

# Häufig gestellte Fragen zu Catalyst 6500/6000 QoS

## Inhalt

### [Einführung](#)

[Ist QoS auf Catalyst Switches der Serie 6500 standardmäßig aktiviert?](#)

[Welcher standardmäßige DSCP-Wert \(Differentiated Services Code Point\) wird Paketen zugewiesen?](#)

[Kann ich VLAN-basierte QoS auf einem 6500 einrichten?](#)

[Welche Portfunktionen stehen für jede Linecard zur Verfügung, und wie kann ich die Funktionen für die Warteschlange interpretieren?](#)

[Wie lauten die QoS-Standardkonfigurationen für einen 6500, wenn QoS anfänglich aktiviert ist?](#)

[Wo werden die einzelnen QoS-Prozesse beim Catalyst 6000 durchgeführt?](#)

[Kann ich QoS-Funktionen ohne Policy Feature Card \(PFC\) implementieren?](#)

[Worin besteht der Unterschied in der QoS-Funktionalität zwischen der Policy Feature Card 1 \(PFC1\) und PFC2?](#)

[Welche CoS-Standardklasse \(Class of Service\) dient zum Übertragen von Warteschlangenzuordnungskonfigurationen, wenn Auto-QoS aktiviert ist?](#)

[Wie lautet die standardmäßige Zuordnung von Differentiated Services Code Point \(DSCP\) und Class of Service \(CoS\)?](#)

[Wird bei der Ausgangswarteschlange, wenn die Warteschlange mit höchster Priorität gesättigt ist, der Datenverkehr schließlich in den Warteschlangen mit gewichtetem Round-Robin \(WRR\) weitergeleitet?](#)

[Legt ein gewichteter Round-Robin \(WRR\) die Bandbreitenzuweisung basierend auf der Anzahl der Pakete oder einer bestimmten Anzahl von Byte fest?](#)

[Meine neue 65xx Line Card-Dokumentation sagt, dass sie Deficit Weighted Round-Robin \(DWRR\) unterstützt. Was ist DWRR und was bedeutet es?](#)

[Welche Standardgewichte gelten für einen 2q2t-Port, und wie kann ich diese ändern?](#)

[Ich möchte das Simple Network Management Protocol \(SNMP\) verwenden, um die Anzahl der verworfenen Pakete nach einzelnen Policers zu erfassen. Ist das möglich? Wenn ja, welche MIB wird verwendet?](#)

[Gibt es einen Befehl show, der die Anzahl der verworfenen Pakete nach Policer anzeigt?](#)

[Ich möchte das Simple Network Management Protocol \(SNMP\) verwenden, um einen Policer so zu ändern, dass die Rate- und Burst-Parameter dynamisch geändert werden können. Zum Beispiel nach Tageszeit. Ist das möglich? Wenn ja, welche MIB wird verwendet?](#)

[Ist es möglich, eine zeitbasierte QoS \(insbesondere zur Änderung der maximalen und Burst-Rate\) mithilfe der Cisco IOS-Software auf der Multilayer Switch Feature Card \(MSFC\) im Hybridmodus zu implementieren? Ist diese QoS, wenn möglich, in der Hardware erfolgt und nicht vom MSFC-Prozessor?](#)

[Ich habe keine Beschreibung der Implementierung der Policer-Rate und der Policer-Burst-Werte erhalten. Ich möchte technische Dokumentation zu diesen Themen erstellen, damit ich die Auswirkungen auf mein Netzwerk verstehen kann.](#)

Ich habe vor, meine Sup1A-Supervisoren durch Sup2s zu ersetzen. Ändern sich die Mechanismen von QoS, z. B. die Burst-Rate, zwischen Sup1A und Sup2?

Welche Befehle kann ich verwenden, um meine QoS-Einstellungen zu überwachen?

Gibt es beim Ausführen des Catalyst-Betriebssystemcodes (CatOS) auf einem 6500 und der Cisco IOS-Software auf der Multilayer Switch Feature Card (MSFC) QoS-Befehle auf der MSFC oder dem Supervisor?

Was passiert, wenn der Befehl **set port qos trust** nicht von meiner Linecard unterstützt wird?

Was ist der Unterschied zwischen Aggregat- und Mikroflow-Überwachung?

Mit welchen Befehlen kann ich Statistiken zu Aggregat- oder Mikroflow-Policern anzeigen?

Wird Traffic Shaping auf dem Catalyst Switch der Serie 6500 (Cat6K) unterstützt?

Wie viele Aggregat- oder Mikroflow-Policer werden auf dem Catalyst 6500 (Cat6K)-Switch unterstützt?

Welches Catalyst-Betriebssystem (CatOS) oder Multilayer Switch Feature Card (MSFC) Cisco IOS-Image ist zur Unterstützung der Richtlinienvergabe erforderlich?

Ich habe ein Upgrade von Sup2 auf Sup720 durchgeführt, und meine Statistiken zur Datenverkehrsrate für Richtlinien werden bei gleichem Datenverkehr unterschiedlich angezeigt. Warum?

Woher weiß ich, welche Werte für die Rate und für Burst verwendet werden, wenn ich einen Policer konfiguriere?

Ich konfiguriere QoS über einen Port-Channel. Gibt es irgendwelche Einschränkungen, die ich kennen muss?

Warum kann ich den Schwellenwert nicht anpassen?

Ich habe Schwierigkeiten, die Puffer für die Übertragungs-Warteschlange anzupassen. Gibt es irgendwelche Einschränkungen?

Ich habe eine 62xx/63xx Line Card. Ich kann den Befehl **set** nicht anwenden, der Differentiated Services Code Point (DSCP) auf einem Port vertraut. Besteht auf dieser Linecard eine Einschränkung für QoS-Funktionen?

Welche Catalyst-Betriebssystemversionen (CatOS) und Supervisoren sind zur Unterstützung der Richtlinienvergabe erforderlich?

Was muss ich über die Konfiguration von QoS über EtherChannel wissen?

Wo finde ich Beispiele für die Verwendung von QoS-Zugriffskontrolllisten (ACLs) zur Markierung oder Überwachung von Datenverkehr?

Worin besteht der Unterschied zwischen portbasierten und VLAN-basierten QoS-Zugriffskontrolllisten (ACLs)?

Wie hoch ist der typische Wert der Burst-Größe für die Ratenbegrenzung auf Layer-3-Switches?

Warum erhalte ich eine geringere Leistung für TCP-Datenverkehr mit Ratenbegrenzung?

Welchen Vorteil bietet Weighted Random Early Detection (WRED), und wie kann ich feststellen, ob meine Linecard WRED unterstützen kann?

Was ist der interne Differentiated Services Code Point (DSCP)?

Welche Quellen stehen für den internen Differentiated Services Code Point (DSCP) zur Verfügung?

Wie wird der interne Differentiated Services Code Point (DSCP) gewählt?

Wird klassenbasiertes Weighted Fair Queuing (CBWFQ) oder Low Latency Queuing (LLQ) im Catalyst 6500 (Cat6K)-Switch unterstützt?

Wird der CoS-Wert (Class of Service) für geroutete Pakete beibehalten?

Wenden QoS die gleiche Konfiguration auf alle LAN-Ports an, die über denselben ASIC gesteuert werden?

Warum zeigt der Befehl **show traffic-shape statistics** kein positives Ergebnis an, selbst wenn die

[Datenverkehrsflutung konfiguriert ist?](#)

[Unterstützt der Catalyst 6500 PFC alle QoS-Standardbefehle?](#)

[Warum sind die Software-CoPP-Zähler größer als die Hardware-CoPP-Zähler?](#)

[Funktioniert die QoS-Standardkonfiguration \(Schnittstelle\) für andere Schnittstellen/Ports?](#)

[Kann ich QoS in einer Schnittstelle mit sekundärer IP-Adresse konfigurieren?](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument werden häufig gestellte Fragen (FAQs) zur Quality of Service (QoS)-Funktion des Catalyst 6500/6000 mit Supervisor 1 (Sup1), Supervisor 1A (Sup1A), Supervisor 2 (Sup2) und Supervisor 720 (Sup720) beantwortet, auf denen Catalyst OS ausgeführt wird. atOS). In diesem Dokument werden diese Switches als Catalyst 6500-Switches (Cat6K) bezeichnet, die CatOS ausführen. Informationen zur [Konfiguration der PFC QoS](#) für QoS-Funktionen auf Catalyst 6500/6000-Switches, auf denen die Cisco IOS®-Software ausgeführt wird, finden Sie unter Konfigurieren der Cisco IOS®-Funktionen.

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

### F. Ist QoS auf Catalyst Switches der Serie 6500 standardmäßig aktiviert?

**Antwort:** QoS ist standardmäßig nicht aktiviert. Geben Sie den Befehl `set qos enable` ein, um QoS zu aktivieren.

### F. Welcher standardmäßige DSCP-Wert (Differentiated Services Code Point) wird Paketen zugewiesen?

**Antwort:** Der gesamte Datenverkehr, der an einen nicht vertrauenswürdigen Port geleitet wird, wird mit dem DSCP 0 markiert. DSCP wird durch den Ausgangsport erneut auf 0 markiert.

### F. Kann ich VLAN-basierte QoS auf einem 6500 einrichten?

**Antwort:** Die Standardeinstellung ist portbasiert. Sie können dies ändern, wenn Sie den Befehl `set port qos mod/port vlan-basiert` ausgeben.

### F. Welche Portfunktionen stehen für jede Linecard zur Verfügung, und wie kann ich die Funktionen für die Warteschlange interpretieren?

**Antwort:** In der Tabelle mit den Portfunktionen unter [Understanding the Queueing Capability of a Port](#) section of [QoS Output Scheduling on Catalyst 6500/6000 Series Switches Running CatOS System Software](#) finden Sie Informationen [zur Warteschlangenfähigkeit von](#) Ports.

### F. Wie lauten die QoS-Standardkonfigurationen für einen 6500, wenn QoS anfänglich aktiviert ist?

**Antwort:** Informationen zur [Standardkonfiguration für QoS auf Catalyst 6000-Switches der Serie Catalyst 6500/6000 mit CatOS-Systemsoftware](#) finden Sie im Abschnitt [QoS-Ausgabeplanung](#).

## F. Wo werden die einzelnen QoS-Prozesse beim Catalyst 6000 durchgeführt?

**Antwort:** Input Scheduling (Eingabeplanung) - erfolgt über PINACLE/COIL Port Application-Specific Integrated Circuits (ASICs). Nur Layer 2 mit oder ohne Policy Feature Card (PFC).

Klassifizierung - erfolgt durch Supervisor oder PFC über die ACL-Engine (Access Control List). Nur Layer 2 ohne PFC; Layer 2 oder Layer 3 mit PFC.

Policing (Richtlinienvergabe) - durch PFC über die Layer-3-Weiterleitungs-Engine durchgeführt. Layer 2 oder Layer 3 mit PFC (erforderlich)

Packet Re-Write (Paket neu schreiben): Fertig durch PINNACLE-/COIL-Port-ASICs. Layer 2 oder Layer 3 basierend auf der zuvor erfolgten Klassifizierung.

Ausgabeplanung - erfolgt über PINACLE/COIL-Port-ASICs. Layer 2 oder Layer 3 basierend auf der zuvor erfolgten Klassifizierung.

## F. Kann ich QoS-Funktionen ohne Policy Feature Card (PFC) implementieren?

**Antwort:** Bei Catalyst Switches der Serie 6000 befindet sich das Kernstück der QoS-Funktionalität auf der PFC und ist Voraussetzung für die Layer-3- oder Layer-4-QoS-Verarbeitung. Ein Supervisor ohne PFC kann jedoch für die Layer-2-QoS-Klassifizierung und -Kennzeichnung verwendet werden.

## F. Worin besteht der Unterschied in der QoS-Funktionalität zwischen der Policy Feature Card 1 (PFC1) und PFC2?

**Antwort:** Mit PFC2 können Sie die QoS-Richtlinie auf eine Distributed Forwarding Card (DFC) drücken. PFC2 bietet außerdem Unterstützung für einen Überhang, was eine zweite Ebene der Richtlinienvergabe angibt, auf der Richtlinienaktionen durchgeführt werden können. Weitere Informationen finden Sie im Abschnitt [Hardwaresupport für QoS in der Catalyst 6000-Produktfamilie Quality of Service für Catalyst Switches der Serie 600](#).

## F. Welche CoS-Standardklasse (Class of Service) dient zum Übertragen von Warteschlangenzuordnungskonfigurationen, wenn Auto-QoS aktiviert ist?

**Antwort:** set qos map 2q2t tx queue 2 2 cos 5,6,7

set qos map 2q2t tx queue 2 1 cos 1,2,3,4

set qos map 2q2t tx queue 1 1 cos 0

## F. Wie lautet die standardmäßige Zuordnung von Differentiated Services Code Point (DSCP) und Class of Service (CoS)?

**Antwort:** 8 bis 1 (Dividieren Sie DSCP durch 8, um CoS zu erhalten).

## F. Wird bei der Ausgangswarteschlange, wenn die Warteschlange mit höchster Priorität gesättigt ist, der Datenverkehr schließlich in den Warteschlangen mit

## **gewichtetem Round-Robin (WRR) weitergeleitet?**

**Antwort:** Nein, die WRR-Warteschlangen werden erst dann bereitgestellt, wenn die Prioritätswarteschlange vollständig leer ist.

## **F. Legt ein gewichteter Round-Robin (WRR) die Bandbreitenzuweisung basierend auf der Anzahl der Pakete oder einer bestimmten Anzahl von Byte fest?**

**Antwort:** Basierend auf einer bestimmten Anzahl von Bytes, die mehr als ein Paket darstellen können. Das letzte Paket, das die zugewiesenen Bytes überschreitet, wird nicht gesendet. Bei einer Konfiguration mit extrem hohem Gewicht, z. B. 1 % für die Warteschlange 1 und 99 % für die Warteschlange 2, wird das exakte konfigurierte Gewicht möglicherweise nicht erreicht. Der Switch verwendet einen WRR-Algorithmus, um Frames jeweils aus einer Warteschlange zu übertragen. WRR verwendet einen Gewichtungswert, um festzulegen, wie viel von einer Warteschlange übertragen werden soll, bevor sie zur anderen Warteschlange wechselt. Je höher das Gewicht, das einer Warteschlange zugewiesen wird, desto mehr Bandbreite wird ihr zugewiesen.

**Hinweis:** Die tatsächliche Anzahl der übertragenen Bytes stimmt nicht mit der Berechnung überein, da ganze Frames übertragen werden, bevor sie zur anderen Warteschlange wechselt.

## **F. Meine neue 65xx Line Card-Dokumentation sagt, dass sie Deficit Weighted Round-Robin (DWRR) unterstützt. Was ist DWRR und was bedeutet es?**

**Antwort:** DWRR überträgt aus den Warteschlangen, ohne die Warteschlange mit niedriger Priorität zu verlieren, da es die untergeordnete Übertragung von Warteschlangen mit niedriger Priorität verfolgt und sie in der nächsten Runde kompensiert. Wenn eine Warteschlange ein Paket nicht senden kann, weil die Paketgröße größer als die verfügbaren Bytes ist, werden die nicht verwendeten Bytes der nächsten Runde gutgeschrieben.

## **F. Welche Standardgewichte gelten für einen 2q2t-Port, und wie kann ich diese ändern?**

**Antwort:** Geben Sie den Befehl `set qos wrr 2q2t q1_weight q2_weight` ein, um die Standardgewichte für Warteschlange 1 (die Warteschlange mit niedriger Priorität dient 5/260. Zeit) und Warteschlange 2 (die Warteschlange mit hoher Priorität dient 255/260. Zeit) zu ändern.

## **F. Ich möchte das Simple Network Management Protocol (SNMP) verwenden, um die Anzahl der verworfenen Pakete nach einzelnen Policers zu erfassen. Ist das möglich? Wenn ja, welche MIB wird verwendet?**

**Antwort:** Ja, SNMP unterstützt CISCO-QOS-PIB-MIB und CISCO-CAR-MIB.

## **F. Gibt es einen Befehl show, der die Anzahl der verworfenen Pakete nach Policer anzeigt?**

**Antwort:** Die Befehle `show qos statistics aggregate-policer` und `show qos statistics l3stats` zeigen die Anzahl der verworfenen Pakete nach Policer an.

## **F. Ich möchte das Simple Network Management Protocol (SNMP) verwenden, um**

einen Policer so zu ändern, dass die Rate- und Burst-Parameter dynamisch geändert werden können. Zum Beispiel nach Tageszeit. Ist das möglich? Wenn ja, welche MIB wird verwendet?

Antwort: Ja, SNMP unterstützt CISCO-QOS-PIB-MIB und CISCO-CAR-MIB.

F. Ist es möglich, eine zeitbasierte QoS (insbesondere zur Änderung der maximalen und Burst-Rate) mithilfe der Cisco IOS-Software auf der Multilayer Switch Feature Card (MSFC) im Hybridmodus zu implementieren? Ist diese QoS, wenn möglich, in der Hardware erfolgt und nicht vom MSFC-Prozessor?

Antwort: Nein, das kann nicht getan werden. Im Hybrid-Modus (CatOS) erfolgt die gesamte QoS-Richtlinienvergabe durch den Supervisor.

F. Ich habe keine Beschreibung der Implementierung der Policer-Rate und der Policer-Burst-Werte erhalten. Ich möchte technische Dokumentation zu diesen Themen erstellen, damit ich die Auswirkungen auf mein Netzwerk verstehen kann.

Antwort: Die Policer-Rate und die Burst-Werte für Policer werden auf diese Weise implementiert:

$burst = sustained\ rate\ bps \times 0.00025\ (the\ leaky\ bucket\ rate) + MTU\ kbps$

Wenn Sie beispielsweise eine 20-Mbit/s-Überwachung und eine MTU (auf Ethernet) mit maximal 1.500 Byte wünschen, wird der Burst wie folgt berechnet:

$burst = (20,000,000\ bps \times 0.00025) + (1500 \times 0.008\ kbps)$   
 $= 5000\ bps + 12\ kbps$   
 $= 17\ kbps$

Aufgrund der Detailliertheit der Überwachungshardware mit Sup1 und Sup2 müssen Sie diese jedoch auf mindestens 32 Kbit/s aufrunden.

Weitere Informationen zur Policer-Rate und Burst-Werte-Implementierung finden Sie in diesen Dokumenten:

- [QoS-Ausgabeplanung für Catalyst Switches der Serien 6500 und 6000 mit CatOS-Systemsoftware](#)
- [Konfigurieren von QoS](#)

F. Ich habe vor, meine Sup1A-Supervisoren durch Sup2s zu ersetzen. Ändern sich die Mechanismen von QoS, z. B. die Burst-Rate, zwischen Sup1A und Sup2?

Antwort: Ja, es besteht ein Unterschied zwischen zwei Supervisoren, wenn ein Catalyst Switch der Serie 6500 über SUP2/PFC2 verfügt. Wenn Cisco Express Forwarding (CEF) ausgeführt wird, ist das Verhalten beim Konfigurieren des NetFlow in SUP2 etwas anders.

F. Welche Befehle kann ich verwenden, um meine QoS-Einstellungen zu überwachen?



**Antwort:** Informationen zur [QoS-Klassifizierung und -Kennzeichnung](#) von [Catalyst Switches der Serien 6500/6000 mit CatOS-Software](#) finden Sie im Abschnitt [Überwachung und Überprüfung einer Konfiguration](#).

## **F. Gibt es beim Ausführen des Catalyst-Betriebssystemcodes (CatOS) auf einem 6500 und der Cisco IOS-Software auf der Multilayer Switch Feature Card (MSFC) QoS-Befehle auf der MSFC oder dem Supervisor?**

**Antwort:** Beim Ausführen von Hybrid Code (CatOS) geben Sie die QoS-Befehle auf der Supervisor/Policy Feature Card (PFC) aus. Der 6500 führt QoS an drei Stellen aus:

- Softwarebasiert in der MSFC
- Hardwarebasiert (Multilayer-Switching-basiert) im PFC
- Softwarebasiert auf einigen Linecards

Dieses Problem tritt auf, wenn Sie mit Hybrid-IOS (CatOS + IOS für MSFC) arbeiten. CatOS und IOS verfügen über zwei Gruppen von Konfigurationsbefehlen. Wenn Sie jedoch QoS unter nativem IOS konfigurieren, z. B. mit den neueren Sup32- oder Sup720-Engines, sind Sie von der Hardware entfernt, und der Teil der Linecard ist für den Benutzer nicht sichtbar. Dies ist wichtig, da der Großteil des Datenverkehrs Multilayer-Switched (Hardware Switched) ist. Daher wird sie von der PFC-Logik behandelt. Die MSFC sieht diesen Datenverkehr nie. Wenn Sie keine PFC-basierte QoS einrichten, geht der Großteil des Datenverkehrs verloren.

## **F. Was passiert, wenn der Befehl `set port qos trust` nicht von meiner Linecard unterstützt wird?**

**Antwort:** Sie können eine QoS-Zugriffskontrollliste (ACL) erstellen, um dem DSCP-Wert (Differentiated Services Code Point) des eingehenden Pakets zu vertrauen. Führen Sie z. B. den Befehl `set qos acl ip test trust-dscp any` aus.

## **F. Was ist der Unterschied zwischen Aggregat- und Mikroflow-Überwachung?**

**Antwort:** Informationen zur [Klassifizierung und Richtlinienvergabe mit PFC](#) finden Sie im Abschnitt [Quality of Service \(QoS\) für Catalyst Switches der Serie 6000](#).

## **F. Mit welchen Befehlen kann ich Statistiken zu Aggregat- oder Mikroflow-Policern anzeigen?**

**Antwort:** Mit der Supervisor Engine 1 und 1A können keine Policing-Statistiken für einzelne aggregierte Policers erstellt werden. Geben Sie den Befehl `show qos statistics l3stats` aus, um die Statistiken zur systembezogenen Richtlinienvergabe anzuzeigen.

Mit der Supervisor Engine 2 können Sie aggregierte Policing-Statistiken pro Policer anzeigen, indem Sie den Befehl `show qos statistics aggregate-policer` ausführen. Geben Sie den Befehl `show mls entry qos short` ein, um Statistiken zur Mikroflow-Überwachung zu überprüfen.

## **F. Wird Traffic Shaping auf dem Catalyst Switch der Serie 6500 (Cat6K) unterstützt?**

**Antwort:** Traffic Shaping wird nur auf bestimmten WAN-Modulen für die Catalyst 6500/7600-Serie

unterstützt, z. B. die Optical Services Modules (OSMs) und die FlexWAN-Module. Weitere Informationen finden Sie unter [Konfigurieren von Class-Based Traffic Shaping](#) und [Traffic Shaping](#).

## **F. Wie viele Aggregat- oder Mikroflow-Policer werden auf dem Catalyst 6500 (Cat6K)-Switch unterstützt?**

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

## **F. Welches Catalyst-Betriebssystem (CatOS) oder Multilayer Switch Feature Card (MSFC) Cisco IOS-Image ist zur Unterstützung der Richtlinienvergabe erforderlich?**

**Antwort:** Die Supervisor Engine 1A unterstützt die Eingangs-Policing in CatOS Version 5.3(1) und höher sowie in Cisco IOS Software Release 12.0(7)XE und höher.

Die Supervisor Engine 2 unterstützt die Eingangs-Policing in CatOS 6.1(1) und höher sowie in Cisco IOS Software Release 12.1(5c)EX und höher. Microflow-Policing wird jedoch nur in der Cisco IOS-Software unterstützt.

## **F. Ich habe ein Upgrade von Sup2 auf Sup720 durchgeführt, und meine Statistiken zur Datenverkehrsrate für Richtlinien werden bei gleichem Datenverkehr unterschiedlich angezeigt. Warum?**

**Antwort:** Eine wichtige Änderung bei der Richtlinienvergabe für die Supervisor Engine 720 ist, dass sie Datenverkehr nach der Layer-2-Länge des Frames zählen kann. Dies unterscheidet sich von der Supervisor Engine 1 und der Supervisor Engine 2, die IP- und IPX-Frames nach ihrer Layer-3-Länge zählen. Bei einigen Anwendungen ist die Layer-2- und Layer-3-Länge möglicherweise nicht konsistent. Ein Beispiel ist ein kleines Layer-3-Paket in einem großen Layer-2-Frame. In diesem Fall zeigt die Supervisor Engine 720 möglicherweise eine etwas andere überwachte Datenverkehrsrate an als die Supervisor Engine 1 und die Supervisor Engine 2.

## **F. Woher weiß ich, welche Werte für die Rate und für Burst verwendet werden, wenn ich einen Policer konfiguriere?**

**Antwort:** Diese Parameter steuern den Betrieb der Tokenbuchse:

- **Rate** (Übertragungsrate): Definiert, wie viele Token in jedem Intervall entfernt werden. Dadurch wird effektiv die Policing-Rate festgelegt. Der gesamte Datenverkehr unter der Rate wird als "In-Profile" betrachtet.
- **Interval** (Intervall): Definiert, wie oft Token aus dem Eimer entfernt werden. Das Intervall ist auf 0,00025 Sekunden festgelegt, sodass Token 4000 Mal pro Sekunde aus dem Eimer entfernt werden. Das Intervall kann nicht geändert werden.
- **Burst** (Burst): Definiert die maximale Anzahl von Token, die der Eimer gleichzeitig speichern kann. Der Burst sollte mindestens die Durchsatzzeiten des Intervalls betragen, um die angegebene Datenverkehrsrate aufrechtzuerhalten. Ein weiterer Grund ist, dass das Paket mit maximaler Größe in die Eimer passen muss.

Verwenden Sie diese Gleichung, um den Burst-Parameter zu bestimmen:



$Burst = (rate\ bps * 0.00025\ sec/interval) \text{ or } (maximum\ packet\ size\ bits) \text{ [whichever is greater]}$

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

$Burst = (1,000,000\ bps * 0.00025) \text{ or } (1518\ bytes * 8\ bits/byte) = 250 \text{ or } 12144$

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

**Hinweis:** In der Cisco IOS-Software wird die Regelungsrate in Bit pro Sekunde (bps) definiert. Im Catalyst-Betriebssystem (CatOS) ist es in Kbit/s definiert. In der Cisco IOS-Software ist die Burst-Rate zudem in Byte definiert, in CatOS jedoch in Kilobit.

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

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

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

Aus demselben Grund ist es nicht empfehlenswert, die Richtlinienoperation mit verbindungsorientiertem Datenverkehr zu vergleichen. Dies zeigt in der Regel eine geringere Leistung als die Überwachung.

## **F. Ich konfiguriere QoS über einen Port-Channel. Gibt es irgendwelche Einschränkungen, die ich kennen muss?**

**Antwort:** Wenn Sie QoS auf Ports konfigurieren, die Teil eines Port-Channels im Catalyst-Betriebssystem (CatOS) sind, müssen Sie dieselbe Konfiguration auf alle physischen Ports im Port-Channel anwenden. Diese Parameter müssen für alle Ports im Port-Channel übereinstimmen:

- Port-Vertrauenstyp
- Empfangs-Port-Typ (2q2t oder 1p2q2t)
- Porttyp übertragen (1q4t oder 1p1q4t)
- Standard-Port Class of Service (CoS)
- Port-basierte QoS oder VLAN-basierte QoS
- Zugriffskontrollliste (ACL) oder Protokollpaar, das der Port überträgt

## F. Warum kann ich den Schwellenwert nicht anpassen?

**Antwort:** Bei Versionen des Catalyst-Betriebssystems (CatOS) vor 6.2 wird mit dem Befehl Weighted Random Early Detection (WRED) threshold (Weighted Random Early Detection) nur der max. Grenzwert festgelegt, während der min-Schwellenwert fest auf 0 % codiert ist. Dies wird in CatOS 6.2 und höher korrigiert, wodurch die Konfiguration des Min-Schwellenwert-Werts ermöglicht wird. Der Standard-Min-Schwellenwert hängt von der Rangfolge ab. Der Min.-Schwellenwert für die IP-Rangfolge 0 entspricht der Hälfte des maximalen Schwellenwerts. Die Werte für die Präzedenzfälle, die beibehalten werden, liegen zwischen der Hälfte des maximalen Schwellenwerts und der maximalen Schwellenwerte in gleichmäßigen Intervallen.

## F. Ich habe Schwierigkeiten, die Puffer für die Übertragungs-Warteschlange anzupassen. Gibt es irgendwelche Einschränkungen?

**Antwort:** Wenn Sie über drei Warteschlangen (1p2q2t) verfügen, müssen die Warteschlange mit gewichtetem Round-Robin (WRR) mit hoher Priorität und die Warteschlange mit strikter Priorität auf derselben Ebene festgelegt werden.

## F. Ich habe eine 62xx/63xx Line Card. Ich kann den Befehl set nicht anwenden, der Differentiated Services Code Point (DSCP) auf einem Port vertraut. Besteht auf dieser Linecard eine Einschränkung für QoS-Funktionen?

**Antwort:** Ja, da Sie die Befehle `trust-dscp`, `trust-ipprec` oder `trust-cos` auf den Linecards WS-X6248-xx, WS-X6224-xx und WS-X6348-xx nicht ausgeben können. In dieser Situation ist es am einfachsten, alle Ports als nicht vertrauenswürdig zu belassen und die Standardzugriffskontrollliste (ACL) in den Befehl `trust-dscp` zu ändern:

```
set qos enable

set port qos 2/1-16 trust untrusted

set qos acl default-action ip trust-dscp
```

Weitere Informationen finden Sie im [Abschnitt zu den Einschränkungen der Line Cards WS-X6248-xx, WS-X6224-xx und WS-X6348-xx](#) bei [QoS-Klassifizierung und -Kennzeichnung auf Catalyst Switches der Serien 6500/6000 CatOS-Software](#) für zusätzliche Line Card-spezifische Einschränkungen.

## F. Welche Catalyst-Betriebssystemversionen (CatOS) und Supervisoren sind zur Unterstützung der Richtlinienvergabe erforderlich?

**Antwort:** Die Supervisor Engine 1A unterstützt die Eingangs-Policing in CatOS Version 5.3(1) und höher sowie in Cisco IOS Software Release 12.0(7)XE und höher.

**Hinweis:** Für die Regelung mit der Supervisor Engine 1A ist eine Policy Feature Card (PFC)-Tochterkarte erforderlich.

Die Supervisor Engine 2 unterstützt die Eingangs-Policing in CatOS 6.1(1) und höher sowie in Cisco IOS Software Release 12.1(5c)EX und höher. Die Supervisor Engine 2 unterstützt den

Parameter für die Überwachung bei Überschreitungsdaten.

Der Supervisor 720 unterstützt die Eingangs-Policing auf Port- und VLAN-Schnittstellenebene. Weitere Informationen zu den Überwachungsfunktionen finden Sie im Abschnitt [zur Aktualisierung der Richtlinienfunktionen für die Supervisor Engine 720](#) der [QoS-Richtlinienzuweisung für Catalyst Switches der Serien 6500/6000](#).

## F. Was muss ich über die Konfiguration von QoS über EtherChannel wissen?

**Antwort:** Wenn Sie QoS auf einem Port konfigurieren, der Teil eines EtherChannels auf CatOS ist, müssen Sie es immer auf Port-Basis konfigurieren. Außerdem müssen Sie sicherstellen, dass Sie dieselbe QoS-Konfiguration auf alle Ports anwenden, da der EtherChannel nur Ports mit denselben QoS-Konfigurationen bündeln kann. Dies bedeutet, dass Sie die folgenden Parameter konfigurieren müssen:

- Port-Vertrauenstyp
- Empfangs-Port-Typ (2q2t oder 1p2q2t)
- Porttyp übertragen (1q4t oder 1p1q4t)
- Standard-Port Class of Service (CoS)
- Port-basierte QoS oder VLAN-basierte QoS
- Zugriffskontrollliste (ACL) oder Protokollpaar, das der Port überträgt

## F. Wo finde ich Beispiele für die Verwendung von QoS-Zugriffskontrolllisten (ACLs) zur Markierung oder Überwachung von Datenverkehr?

**Antwort:** Weitere Informationen finden Sie in [Fall 1: Markierung im Edge](#)-Abschnitt der [QoS-Klassifizierung und -Kennzeichnung auf Catalyst Switches der Serien 6500/6000 mit CatOS-Software](#) als Beispiel für das Markieren von Datenverkehr.

Im Abschnitt [Konfiguration und Überwachung der Richtlinienvergabe in der CatOS-Software](#) von [QoS-Richtlinien für Catalyst Switches der Serien 6500/600](#) finden Sie ein Beispiel für die Überwachung des Datenverkehrs.

## F. Worin besteht der Unterschied zwischen portbasierten und VLAN-basierten QoS-Zugriffskontrolllisten (ACLs)?

**Antwort:** Jede QoS-ACL kann entweder auf einen Port oder auf ein VLAN angewendet werden. Es muss jedoch ein zusätzlicher Konfigurationsparameter berücksichtigt werden: den ACL-Port-Typ. Ein Port kann für VLAN-basierte oder Port-basierte Verbindungen konfiguriert werden. Es gibt zwei Arten von Konfigurationen:

1. Wenn ein VLAN-basierter Port mit einer angewendeten ACL einem VLAN zugewiesen wird, das ebenfalls über eine angewendete ACL verfügt, hat die VLAN-basierte ACL Vorrang vor der Port-basierten ACL.
2. Wenn einem VLAN, das ebenfalls über eine ACL verfügt, ein Port-basierter Port mit einer angewendeten ACL zugewiesen wird, hat die Port-basierte ACL Vorrang vor der VLAN-basierten ACL.

Weitere Informationen finden Sie unter [Welche der vier möglichen Quellen für internes DSCP wird verwendet?](#) Abschnitt zur [QoS-Klassifizierung und -Kennzeichnung für Catalyst Switches der Serien 6500 und 6000 mit CatOS-Software](#) für weitere Informationen.

## F. Wie hoch ist der typische Wert der Burst-Größe für die Ratenbegrenzung auf Layer-3-Switches?

**Antwort:** Layer-3-Switches implementieren eine Annäherung an den Single-Token-Bucket-Algorithmus in der Firmware. Eine angemessene Burst-Größe für den Datenverkehrsbereich beträgt etwa 64.000 Byte. Die Burst-Größe sollte mindestens ein maximales Paket enthalten. Bei jedem eingehenden Paket bestimmt der Richtlinienalgorithmus die Zeit zwischen diesem Paket und dem letzten Paket und berechnet die Anzahl der Token, die während der verstrichenen Zeit generiert werden. Anschließend wird diese Anzahl von Token dem Bucket hinzugefügt und bestimmt, ob das ankommende Paket den angegebenen Parametern entspricht oder diese überschreitet.

## F. Warum erhalte ich eine geringere Leistung für TCP-Datenverkehr mit Ratenbegrenzung?

**Antwort:** TCP-Anwendungen verhalten sich schlecht, wenn Pakete aufgrund von Ratenbegrenzungen verworfen werden. Dies liegt an dem Fensterschema, das in der Flusssteuerung verwendet wird. Sie können den Burst-Size-Parameter oder den Rate-Parameter anpassen, um den erforderlichen Durchsatz zu erhalten.

## F. Welchen Vorteil bietet Weighted Random Early Detection (WRED), und wie kann ich feststellen, ob meine Linecard WRED unterstützen kann?

**Antwort:** Zur Vermeidung von Überlastungen bei der Ausgabeplanung unterstützt der Catalyst Switch der Serie 6500 (Cat6K) WRED in einigen Ausgangs-Warteschlangen. Jede Warteschlange hat eine konfigurierbare Größe und einen konfigurierbaren Grenzwert. Einige haben WRED. WRED ist ein Überlastungsvermeidungsmechanismus, der Pakete mit einer bestimmten IP-Rangfolge willkürlich verwirft, wenn die Puffer eine festgelegte Schwellwert-Füllung erreichen. WRED ist eine Kombination aus zwei Funktionen: Tail Drop und willkürliche Früherkennung (RED). Die frühe Catalyst-Betriebssystem-Implementierung (CatOS) von WRED setzte nur den maximalen Grenzwert fest, während der Min.-Schwellenwert fest auf 0 % festgelegt war. Beachten Sie, dass die Drop-Wahrscheinlichkeit für ein Paket immer nicht NULL ist, da sie immer über dem Min-Schwellenwert liegen. Dieses Verhalten wird in CatOS 6.2 und höher korrigiert. WRED ist ein sehr nützlicher Mechanismus zur Vermeidung von Überlastungen, wenn der Datenverkehrstyp TCP-basiert ist. Bei anderen Datenverkehrstypen ist ROT nicht sehr effizient, da ROT den Fenstermechanismus nutzt, der von TCP zur Überlastungsverwaltung verwendet wird.

Im Abschnitt [Understanding the Queueing Capability of a Port](#) of [QoS Output Scheduling on Catalyst 6500/6000 Series Switches Running CatOS System Software \(Informationen zur Warteschlangenfähigkeit von Catalyst Switches der Serien 6500 und 600\)](#) können Sie bestimmen, ob eine Linecard- oder Warteschlangenstruktur WRED unterstützen kann. Sie können auch den Befehl **show port functions (Portfunktionen anzeigen)** ausführen, um die Warteschlangenstruktur Ihrer Linecard anzuzeigen.

## F. Was ist der interne Differentiated Services Code Point (DSCP)?

**Antwort:** Jedem Frame ist eine interne CoS-Klasse (Class of Service, CoS) zugewiesen, entweder das empfangene CoS oder das Standard-Port-CoS. Dies schließt Frames ohne Tags ein, die keine echten CoS-Werte enthalten. Diese interne CoS und das empfangene DSCP werden in einem speziellen Paket-Header (einem so genannten Data Bus-Header) geschrieben und über den Data Bus an die Switching-Engine gesendet. Dies geschieht an der Eingangs-Linecard. Zu

diesem Zeitpunkt ist noch nicht bekannt, ob diese interne CoS in den ausgehenden anwendungsspezifischen integrierten Schaltkreis (ASIC) übertragen und in den ausgehenden Frame eingesetzt wird. Sobald der Header die Switching-Engine erreicht hat, weist die Engine Encoded Address Recognition Logic (EARL) jedem Frame ein internes DSCP zu. Bei diesem internen DSCP handelt es sich um eine interne Priorität, die dem Frame von der Policy Feature Card (PFC) beim Durchlaufen des Switches zugewiesen wird. Dies ist nicht der DSCP im IPv4-Header. Sie basiert auf einer bestehenden CoS- oder ToS-Einstellung (Type of Service) und wird zum Zurücksetzen des CoS oder ToS verwendet, wenn der Frame den Switch verlässt. Dieses interne DSCP wird allen Frames zugewiesen, die von der PFC (auch Nicht-IP-Frames) geschwicht (oder geroutet) werden.

## **F. Welche Quellen stehen für den internen Differentiated Services Code Point (DSCP) zur Verfügung?**

**Antwort:** Informationen zur [QoS-Klassifizierung und -Kennzeichnung von Catalyst Switches](#) der [Serien 6500/6000 mit CatOS-Software finden Sie im Abschnitt "Vier mögliche Quellen für internes DSCP"](#).

## **F. Wie wird der interne Differentiated Services Code Point (DSCP) gewählt?**

**Antwort:** Das interne DSCP hängt von folgenden Faktoren ab:

- Port-Vertrauensstatus
- Zugriffskontrollliste (ACL), die an den Port angeschlossen ist
- Standard-ACL
- VLAN-basiert oder Port-basiert in Bezug auf die ACL

Dieses Flussdiagramm fasst zusammen, wie das interne DSCP basierend auf der Konfiguration gewählt wird:



## F. Wird klassenbasiertes Weighted Fair Queuing (CBWFQ) oder Low Latency Queuing (LLQ) im Catalyst 6500 (Cat6K)-Switch unterstützt?

**Antwort:** Ja, mit der CBWFQ können Sie eine Datenverkehrsklasse definieren und ihr eine garantierte Mindestbandbreite zuweisen. Der Algorithmus hinter diesem Mechanismus ist Weighted Fair Queuing (WFQ), der den Namen erklärt. Sie definieren spezifische Klassen in Zuordnungsklassenanweisungen, um CBWFQ zu konfigurieren. Anschließend weisen Sie jeder Klasse in einer Richtlinienzuordnung eine Richtlinie zu. Diese Richtlinienzuweisung wird dann an die ein- und ausgehende Schnittstelle angefügt.

## F. Wird der CoS-Wert (Class of Service) für geroutete Pakete beibehalten?

**Antwort:** Ja, der interne Differentiated Services Code Point (DSCP) wird verwendet, um die CoS auf Ausgangs-Frames zurückzusetzen.

## F. Wenden QoS die gleiche Konfiguration auf alle LAN-Ports an, die über denselben ASIC gesteuert werden?

**Antwort:** Ja, wenn diese Befehle konfiguriert sind, wendet QoS die gleiche Konfiguration auf alle LAN-/gerouteten Ports an, die vom gleichen Application Specific Integrated Circuit (ASIC) gesteuert werden. QoS-Einstellungen werden an andere Ports propagiert, die demselben ASIC angehören, unabhängig davon, ob es sich bei dem Port um einen Zugriffsport, einen Trunk-Port oder einen gerouteten Port handelt.

- rcv-queue random-detect



- Warteschlangenlimit für rcv-queue
- Warteschlangen-Limit
- wrr-queue-Bandbreite (außer Gigabit-Ethernet-LAN-Ports)
- priority-queue cos-map
- rcv-queue cos-map
- wrr-queue cos-map
- Wrr-Queue-Grenzwert
- Rcv-queue-Grenzwert
- Wrr-queue random-detect
- wrr-queue random-detect min-threshold
- wrr-queue random-detect max-threshold

Wenn der **Standard-Schnittstellenbefehl** für einen der Ports ausgeführt wird, setzt der ASIC, der den jeweiligen Port steuert, die QoS-Konfiguration für alle Ports zurück, die von ihm gesteuert werden.

## F. Warum zeigt der Befehl `show traffic-shape statistics` kein positives Ergebnis an, selbst wenn die Datenverkehrsflutung konfiguriert ist?

```
Router#show traffic-shape statistics
      Access Queue   Packets   Bytes   Packets   Bytes   Shaping
I/F    List   Depth           Bytes   Delayed   Delayed   Active
Et0    101     0           2       180         0         0       no
Et1           0           0           0         0         0         0       no
```

**Antwort:** Das Shaping Active-Attribut hat **yes**, wenn Timer anzeigen, dass Datenverkehr Shaping stattfindet, und **no**, wenn kein Traffic Shaping auftritt.

Sie können den Befehl `show policy-map` verwenden, um zu überprüfen, ob der konfigurierte Datenverkehr funktioniert.

```
Router#show policy-map
Policy Map VSD1
  Class VOICE1
    Strict Priority
    Bandwidth 10 (kbps) Burst 250 (Bytes)
  Class SIGNALS1
    Bandwidth 8 (kbps) Max Threshold 64 (packets)
  Class DATA1
    Bandwidth 15 (kbps) Max Threshold 64 (packets)
Policy Map MQC-SHAPE-LLQ1
  Class class-default
    Traffic Shaping
      Average Rate Traffic Shaping
        CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
        Adapt to 8000 (bps)
        Voice Adapt Deactivation Timer 30 Sec
  service-policy VSD1
```

## F. Unterstützt der Catalyst 6500 PFC alle QoS-Standardbefehle?

**Antwort:** Die PFC-QoS für den Cisco Catalyst 6500 weist einige Einschränkungen auf und unterstützt einige QoS-bezogene Befehle nicht. Eine vollständige Liste der nicht unterstützten Befehle finden Sie in diesen Dokumenten.

- [Befehlsbeschränkungen für Klassenzuordnungen](#)
- [Befehlsbeschränkungen für Richtlinienzuweisungen](#)
- [Befehlsbeschränkungen für Policy Map Class](#)

## F. Warum sind die Software-CoPP-Zähler größer als die Hardware-CoPP-Zähler?

**Antwort:** Die CoPP-Zähler (Software Control Plane Policing) sind die Summe der Pakete, die Hardware-CoPP und Hardware-Ratenbegrenzung durchlaufen. Pakete werden zuerst von Hardware-Ratenlimitierungen behandelt. Wenn sie nicht übereinstimmen, wird das Hardware-CoPP angezeigt. Wenn der Hardware-Ratenlimitierer die Pakete zulässt, wird dieses Paket an die Software weitergeleitet, in der es von der Software CoPP verarbeitet wird. Aufgrund dieser Software kann CoPP größer sein als Hardware-CoPP-Zähler.

Es gibt auch einige Einschränkungen, bei denen CoPP in der Hardware nicht unterstützt wird. Einige davon sind:

- CoPP wird in der Hardware für Multicast-Pakete nicht unterstützt. Die Kombination aus ACLs, Multicast-CPU-Ratenlimitierungen und CoPP-Softwareschutz bietet Schutz vor Multicast-DoS-Angriffen.
- CoPP wird in der Hardware für Broadcast-Pakete nicht unterstützt. Die Kombination aus ACLs, Datenverkehrs-Sturmkontrolle und CoPP-Softwareschutz bietet Schutz vor Broadcast-DoS-Angriffen.
- Klassen, die Multicast entsprechen, werden nicht in der Hardware angewendet, sondern in der Software.
- CoPP ist in der Hardware nur aktiviert, wenn die MMLS-QoS mit dem Befehl `mls qos global` aktiviert ist. Wenn der Befehl `mls qos` nicht eingegeben wird, funktioniert CoPP nur in der Software und bietet der Hardware keine Vorteile.

Weitere Informationen finden Sie unter [Konfigurieren von CoPP \(Control Plane Policing\)](#).

## F. Funktioniert die QoS-Standardkonfiguration (Schnittstelle) für andere Schnittstellen/Ports?

**Antwort:** Wenn der **Standard-Schnittstellenbefehl** ausgegeben wird, wird die nicht standardmäßige Konfiguration gesammelt, die dem ähnelt, was in der `show running-config interface x/y` angezeigt wird, und für jeden dieser Konfigurationen sind die Standardwerte festgelegt. Dies kann auch eine einfache Ablehnung eines Befehls sein.

Wenn für diese Schnittstelle QoS oder andere Funktionen konfiguriert sind und diese Befehle abgelehnt werden, können sie an andere Schnittstellen der Linecard weitergeleitet werden.

Es wird empfohlen, die Ausgabe des Befehls **show interface x/y-Funktionen** zu überprüfen, bevor Sie mit der Standardeinstellung einer Schnittstelle fortfahren. Weitere Informationen finden Sie unter [Wird die identische Konfiguration von QoS auf alle LAN-Ports angewendet, die vom gleichen ASIC gesteuert werden?](#) für weitere Informationen.

Die Ausgabe des Befehls **Standard-Schnittstellen zeigt (falls vorhanden) auch andere Schnittstellen an, die für QoS und andere in diesem Port-ASIC implementierte Funktionen betroffen sind.**

## F. Kann ich QoS in einer Schnittstelle mit sekundärer IP-Adresse konfigurieren?

Antwort: Ja. Sie können QoS auf einer sekundären IP konfigurieren.

## Zugehörige Informationen

- [QoS-Ausgabeplanung für Catalyst Switches der Serien 6500 und 6000 mit CatOS-Systemsoftware](#)
- [QoS-Klassifizierung und -Kennzeichnung für Catalyst Switches der Serien 6500 und 6000 mit CatOS-Software](#)
- [QoS-Richtlinien für Catalyst Switches der Serien 6500 und 6000](#)
- [LAN-Produktunterstützung](#)
- [Unterstützung der LAN Switching-Technologie](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)