richtlinienklassen mithilfe von Aggregat- und Microflow-Policers die Policing-Richtlinien auf den entsprechenden Datenverkehr anwenden.

In den folgenden Abschnitten wird die Konfiguration der Richtlinienvergabe für das integrierte Cisco IOS (Native Mode) ausführlich erläutert.

Aggregate und Mikroflows (integriertes Cisco IOS (nativer Modus))

Aggregate und Mikroflows sind Begriffe, die zum Definieren des Regelungsbereichs verwendet werden, den die PFC durchführt. Ähnlich wie bei CatOS werden auch in Integrated Cisco IOS (Native Mode) Aggregate und Mikroflows verwendet.

Ein Mikroflow definiert die Richtlinienvergabe für einen einzelnen Fluss. Ein Datenfluss wird durch eine Sitzung mit einer eindeutigen SA/DA-MAC-Adresse, SA/DA-IP-Adresse und TCP/UDP-Portnummern definiert. Für jeden neuen Datenfluss, der über einen VLAN-Port initiiert wird, kann der Microflow verwendet werden, um die Datenmenge zu begrenzen, die der Switch für diesen Datenfluss empfängt. In der Mikroflow-Definition können Pakete, die die vorgeschriebene Ratengrenze überschreiten, entweder verworfen werden oder ihr DSCP-Wert wird deaktiviert. Mikroflows werden mithilfe des Befehls für den Polizeifluss angewendet, der Teil einer Richtlinienzuordnungsklasse ist.

Um die Mikroflow-Überwachung im integrierten Cisco IOS (Native Mode) zu aktivieren, muss sie global auf dem Switch aktiviert werden. Dies kann mithilfe des folgenden Befehls erreicht werden:

```
Cat6500(config)# mls qos flow-policing
```

Microflow-Richtlinien können auch auf überbrückten Datenverkehr angewendet werden, d. h. Datenverkehr, der nicht über das L3-Protokoll geleitet wird. Führen Sie den folgenden Befehl aus, um den Switch für die Unterstützung der Microflow-Überwachung bei überbrücktem Datenverkehr zu aktivieren:

```
Cat6500(config)# mls qos bridged
```

Dieser Befehl ermöglicht auch die Microflow-Überwachung von Multicast-Datenverkehr. Wenn für Multicast-Datenverkehr eine Microflow-Überwachung angewendet werden muss, muss dieser Befehl (**mls qos Bridged**) aktiviert werden.

Ähnlich wie bei einem Mikroflow kann ein Aggregat verwendet werden, um den Datenverkehr zu begrenzen. Die Aggregatrate gilt jedoch für den gesamten eingehenden Datenverkehr an einem Port oder VLAN, der mit einer angegebenen QoS-ACL übereinstimmt. Sie können das Aggregat als Richtlinie für den kumulativen Datenverkehr anzeigen, der mit einem definierten Datenverkehrsprofil übereinstimmt.

Es gibt zwei Arten von Aggregaten, die in Integrated Cisco IOS (Native Mode) wie folgt definiert werden können:

- Aggregations-Policys für jede Schnittstelle
- benannte Aggregat Policers

Die Aggregate werden pro Schnittstelle auf eine einzelne Schnittstelle angewendet, indem der **Befehl** für die **Polizei** in einer Richtlinienzuordnungsklasse ausgegeben wird. Diese Zuordnungsklassen können auf mehrere Schnittstellen angewendet werden, aber der Policer ordnet jede Schnittstelle separat zu. Benannte Aggregate werden kumulativ für eine Gruppe von Ports und für den Richtlinienverkehr über alle Schnittstellen angewendet. Benannte Aggregate werden mithilfe des Befehls **mls qos aggregate policer** angewendet.

Bei der Definition von Mikroströmen können bis zu 63 davon definiert und bis zu 1023 Aggregate definiert werden.

Erstellen von Policing-Regeln (integriertes Cisco IOS (nativer Modus))

Beim Erstellen einer Richtlinienregel wird ein Aggregat (oder Mikroflow) über eine Richtlinienzuordnung erstellt und diese Richtlinienzuordnung dann an eine Schnittstelle angefügt.

Betrachten Sie das gleiche Beispiel, das für CatOS erstellt wurde. Die Anforderung bestand darin, den gesamten eingehenden IP-Datenverkehr an Port 5/3 auf maximal 20 MBPS zu beschränken.

Zunächst muss eine Richtlinienzuordnung erstellt werden. Erstellen Sie eine Richtlinienzuordnung mit dem Namen "limit-traffic". Dies erfolgt wie folgt:

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)#
```

Sie werden sofort feststellen, dass sich die Switch-Eingabeaufforderung ändert, um anzuzeigen, dass Sie sich im Konfigurationsmodus zum Erstellen einer Zuordnungsklasse befinden. Beachten Sie, dass eine Richtlinienzuordnung mehrere Klassen enthalten kann. Jede Klasse enthält einen separaten Satz von Richtlinienaktionen, die auf verschiedene Datenverkehrsströme angewendet werden können.

Wir erstellen eine Datenverkehrsklasse, um den eingehenden Datenverkehr auf 20 MBPS zu beschränken. Diese Klassengrenze wird als "limit-to-20" bezeichnet. Dies ist unten abgebildet.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20
Cat6500(config-pmap-c)#
```

Die Eingabeaufforderung ändert sich erneut, um anzuzeigen, dass Sie sich jetzt in der Klassenkonfiguration der Map befinden (dargestellt mit der -c am Ende der Eingabeaufforderung). Wenn Sie die Ratenbeschränkung auf bestimmten eingehenden Datenverkehr anwenden möchten, können Sie eine ACL konfigurieren und diese auf den Klassennamen anwenden. Wenn Sie das 20-MBPS-Limit auf Datenverkehr anwenden möchten, der vom Netzwerk 10.10.1.x stammt, führen Sie die folgende ACL aus:

```
Cat6500(config)# access-list 101 permit ip 10.10.1.0  0.0.0.255 any
```

Sie können diese ACL dem Klassennamen wie folgt hinzufügen:

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)#
```

Nachdem Sie die Klassenzuordnung definiert haben, können Sie jetzt einzelne Policers für diese Klasse definieren. Sie können Aggregate (mithilfe des Schlüsselworts "Police") oder Microflows (mithilfe des Schlüsselworts "Police Flow") erstellen. Erstellen Sie die Aggregation, wie unten gezeigt.

```
Cat6500(config)# policy-map limit-traffic
Cat6500(config-pmap)# class limit-to-20 access-group 101
Cat6500(config-pmap-c)# police 20000000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

In der obigen Klassenanweisung (polizeilicher Befehl) wird eine Ratenbeschränkung von 2000.000 (20 MBPS) bei einem Burst von 52 MBPS (13.000 x 4.000 = 52 MB) festgelegt. Wenn der Datenverkehr mit dem Profil übereinstimmt und innerhalb des angegebenen Grenzwerts liegt, wird die Aktion durch die confirm-action-Anweisung festgelegt, um den Datenverkehr im Profil zu übertragen. Wenn der Datenverkehr außerhalb des Profils läuft (in unserem Beispiel über dem Grenzwert von 20 MB), wird die Anweisung "Mehr-Aktion" so eingestellt, dass der Datenverkehr verworfen wird (in unserem Beispiel wird der gesamte Datenverkehr über 20 MB verworfen).

Bei der Konfiguration eines Microflows wird eine ähnliche Aktion ausgeführt. Wenn alle Datenflüsse in einen Port begrenzt werden sollen, der einer bestimmten Klassenzuordnung jeweils 200 KB entspricht, entspricht die Konfiguration dieses Datenflusses der folgenden:

```
Cat6500(config)# mls qos flow-policing
Cat6500(config)# policy-map limit-each-flow
Cat6500(config-pmap)# class limit-to-200
Cat6500(config-pmap-c)# police flow 200000 13000 confirm-action transmit exceed-action drop
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
```

DSCP-Markdown-Karten

DSCP-Markdown-Karten werden verwendet, wenn die Richtlinie so definiert ist, dass der Out-of-Profile-Datenverkehr markiert wird, anstatt ihn zu verwerfen. Der Out-of-Profile-Datenverkehr wird definiert als Datenverkehr, der die definierte Burst-Einstellung überschreitet.

Wenn QoS aktiviert ist, wird eine Standard-DSCP-Markdown-Karte erstellt. Diese Standard-Markdown-Zuordnung ist in dieser Tabelle aufgeführt. Mit der CLI kann ein Administrator die Standard-Markdown-Zuordnung ändern, indem er den Befehl **set qos policed-dscp-map** ausgibt. Ein Beispiel hierfür ist unten dargestellt.

```
Cat6500(config)#

mls qos map policed-dscp normal-burst 32 to 16
```

In diesem Beispiel wird eine Änderung der standardmäßigen, überwachten DSCP-Zuordnung definiert, bei der der DSCP-Wert 32 nach unten auf den DSCP-Wert 16 markiert wird. Für einen Port mit dieser Richtlinie ist der DSCP-Wert für eingehende Daten, die Teil eines Datenblocks sind, der den angegebenen Burst übersteigt, auf 16 festgelegt.

Zuordnen von Richtlinien zu VLANs und Ports (integriertes Cisco IOS (nativer Modus))

Nachdem eine Richtlinie erstellt wurde, muss sie entweder einem Port oder einem VLAN zugeordnet werden, damit diese Richtlinie wirksam wird. Im Gegensatz zum Commit-Prozess in CatOS gibt es in Integrated Cisco IOS (Native Mode) keine Entsprechung. Wenn eine Richtlinie einer Schnittstelle zugeordnet wird, ist diese Richtlinie in Kraft. Führen Sie den folgenden Befehl aus, um die oben genannte Richtlinie einer Schnittstelle zuzuordnen:

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# service-policy input limit-traffic
```

Wenn einem VLAN eine Richtlinie zugeordnet ist, müssen Sie für jeden Port im VLAN, auf den die VLAN-Richtlinie angewendet werden soll, die Schnittstelle darüber informieren, dass QoS VLAN-basiert ist, indem Sie den Befehl **mls qos vlan-basiert** eingeben.

```
Cat6500(config)# interface fastethernet 3/5
Cat6500(config-if)# mls qos vlan-based
```

```
Cat6500(config-if)# exit
Cat6500(config)# interface vlan 100
Cat6500(config-if)# service-policy input limit-traffic
```

Wenn die Schnittstelle 3/5 Teil von VLAN 100 war, gilt die Richtlinie mit dem Namen "limit-traffic", die auf VLAN 100 angewendet wurde, auch für die Schnittstelle 3/5.

Konfigurieren der Klassifizierung auf der Catalyst 6000-Familie mit CatOS

Die PFC bietet Unterstützung für die Klassifizierung von Daten mithilfe von ACLs, die L2-, L3- und L4-Headerinformationen anzeigen können. Bei einer SupI oder IA (ohne PFC) ist die Klassifizierung auf die Verwendung der Schlüsselwörter "trust" (Vertrauen) auf den Ports beschränkt.

Im folgenden Abschnitt werden die QoS-Konfigurationskomponenten beschrieben, die vom PFC für die Klassifizierung in CatOS verwendet werden.

COs zu DSCP-Zuordnung (CatOS)

Beim Eingang zum Switch wird für einen Frame ein DSCP-Wert vom Switch festgelegt. Wenn sich der Port in einem vertrauenswürdigen Zustand befindet und der Administrator das Schlüsselwort trust-COs verwendet hat, wird der im Frame festgelegte COs-Wert verwendet, um den DSCP-Wert für den Frame zu bestimmen. Wie bereits erwähnt, kann der Switch dem Frame während der Switch-Übertragung Servicelevel zuweisen, basierend auf dem internen DSCP-Wert.

Dieses Schlüsselwort für einige der früheren 10/100-Module (WS-X6248 und WS-X6348) wird nicht unterstützt. Für diese Module wird empfohlen, mithilfe von ACLs CO-Einstellungen für eingehende Daten anzuwenden.

Wenn QoS aktiviert ist, erstellt der Switch eine Standardzuordnung. Diese Zuordnung wird verwendet, um den DSCP-Wert zu identifizieren, der basierend auf dem CO-Wert festgelegt wird. Diese Karten sind in dieser Tabelle weiter oben im Dokument aufgeführt. Alternativ kann der Administrator eine eindeutige Karte einrichten. Ein Beispiel hierfür ist unten dargestellt.

```
Console> (enable) set qos cos-dscp-map 20 30 1 43 63 12 13 8
!-- QoS cos-dscp-map set successfully. Console> (enable)
```

Der obige Befehl legt die folgende Zuordnung fest:

COs	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Obwohl es sehr unwahrscheinlich ist, dass die obige Karte in einem realen Netzwerk verwendet wird, dient sie dazu, eine Vorstellung davon zu geben, was mit diesem Befehl erreicht werden kann.

IP Precedence to DSCP Mapping (CatOS)

Ähnlich wie bei der DSCP-Zuordnung von COs kann auch ein Frame einen DSCP-Wert haben, der anhand der Einstellung für die IP-Rangfolge eingehender Pakete bestimmt wird. Dies tritt nur dann auf, wenn der Port vom Administrator als vertrauenswürdig festgelegt wurde und das Schlüsselwort trust-ipprec verwendet wurde.

Wenn QoS aktiviert ist, erstellt der Switch eine Standardzuordnung. Auf diese Karte wird in dieser

Tabelle weiter oben in diesem Dokument verwiesen. Diese Zuordnung wird verwendet, um den DSCP-Wert zu identifizieren, der basierend auf dem IP-Rangfolgewert festgelegt wird. Alternativ kann der Administrator eine eindeutige Karte einrichten. Ein Beispiel hierfür ist unten aufgeführt:

```
Console> (enable) set qos ipprec-dscp-map 20 30 1 43 63 12 13 8
!-- QoS ipprec-dscp-map set successfully. Console> (enable)
```

Der obige Befehl legt die folgende Zuordnung fest:

IP-Rangfolge	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Obwohl es sehr unwahrscheinlich ist, dass die obige Karte in einem realen Netzwerk verwendet wird, dient sie dazu, eine Vorstellung davon zu geben, was mit diesem Befehl erreicht werden kann.

Klassifizierung (CatOS)

Wenn ein Frame zur Verarbeitung an die PFC übergeben wird, wird der Klassifizierungsprozess für den Frame durchgeführt. Die PFC verwendet eine vorkonfigurierte ACL (oder eine Standard-ACL), um dem Frame ein DSCP zuzuweisen. Innerhalb des ACE wird eines von vier Schlüsselwörtern verwendet, um einen DSCP-Wert zuzuweisen. Sie sind wie folgt:

1. TRUST-DSCP (nur IP-Zugriffskontrolllisten)
2. TRUST-IPPREC (nur IP ACL'=s)
3. TRUST-COS (alle ACLs außer IPX und MAC auf einem PFC2)
4. DSCP

Das Schlüsselwort TRUST-DSCP geht davon aus, dass für den im PFC ankommenden Frame bereits ein DSCP-Wert festgelegt wurde, bevor er in den Switch eingegeben wird. Der Switch behält diesen DSCP-Wert bei.

Bei TRUST-IPPREC leitet die PFC einen DSCP-Wert vom vorhandenen IP-Rangfolgewert ab, der im ToS-Feld vorhanden ist. Die PFC verwendet die IP-Rangfolge für DSCP-Zuordnungen, um das richtige DSCP zuzuweisen. Eine Standardzuordnung wird erstellt, wenn QoS auf dem Switch aktiviert ist. Alternativ kann eine vom Administrator erstellte Zuordnung verwendet werden, um den DSCP-Wert abzuleiten.

Ähnlich wie TRUST-IPPREC weist das Schlüsselwort TRUS-COS die PFC an, einen DSCP-Wert von den COs im Frame-Header abzuleiten. Es gibt auch eine "COs to DSCP"-Zuordnung (entweder eine standardmäßige Zuordnung eines Administrator, dem eine zugewiesen wurde), um die PFC bei der Ableitung des DSCP zu unterstützen.

Das DSCP-Schlüsselwort wird verwendet, wenn ein Frame von einem nicht vertrauenswürdigen Port eintrifft. Dies stellt eine interessante Situation für die Ableitung des DSCP dar. An diesem Punkt wird das in der set qos acl-Anweisung konfigurierte DSCP zum Ableiten des DSCP verwendet. An diesem Punkt können die ACLs jedoch verwendet werden, um ein DSCP für Datenverkehr basierend auf den im ACE festgelegten Klassifizierungskriterien abzuleiten. Das bedeutet, dass in einem ACE Klassifizierungskriterien wie IP-Quell- und Zieladresse, TCP/UDP-Portnummern, ICMP-Codes, IGMP-Typ, IPX-Netzwerk- und Protokollnummern, MAC-Quell- und -Zieladressen und Ethertypes (nur für Nicht-IP- und Nicht-IPX-Datenverkehr) zur Identifizierung des Datenverkehrs verwendet werden können. Dies bedeutet, dass ein ACE so konfiguriert werden könnte, dass er einen bestimmten DSCP-Wert zuweist, d. h. HTTP-Datenverkehr über FTP-Datenverkehr.

Betrachten Sie das folgende Beispiel:

```
Console> (enable) set port qos 3/5 trust untrusted
```

Wenn Sie einen Port als nicht vertrauenswürdig festlegen, wird der PFC angewiesen, einen ACE zu verwenden, um das DSCP für den Frame abzuleiten. Wenn der ACE mit Klassifizierungskriterien konfiguriert ist, können einzelne Datenflüsse von diesem Port mit unterschiedlichen Prioritäten klassifiziert werden. Die folgenden Aussagen veranschaulichen dies:

```
Console> (enable) set qos acl ip abc dscp 32 tcp any any eq http
Console> (enable) set qos acl ip ABC dscp 16 tcp any any eq ftp
```

In diesem Beispiel gibt es zwei ACE-Anweisungen. Die erste identifiziert alle TCP-Datenflüsse (das Schlüsselwort any wird zur Identifizierung des Quell- und Zieldatenverkehrs verwendet), deren Portnummer 80 (80 = HTTP) lautet und denen ein DSCP-Wert von 32 zugewiesen wird. Der zweite ACE identifiziert Datenverkehr, der von einem beliebigen Host stammt und für jeden Host bestimmt ist, dessen TCP-Portnummer 21 (FTP) lautet und dem ein DSCP-Wert von 16 zugewiesen wird.

Konfiguration der Klassifizierung auf der Catalyst 6000-Familie mit integriertem Cisco IOS (nativer Modus)

Im folgenden Abschnitt werden die QoS-Konfigurationskomponenten beschrieben, die zur Unterstützung der Klassifizierung auf der PFC mithilfe des integrierten Cisco IOS (Native Mode) verwendet werden.

COs zu DSCP-Zuordnung (integriertes Cisco IOS (nativer Modus))

Beim Eingang zum Switch wird für einen Frame ein DSCP-Wert vom Switch festgelegt. Wenn sich der Port in einem vertrauenswürdigen Zustand befindet und der Administrator das Schlüsselwort mls qos trust-COs verwendet hat (auf GE-Ports oder 10/100-Ports auf den WS-X6548-Linecards), wird der im Frame festgelegte CO-Wert zur Bestimmung des DSCP-Werts für den Frame verwendet. Wie bereits erwähnt, kann der Switch dem Frame während der Switch-Übertragung Servicelevel zuweisen, basierend auf dem internen DSCP-Wert.

Wenn QoS aktiviert ist, erstellt der Switch eine Standardzuordnung. In dieser Tabelle finden Sie die Standardeinstellungen. Diese Zuordnung wird verwendet, um den DSCP-Wert zu identifizieren, der basierend auf dem CO-Wert festgelegt wird. Alternativ kann der Administrator eine eindeutige Karte einrichten. Ein Beispiel hierfür ist unten dargestellt.

```
Cat6500(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

Der obige Befehl legt die folgende Zuordnung fest:

COs	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Obwohl es sehr unwahrscheinlich ist, dass die obige Karte in einem realen Netzwerk verwendet

wird, dient sie dazu, eine Vorstellung davon zu geben, was mit diesem Befehl erreicht werden kann.

IP-Rangfolge zu DSCP-Zuordnung (integriertes Cisco IOS (nativer Modus))

Ähnlich wie bei der DSCP-Zuordnung von COs kann auch ein Frame einen DSCP-Wert haben, der anhand der Einstellung für die IP-Rangfolge eingehender Pakete bestimmt wird. Dies tritt nur dann auf, wenn der Port vom Administrator als vertrauenswürdig festgelegt wurde und das Schlüsselwort mls qos trust-ipprec verwendet wurde. Dieses Schlüsselwort wird nur auf GE-Ports und 10/100-Ports auf den WS-X6548-Linecards unterstützt. Für 10/100-Ports der WS-X6348- und WS-X6248-Linecards sollten Zugriffskontrolllisten verwendet werden, um eingehenden Daten ip-Precedence-Vertrauenswürdigkeit zuzuweisen.

Wenn QoS aktiviert ist, erstellt der Switch eine Standardzuordnung. In dieser Tabelle finden Sie die Standardeinstellungen. Diese Zuordnung wird verwendet, um den DSCP-Wert zu identifizieren, der basierend auf dem IP-Rangfolgewert festgelegt wird. Alternativ kann der Administrator eine eindeutige Karte einrichten. Ein Beispiel hierfür ist unten dargestellt.

```
Cat6500(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Cat6500(config)#
```

Der obige Befehl legt die folgende Zuordnung fest:

IP-Rangfolge	0	1	2	3	4	5	6	7
DSCP	20	30	1	43	63	12	13	8

Obwohl es sehr unwahrscheinlich ist, dass die obige Karte in einem realen Netzwerk verwendet wird, dient sie dazu, eine Vorstellung davon zu geben, was mit diesem Befehl erreicht werden kann.

Klassifizierung (integriertes Cisco IOS (nativer Modus))

Wenn ein Frame an die PFC übergeben wird, kann der Klassifizierungsprozess durchgeführt werden, um einem eingehenden Frame eine neue Priorität zuzuweisen. Der Nachteil hierbei ist, dass dies nur möglich ist, wenn der Frame von einem nicht vertrauenswürdigen Port stammt oder der Frame als nicht vertrauenswürdig eingestuft wurde.

Mit einer Richtlinienzuordnungsklassenaktion können Sie:

1. TRUST COs
2. TRUST IP PRECEDENCE
3. TRUST DSCP
4. KEIN VERTRAUEN

Das Schlüsselwort TRUST DSCP geht davon aus, dass für den in die PFC eingehenden Frame bereits ein DSCP-Wert festgelegt wurde, bevor er in den Switch eingegeben wird. Der Switch behält diesen DSCP-Wert bei.

Bei TRUST IP-PRECEDENCE leitet die PFC einen DSCP-Wert vom vorhandenen IP-Rangfolgewert ab, der im ToS-Feld vorhanden ist. Die PFC verwendet eine IP-Priorität für die DSCP-Zuordnung, um das richtige DSCP zuzuweisen. Eine Standardzuordnung wird erstellt, wenn QoS auf dem Switch aktiviert ist. Alternativ kann eine vom Administrator erstellte Zuordnung verwendet werden, um den DSCP-Wert abzuleiten.

Ähnlich wie TRUST IP-PRECEDENCE weist das Schlüsselwort TRUST COs den PFC an, einen DSCP-Wert von den COs im Frame-Header abzuleiten. Es gibt auch eine "COs to DSCP"-Zuordnung (entweder eine standardmäßige Zuordnung eines Administrator, dem eine zugewiesen wurde), um die PFC bei der Ableitung des DSCP zu unterstützen.

Ein Beispiel für die Ableitung von DSCP von einer bestehenden Priorität (DSCP, IP-Rangfolge oder COs) ist unten dargestellt.

```
Cat6500(config)# policy-map assign-dscp-value
Cat6500(config-pmap)# class test
Cat6500(config-pmap-c)# trust COs
Cat6500(config-pmap-c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

Die obige Klassenzuordnung leitet den DSCP-Wert von den COs im Ethernet-Header ab.

Das Schlüsselwort NO TRUST wird verwendet, wenn ein Frame von einem nicht vertrauenswürdigen Port eintrifft. Dadurch kann dem Frame während des Richtlinienprozesses ein DSCP-Wert zugewiesen werden.

Im folgenden Beispiel wird veranschaulicht, wie verschiedene, in die PFC eingehende Flows mit der folgenden Richtliniendefinition eine neue Priorität (DSCP) zugewiesen werden können.

```
Cat6500(config)# access-list 102 permit tcp any any eq http
Cat6500(config)# policy-map new-dscp-for-flow
Cat6500(config-pmap)# class test access-group 102
Cat6500(config-pmap-c)# no trust
Cat6500(config-pmap-c)# police 1000 1 confirm-action set-dscp-transmit 24  Cat6500(config-pmap-
c)# exit
Cat6500(config-pmap)# exit
Cat6500(config)#
```

Das obige Beispiel zeigt Folgendes:

1. Eine ACL wird erstellt, um HTTP-Flüsse zu identifizieren, die in den Port gelangen.
2. Eine Richtlinienzuordnung mit dem Namen new-dscp-for-flow.
3. Eine Klassenzuordnung (Namenstest), die die Zugriffsliste 102 verwendet, um den Datenverkehr zu identifizieren, für den diese Klassenzuordnung ihre Aktion ausführt.
4. Der Klassenzuordnungstest legt den Vertrauensstatus für den eingehenden Frame auf nicht vertrauenswürdig fest und weist diesem Fluss ein DSCP von 24 zu.
5. Diese Klassenzuordnung beschränkt auch die Summe aller HTTP-Datenflüsse auf maximal 1 MB.

Common Open Policy Server (COPS)

COPS ist ein Protokoll, das es der Catalyst 6000-Familie ermöglicht, QoS von einem Remote-Host zu konfigurieren. COPS wird derzeit nur von CatOS unterstützt und ist Teil der intserv-Architektur für QoS. COPS wird zum Zeitpunkt der Verwendung des integrierten Cisco IOS (Nativer Modus) derzeit nicht unterstützt (zum Zeitpunkt der Veröffentlichung dieses Dokuments). Während das COPS-Protokoll die QoS-Konfigurationsinformationen an den Switch überträgt, ist es nicht die

Quelle der QoS-Konfigurationsinformationen. Für die Verwendung des COPS-Protokolls ist ein externer QoS-Manager erforderlich, der die QoS-Konfigurationen für den Switch hostet. Der externe QoS-Manager initiiert den Abwärtsdruck dieser Konfigurationen auf den Switch mithilfe des COPS-Protokolls. Der QoS Policy Manager (QPM) von Cisco ist ein Beispiel für einen externen QoS-Manager.

In diesem Dokument wird nicht die Funktionsweise von QPM erläutert, sondern die Konfiguration, die für die Unterstützung externer QoS-Konfigurationen bei der Verwendung von QPM erforderlich ist.

COPS-Konfiguration

Standardmäßig ist die COPS-Unterstützung deaktiviert. Um COPS auf dem Switch zu verwenden, muss dieser aktiviert sein. Dies kann mithilfe des folgenden Befehls erreicht werden:

```
Console> (enable) set qos policy-source cops
!-- QoS policy source for the switch set to COPS. Console> (enable)
```

Wenn dieser Befehl initiiert wird, werden bestimmte standardmäßige QoS-Konfigurationswerte vom COPS-Server bezogen. Dazu gehören:

1. Zuordnungen von COs in Warteschlangen
2. Grenzwertzuweisungen für Eingangs- und Ausgangswarteschlangen
3. WRR-Bandbreitenzuweisungen
4. Alle Aggregations- und Mikroflow-Richtlinien
5. Karten von DSCP zu COs für ausgehenden Datenverkehr
6. ACLs
7. CO-Standardzuweisungen für Ports

Wenn QoS-Konfigurationen mit COPS durchgeführt werden, ist es wichtig zu verstehen, dass die Anwendung dieser Konfigurationen auf eine andere Weise angewendet wird. Anstatt die Ports direkt zu konfigurieren, wird COPS zum Konfigurieren des Port-ASIC verwendet. Der Port-ASIC steuert in der Regel eine Gruppe von Ports. Daher wird die COPS-Konfiguration auf mehrere Ports gleichzeitig angewendet.

Der konfigurierte Port-ASIC ist der GE ASIC. Auf GE-Linecards gibt es vier Ports pro GE (Ports 1-4, 5-8, 9-12, 13-16). Auf diesen Linecards wirkt sich die COPS-Konfiguration auf jede Port-Gruppe aus. Auf 10/100-Linecards (wie in diesem Whitepaper bereits erläutert) gibt es zwei ASIC-Gruppen: GE und 10/100 ASICs. Ein GE-ASIC ist für vier 10/100-ASICs vorhanden. Jeder 10/100-ASIC unterstützt 12 10/100-Ports. COPS konfiguriert die GE ASIC. Wenn also die QoS-Konfiguration über COPS auf 10/100 Line Cards angewendet wird, gilt die Konfiguration für alle 48 10/100-Ports.

Bei Aktivierung der COPS-Unterstützung durch Ausgabe des Befehls **set qos policy-source cops** wird die QoS-Konfiguration über COPS auf alle ASICs im Switch-Chassis angewendet. Es ist möglich, die COPS-Konfiguration auf bestimmte ASICs anzuwenden. Dies kann mit dem folgenden Befehl erreicht werden:

```
Console> (enable) set port qos 5/4 policy-source cops
!-- QoS policy source set to COPS for port (s) 5/1-4. Console> (enable)
```

Aus der Anwendung des obigen Befehls geht hervor, dass dieser Befehl auf einem GE-Modul

ausgeführt wurde, da vier Ports vom Befehl betroffen waren.

Richtlinienentscheidungspunktserver und Domänennamen

Richtlinienentscheidungspunktserver (PDPS) sind die externen Richtlinienmanager, die zum Speichern von QoS-Konfigurationsdetails verwendet werden, die auf den Switch übertragen werden. Wenn COPS auf dem Switch aktiviert ist, muss der Switch mit der IP-Adresse des externen Managers konfiguriert werden, der dem Switch QoS-Konfigurationsdetails bereitstellt. Dies ähnelt dem Zeitpunkt, an dem SNMP aktiviert und die IP-Adresse des SNMP-Managers definiert ist.

Der Befehl zum Identifizieren der externen PDPS wird wie folgt ausgeführt:

```
Console> (enable) set cops server 192.168.1.1 primary
!-- 192.168.1.1 is added to the COPS diff-serv server table as primary server. !-- 192.168.1.1
is added to the COPS rsvp server table as primary server. Console> (enable)
```

Der obige Befehl identifiziert das Gerät 192.168.1.1 als primären Entscheidungspunktserver.

Wenn der Switch mit dem PDPS kommuniziert, muss er Teil einer auf dem PDPS definierten Domäne sein. Der PDPS kommuniziert nur mit Switches, die Teil seiner definierten Domäne sind. Daher muss der Switch so konfiguriert werden, dass er die COPS-Domäne identifiziert, zu der er gehört. Dazu wird der folgende Befehl ausgegeben:

```
Console> (enable) set cops domain name remote-cat6k
!-- Domain name set to remote-cat6k. Console> (enable)
```

Der obige Befehl zeigt, dass der Switch als Teil der Domäne mit dem Namen remote-cat6k konfiguriert wurde. Diese Domäne sollte in QPM definiert werden, und der Switch muss dieser Domäne hinzugefügt werden.

Zugehörige Informationen

- Produkt-Support für Switches
- Support für LAN-Switching-Technologie
- Technischer Support und Dokumentation für Cisco Systeme
