QoS - Häufig gestellte Fragen

Inhalt

Einführung

Dieses Dokument behandelt die am häufigsten gestellten Fragen (FAQs) im Zusammenhang mit Quality of Service (QoS).

Allgemeines

F. Was ist Quality of Service (QoS)?

Antwort: QoS bezieht sich auf die Fähigkeit eines Netzwerks, einen besseren Service für ausgewählten Netzwerkverkehr über verschiedene zugrunde liegende Technologien bereitzustellen, darunter Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet und 802.1-Netzwerke, SONET und IP-Routed Networks.

QoS ist eine Zusammenstellung von Technologien, mit denen Anwendungen berechenbare Service-Level hinsichtlich Datendurchsatzkapazität (Bandbreite), Latenzschwankungen (Jitter) und Verzögerungen anfordern und empfangen können. QoS-Funktionen bieten mithilfe der folgenden Methoden bessere und besser vorhersagbare Netzwerkdienste:

- Unterstützung dedizierter Bandbreite.
- Verbesserung der Verlusteigenschaften.
- Vermeidung und Management von Netzwerküberlastungen
- Shaping des Netzwerkverkehrs
- Festlegung von Verkehrsprioritäten im gesamten Netzwerk

Die Internet Engineering Task Force (IETF) definiert die folgenden beiden Architekturen für QoS:

- Integrierte Services (IntServ)
- Differenzierte Services (DiffServ)

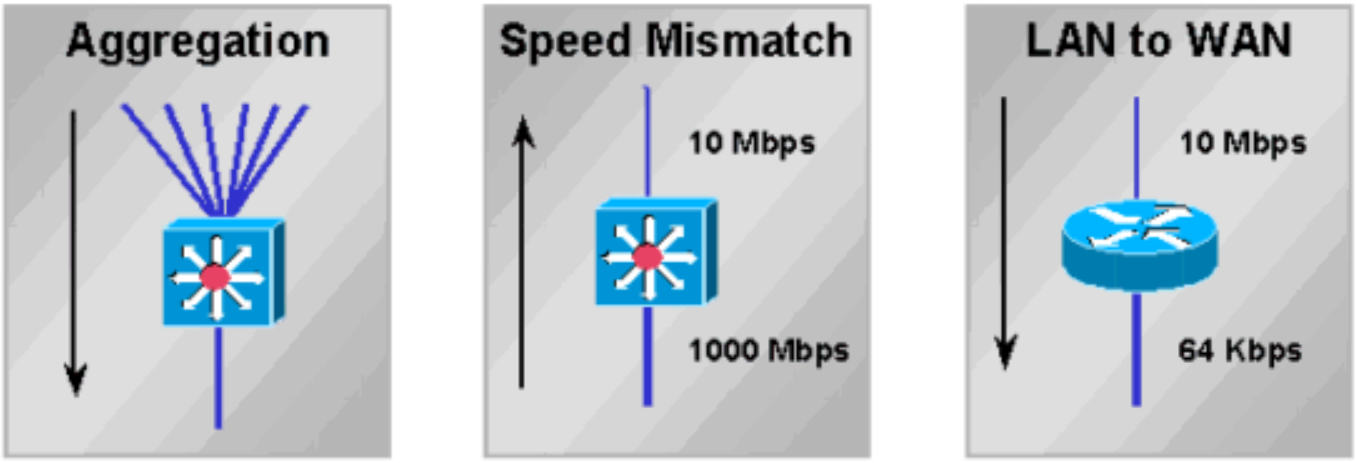
IntServ signalisiert mithilfe des Resource Reservation Protocol (RSVP) explizit die QoS-Anforderungen des Datenverkehrs einer Anwendung entlang der Geräte im End-to-End-Pfad durch das Netzwerk. Wenn jedes Netzwerkgerät auf dem Pfad die erforderliche Bandbreite reservieren kann, kann die ursprüngliche Anwendung mit der Übertragung beginnen. Request for Comments (RFC) 2205 definiert RSVP und RFC 1633 definiert IntServ.

DiffServ konzentriert sich auf aggregierte und bereitgestellte QoS. Anstatt die QoS-Anforderungen einer Anwendung zu signalisieren, verwendet DiffServ einen DiffServ Code Point (DSCP) im IP-Header, um die erforderlichen QoS-Ebenen anzugeben. Mit der Cisco IOS® Software-Version 12.1(5)T wurde die DiffServ-Compliance für Cisco Router eingeführt. Weitere Informationen finden Sie in den folgenden Dokumenten:

- Integrierter Service in Cisco IOS 12.1
- Implementierung von DiffServ für End-to-End Quality of Service
- Implementierung von Quality of Service-Richtlinien mit DSCP

F. Was sind Staus, Verzögerungen und Jitter?

Antwort: Eine Schnittstelle ist überlastet, wenn ihr mehr Datenverkehr als sie verarbeiten kann. Netzwerküberlastungspunkte sind gute Kandidaten für Quality of Service (QoS)-Mechanismen. Nachfolgend finden Sie ein Beispiel für typische Engpässe:



Netzwerküberlastungen führen zu Verzögerungen. Ein Netzwerk und seine Geräte verursachen verschiedene Arten von Verzögerungen, wie in Packet Voice Networks erläutert wird. Abweichungen bei Verzögerungen werden als Jitter bezeichnet, wie in Understanding Jitter in Packet Voice Networks (Cisco IOS-Plattformen) erläutert. Sowohl Verzögerungen als auch Jitter müssen gesteuert und minimiert werden, um den Echtzeit- und interaktiven Datenverkehr zu unterstützen.

F. Was ist der MQC?

Antwort: MQC steht für Modular Quality of Service (QoS) Command Line Interface (CLI). Sie vereinfacht die Konfiguration der QoS auf Cisco Routern und Switches durch die Definition einer gemeinsamen Befehlssyntax und der daraus resultierenden plattformübergreifenden QoS-Verhaltensweisen. Dieses Modell ersetzt das vorherige Modell der Definition eindeutiger Syntaxen für jede QoS-Funktion und für jede Plattform.

Der MQC umfasst die folgenden drei Schritte:

1. Definieren Sie eine Datenverkehrsklasse, indem Sie den Befehl **class-map** eingeben.
2. Erstellen Sie eine Datenverkehrsrichtlinie, indem Sie die Datenverkehrsklasse einem oder mehreren QoS-Features zuordnen, indem Sie den Befehl **policy-map** eingeben.
3. Fügen Sie die Datenverkehrsrichtlinie an die Schnittstelle, Subschnittstelle oder den Virtual Circuit (VC) an, indem Sie den Befehl **service-policy** eingeben.

Hinweis: Sie implementieren die Traffic Conditioning-Funktionen von DiffServ, z. B. Marking und Shaping, mithilfe der MQC-Syntax.

Weitere Informationen finden Sie unter Modular Quality of Service Command Line Interface (Modulare Dienstgüte für Befehlszeilenschnittstellen).

F. Was `bedeutet` die `Service-Richtlinie nur auf VIP-Schnittstellen mit DCEF-aktivierter` Nachricht?

Antwort: Bei VIPs (Versatile Interface Processors) der Cisco Serie 7500 werden nur verteilte Quality of Service (QoS)-Funktionen wie Cisco IOS 12.1(5)T, 12.1(5)E und 12.0(14)S unterstützt. Durch die Aktivierung von verteiltem Cisco Express Forwarding (dCEF) wird die verteilte QoS automatisch aktiviert.

Nicht-VIP-Schnittstellen, die als Legacy Interface Processors (IPs) bezeichnet werden, unterstützen zentrale QoS-Funktionen, die auf dem Route Switch Processor (RSP) aktiviert sind. Weitere Informationen finden Sie in den folgenden Dokumenten:

- Verteiltes, klassenbasiertes Weighted Fair Queueing und verteilte weighted Random Early Detection
- Verteiltes Low Latency Queueing
- Verteiltes Traffic Shaping
- Vielseitige Schnittstellenprozessorbasierte verteilte Versionen FRF.11 und FRF.12 für Cisco IOS Release 12.1 T

F. Wie viele Klassen unterstützt eine Quality of Service (QoS)-Richtlinie?

Antwort: In Cisco IOS-Versionen vor 12.2 können Sie maximal 256 Klassen definieren. Sie können in jeder Richtlinie bis zu 256 Klassen definieren, wenn dieselben Klassen für unterschiedliche Richtlinien wiederverwendet werden. Wenn Sie über zwei Richtlinien verfügen, sollte die Gesamtzahl der Klassen aus beiden Richtlinien 256 nicht überschreiten. Wenn eine Richtlinie Class-Based Weighted Fair Queueing (CBWFQ) (Class-Based Weighted Fair Queueing) enthält (d. h., sie enthält eine Bandbreiten- [oder Prioritätsanweisung] innerhalb einer der Klassen), wird insgesamt eine Anzahl von 64 Klassen unterstützt.

In den Cisco IOS-Versionen 12.2(12), 12.2(12)T und 12.2(12)S wurde diese Einschränkung von 256 globalen Klassenzuordnungen geändert. Es ist jetzt möglich, bis zu 1.024 globale Klassenzuordnungen zu konfigurieren und 256 Klassenzuordnungen innerhalb derselben Richtlinienzuordnung zu verwenden.

F. Wie werden Routing-Updates und Point-to-Point Protocol (PPP)-/High-Level Data Link Control (HDLC)-Keepalives verarbeitet, wenn eine Service-Richtlinie angewendet wird?

Antwort: Cisco IOS-Router priorisieren mithilfe der folgenden beiden Mechanismen Kontrollpakete:

- IP-Rangfolge
- pak_priority

Beide Mechanismen wurden entwickelt, um sicherzustellen, dass Schlüsselkontrollpakete nicht verworfen oder zuletzt vom Router und dem Warteschlangensystem verworfen werden, wenn eine ausgehende Schnittstelle überlastet wird. Weitere Informationen finden Sie unter Informationen zur Warteschlangenverwaltung von Routing-Updates und Steuerungspaketen auf einer Schnittstelle mit einer QoS-Dienstrichtlinie.

F. Wird Quality of Service (QoS) auf Schnittstellen unterstützt, die mit Integrated Routing and Bridging (IRB) konfiguriert sind?

Antwort: Nein. QoS-Funktionen können nicht konfiguriert werden, wenn die Schnittstelle für IRB konfiguriert ist.

Klassifizierung und Kennzeichnung

F. Was ist Quality of Service (QoS)-Vorklassifizierung?

Antwort: Die QoS-Vorklassifizierung ermöglicht Ihnen die Zuordnung und Klassifizierung des ursprünglichen IP-Headerinhalts von Paketen, die Tunnelkapselung und/oder -verschlüsselung unterzogen werden. Diese Funktion beschreibt nicht, wie der ursprüngliche Wert des ToS-Bytes (Type of Service) vom ursprünglichen Paket-Header in den Tunnel-Header kopiert wird. Weitere Informationen finden Sie in den folgenden Dokumenten:

- Konfigurieren von QoS für virtuelle private Netzwerke
- Quality of Service für virtuelle private Netzwerke, 12.2(2)T-Funktionsmodul

F. Welche Paket-Header-Felder können markiert werden? Welche Werte sind verfügbar?

Antwort: Mit der klassenbasierten Markierungsfunktion können Sie den Layer-2-, Layer-3- oder Multiprotocol Label Switching (MPLS)-Header Ihrer Pakete festlegen oder markieren. Weitere Informationen finden Sie in den folgenden Dokumenten:

- Konfigurieren von klassenbasierter Paketkennzeichnung
- Wann legt ein Router die CLP-Bit in einer ATM-Zelle fest?
- Konfigurieren der Paketkennzeichnung auf Frame-Relay-PVCs

F. Kann ich den Datenverkehr anhand der URL priorisieren?

Antwort: Ja. Network Based Application Recognition (NBAR) ermöglicht die Klassifizierung von Paketen, indem Felder auf Anwendungsebene zugeordnet werden. Vor der Einführung von NBAR waren die Portnummern Layer 4 Transmission Control Protocol (TCP) und User Datagram Protocol (UDP) die präziseste Klassifizierung. Weitere Informationen finden Sie in den folgenden Dokumenten:

- Fragen und Antworten zur netzwerkbasierten Anwendungserkennung

- NBAR Application Networking
- Verwenden von netzwerkbasierten Anwendungserkennungs- und Zugriffskontrolllisten zum Blockieren des Code Red Worm
- Schutz des Netzwerks vor dem Nimda-Virus

F. Welche Plattformen und Cisco IOS-Softwareversionen unterstützen die Network Based Application Recognition (NBAR)?

Antwort: Unterstützung für NBAR wird in den folgenden Versionen der Cisco IOS-Software eingeführt:

Plattform	Mindestversion der Cisco IOS Software
7200	12,1(5)T
7100	12,1(5)T
3660	12,1(5)T
3640	12,1(5)T
3620	12,1(5)T
2600	12,1(5)T
1700	12,2(2)T

Hinweis: Sie müssen Cisco Express Forwarding (CEF) aktivieren, um NBAR verwenden zu können.

Distributed NBAR (DNBAR) ist auf den folgenden Plattformen verfügbar:

Plattform	Mindestversion der Cisco IOS Software
7500	12.2(4)T, 12.1(6)E
FlexWAN	12,1(6)E

Hinweis: NBAR wird von den VLAN-Schnittstellen der Catalyst 6000 Multilayer Switch Feature Card (MSFC), der Cisco Serie 12000 oder dem Route Switch Module (RSM) für die Catalyst Serie 5000 nicht unterstützt. Wenn eine bestimmte Plattform oben nicht angezeigt wird, wenden Sie sich an Ihren technischen Ansprechpartner bei Cisco.

Warteschlangen- und Überlastungsmanagement

F. Wozu dient die Warteschlange?

Antwort: Die Warteschlangenverwaltung ist so konzipiert, dass vorübergehende Überlastungen an der Schnittstelle eines Netzwerkgeräts durch Speichern übermäßiger Pakete in Puffern behoben werden, bis die Bandbreite verfügbar wird. Cisco IOS-Router unterstützen verschiedene Warteschlangenmethoden, um die unterschiedlichen Bandbreiten-, Jitter- und Verzögerungsanforderungen verschiedener Anwendungen zu erfüllen.

Der Standardmechanismus der meisten Schnittstellen ist First In First Out (FIFO). Einige Datenverkehrstypen haben höhere Anforderungen an Verzögerungen/Jitter. Daher sollte einer der

folgenden alternativen Warteschlangenmechanismen konfiguriert oder standardmäßig aktiviert werden:

- Weighted Fair Queueing (WFQ)
- Class-Based Weighted Fair Queueing (CBWFQ)
- Low Latency Queueing (LLQ), d. h. CBWFQ mit einer Priority Queue (PQ) (auch PQCBWFQ genannt)
- Priority Queueing (PQ)
- Custom Queueing (CQ)

Die Warteschlangenverwaltung erfolgt in der Regel nur an ausgehenden Schnittstellen. Ein Router stellt Pakete in die Warteschlange, die eine Schnittstelle verlassen. Sie können eingehenden Datenverkehr überwachen, aber in der Regel können Sie keine Warteschlangen für eingehende Anrufe erstellen (eine Ausnahme ist die Empfangs-seitige Pufferung auf einem Cisco Router der Serie 7500, bei der verteilte Cisco Express Forwarding (dCEF) zum Weiterleiten von Paketen vom Eingang an die Ausgangsschnittstelle verwendet wird). Weitere Informationen finden Sie unter Understanding VIP CPU Running at 99% and Rx-Side Buffering. Auf verteilten High-End-Plattformen wie den Cisco Serien 7500 und 12000 kann die Schnittstelle für eingehende Anrufe mithilfe eigener Paketpuffer überschüssigen Datenverkehr speichern, der an eine überlastete Ausgangsschnittstelle weitergeleitet wird, nachdem die Switching-Entscheidung der Eingangsschnittstelle getroffen wurde. In seltenen Fällen kann die Eingangs-Schnittstelle, in der Regel wenn sie eine langsamere Ausgangsschnittstelle eingibt, bei Verlust des Paketspeichers ignorierte Fehler inkrementieren. Übermäßige Überlastungen können zu Verlusten in der Ausgabewarteschlange führen. Beim Verwerfen von Eingabewarteschlangen ist die Ursache meistens unterschiedlich. Weitere Informationen zur Fehlerbehebung finden Sie in folgendem Dokument:

- Fehlerbehebung: Verwerfen von Eingangswarteschlangen und Ausfall von Ausgabewarteschlangen

Weitere Informationen finden Sie in den folgenden Dokumenten:

- Fehlerbehebung bei "Ignoriert"-Fehlern bei einem ATM-Port-Adapter
- Fehlerbehebung Ignorierte Fehler und kein Speicherverlust beim Cisco Internet Router der Serie 12000

F. Wie funktionieren Weighted Fair Queueing (WFQ) und Class Based Weighted Fair Queueing (CBWFQ)?

Antwort: Faire Warteschlangenverwaltung zielt darauf ab, einen angemessenen Anteil der Bandbreite einer Schnittstelle an aktiven Gesprächen oder IP-Datenflüssen zuzuweisen. Sie klassifiziert Pakete in Unterwarteschlangen, die durch eine Konversationsidentifikationsnummer identifiziert werden. Dabei wird ein Hash-Algorithmus verwendet, der auf mehreren Feldern des IP-Headers und der Paketlänge basiert. Das Gewicht wird wie folgt berechnet:

- **W=K/(Rangfolge +1)**

K= 4096 mit Cisco IOS 12.0(4)T und früheren Versionen und 32384 mit 12.0(5)T und höheren Versionen.

Je geringer das Gewicht, desto höher die Priorität und der Anteil der Bandbreite. Neben dem Gewicht wird die Länge des Pakets berücksichtigt.

Mit der CBWFQ können Sie eine Datenverkehrsklasse definieren und ihr eine garantierte Mindestbandbreite zuweisen. Der Algorithmus hinter diesem Mechanismus ist WFQ, der den Namen erklärt. Zum Konfigurieren von CBWFQ definieren Sie bestimmte Klassen in Zuordnungsklassenanweisungen. Anschließend weisen Sie jeder Klasse in einer Richtlinienzuordnung eine Richtlinie zu. Diese Richtlinienzuweisung wird dann ausgehend an eine Schnittstelle angehängt. Weitere Informationen finden Sie in den folgenden Dokumenten:

- Grundlegende Informationen über Class-Based Weighted Fair Queuing auf ATM
- Gewichtete Fair-Warteschlangen auf ATM

F. Wenn eine Klasse in Class Based Weighted Fair Queueing (CBWFQ) ihre Bandbreite nicht nutzt, können andere Klassen die Bandbreite nutzen?

Antwort: Ja. Obwohl die Bandbreitengarantien, die durch die Ausgabe der **Bandbreite** und **Prioritätsbefehle** bereitgestellt werden, mit Wörtern wie "reserviert" und "Bandbreite zu reservieren" beschrieben wurden, implementiert keiner der Befehle eine echte Reservierung. Das heißt, wenn eine Datenverkehrsklasse die konfigurierte Bandbreite nicht nutzt, wird die ungenutzte Bandbreite von den anderen Klassen gemeinsam genutzt.

Das Warteschlangensystem stellt eine wichtige Ausnahme für diese Regel mit einer Prioritätsklasse dar. Wie oben erwähnt, wird die angebotene Last einer Prioritätsklasse durch eine Datenverkehrsüberwachung gemessen. Bei Überlastungen kann eine Prioritätsklasse keine überschüssige Bandbreite verwenden. Weitere Informationen finden Sie unter Vergleichen der Bandbreiten- und Prioritätsbefehle einer QoS-Dienstrichtlinie.

F. Wird Class Based Weighted Fair Queueing (CBWFQ) auf Subschnittstellen unterstützt?

Antwort: Logische Cisco IOS-Schnittstellen unterstützen keinen Überlastungszustand und unterstützen nicht die direkte Anwendung einer Service-Richtlinie, die eine Warteschlangenmethode anwendet. Stattdessen müssen Sie zunächst das Shaping auf die Subschnittstelle anwenden, indem Sie entweder Generic Traffic Shaping (GTS) oder klassenbasiertes Shaping verwenden. Weitere Informationen finden Sie unter Anwenden von QoS-Funktionen auf Ethernet-Subschnittstellen.

F. Worin besteht der Unterschied zwischen den `Prioritäts-` und `Bandbreitenanweisungen` in einer Richtlinienzuweisung?

Antwort: Die Befehle **für Priorität** und **Bandbreite** unterscheiden sich sowohl hinsichtlich der Funktionen als auch der Anwendungen, die sie normalerweise unterstützen. In der folgenden Tabelle sind diese Unterschiede zusammengefasst:

Funktion	Befehl "bandwidth"	priority-Befehl
Minimale Bandbreitengarantie	Ja	Ja
Maximale Bandbreitengarantie	Nein	Ja
Integrierte Überwachung	Nein	Ja

Niedrige Latenz	Nein	Ja

Weitere Informationen finden Sie unter Vergleichen der **Bandbreite** und Prioritätsbefehle einer QoS-Dienstrichtlinie.

F. Wie wird der Warteschlangengrenzwert für die FlexWAN- und VIP-Prozessoren (Versatile Interface Processors) berechnet?

Antwort: Unter Annahme eines ausreichenden SRAM im VIP oder FlexWAN wird der Grenzwert für die Warteschlange basierend auf einer maximalen Verzögerung von 500 ms bei einer durchschnittlichen Paketgröße von 250 Byte berechnet. Das folgende Beispiel zeigt eine Klasse mit einer Mbit/s Bandbreite:

Warteschlangenlimit = 1000000 / (250 x 8 x 2) = 250

Je geringer die verfügbare Speicherkapazität und je mehr Virtual Circuits (VCS) vorhanden sind, desto weniger Warteschlangen werden zugewiesen.

Im folgenden Beispiel wird ein PA-A3 in einer FlexWAN-Karte für die Cisco Serie 7600 installiert und unterstützt mehrere Subschnittstellen mit 2 MB Permanent Virtual Circuits (PVCs). Die Service-Richtlinie wird auf alle VCs angewendet.

```
class-map match-any XETRA-CLASS
  match access-group 104
class-map match-any SNA-CLASS
  match access-group 101
  match access-group 102
  match access-group 103
policy-map POLICY-2048Kbps
  class XETRA-CLASS
    bandwidth 320
  class SNA-CLASS
    bandwidth 512

interface ATM6/0/0
 no ip address
 no atm sonet ilmi-keepalive
 no ATM ilmi-keepalive
!
interface ATM6/0/0.11 point-to-point
 mtu 1578
 bandwidth 2048
 ip address 22.161.104.101 255.255.255.252
 pvc ABCD
  class-vc 2048Kbps-PVC
  service-policy out POLICY-2048Kbps
```

Die ATM-Schnittstelle (Asynchronous Transfer Mode) erhält einen Warteschlangenlimit für die gesamte Schnittstelle. Der Grenzwert hängt von der Gesamtzahl der verfügbaren Puffer, der Anzahl der physischen Schnittstellen im FlexWAN und der maximal zulässigen Warteschlangenverzögerung an der Schnittstelle ab. Jeder PVC erhält einen Teil der Schnittstellenbeschränkung, der auf der Sustained Cell Rate (SCR) oder der Minimum Cell Rate (MCR) der PVC basiert, und jede Klasse erhält einen Teil des PVC-Grenzwerts basierend auf der Bandbreitenzuweisung.

Die folgende Beispielausgabe des Befehls **show policy-map interface** wird von einem FlexWAN mit 3687 globalen Puffern abgeleitet. Geben Sie den Befehl **show buffer** ein, um diesen Wert anzuzeigen. Jeder PVC mit zwei Mbit/s wird 50 Pakete basierend auf der PVC-Bandbreite von zwei Mbit/s zugewiesen (2047/149760 x 3687 = 50). Jeder Klasse wird dann ein Teil der 50 zugewiesen, wie in der folgenden Ausgabe gezeigt:

```
service-policy output: POLICY-2048Kbps
    class-map: XETRA-CLASS (match-any)
      687569 packets, 835743045 bytes
      5 minute offered rate 48000 bps, drop rate 6000 BPS
      match: access-group 104
        687569 packets, 835743045 bytes
        5 minute rate 48000 BPS
      queue size 0, queue limit 7
      packets output 687668, packet drops 22
      tail/random drops 22, no buffer drops 0, other drops 0
      bandwidth: kbps 320, weight 15

    class-map: SNA-CLASS (match-any)
      2719163 packets, 469699994 bytes
      5 minute offered rate 14000 BPS, drop rate 0 BPS
      match: access-group 101
        1572388 packets, 229528571 bytes
        5 minute rate 14000 BPS
      match: access-group 102
        1146056 packets, 239926212 bytes
        5 minute rate 0 BPS
      match: access-group 103
        718 packets, 245211 bytes
        5 minute rate 0 BPS
      queue size 0, queue limit 12
      packets output 2719227, packet drops 0
      tail/random drops 0, no buffer drops 0, other drops 0
      bandwidth: kbps 512, weight 25
      queue-limit 100

    class-map: class-default (match-any)
      6526152 packets, 1302263701 bytes
      5 minute offered rate 44000 BPS, drop rate 0 BPS
      match: any
        6526152 packets, 1302263701 bytes
        5 minute rate 44000 BPS
      queue size 0, queue limit 29
      packets output 6526840, packet drops 259
      tail/random drops 259, no buffer drops 0, other drops 0
```

Wenn Ihre Datenverkehrsströme große Paketgrößen verwenden, kann die Ausgabe des Befehls **show policy-map** interface einen inkrementellen Wert für das Feld `no buffer drop` (Keine Pufferüberläufe) melden, da Ihnen möglicherweise Puffer fehlen, bevor Sie den Grenzwert für die Warteschlange erreichen. Versuchen Sie in diesem Fall, die Warteschlangengrenze in Klassen ohne Priorität manuell zu deaktivieren. Weitere Informationen finden Sie unter Understanding the Transmit Queue Limit with IP to ATM CoS.

F. Wie überprüfen Sie den Grenzwert für Warteschlangen?

Antwort: Auf nicht verteilten Plattformen beträgt die Warteschlangengrenze standardmäßig 64 Pakete. Die folgende Beispielausgabe wurde auf einem Cisco Router der Serie 3600 erfasst:

```
november# show policy-map interface s0
   Serial0

   Service-policy output: policy1

     Class-map: class1 (match-all)
       0 packets, 0 bytes
       5 minute offered rate 0 BPS, drop rate 0 BPS
       Match: ip precedence 5
       Weighted Fair Queueing
         Output Queue: Conversation 265
         Bandwidth 30 (kbps) Max Threshold 64 (packets)
         !--- Max Threshold is the queue-limit. (pkts matched/bytes matched) 0/0 (depth/total
drops/no-buffer drops) 0/0/0 Class-map: class2 (match-all) 0 packets, 0 bytes 5 minute offered
rate 0 BPS, drop rate 0 BPS Match: ip precedence 2 Match: ip precedence 3 Weighted Fair Queueing
Output Queue: Conversation 266 Bandwidth 24 (kbps) Max Threshold 64 (packets) (pkts
matched/bytes matched) 0/0 (depth/total drops/no-buffer drops) 0/0/0 Class-map: class-default
(match-any) 0 packets, 0 bytes 5 minute offered rate 0 BPS, drop rate 0 BPS Match: any
```

F. Kann ich faire Warteschlangen in einer Klasse aktivieren?

Antwort: Die Cisco Serie 7500 mit verteilter Quality of Service (QoS) unterstützt faire Warteschlangen pro Klasse. Andere Plattformen, darunter die Cisco Serien 7200 und 2600/3600, unterstützen Weighted Fair Queueing (WFQ) in der Klasse-Standardklasse. Alle Bandbreitenklassen verwenden First In First Out (FIFO).

F. Mit welchen Befehlen kann ich die Warteschlangenverwaltung überwachen?

Antwort: Verwenden Sie die folgenden Befehle, um Warteschlangen zu überwachen:

- **show queue *{interface}{interface number}* -** Auf anderen Cisco IOS-Plattformen als der Cisco Serie 7500 zeigt dieser Befehl die aktiven Warteschlangen oder Gespräche an. Wenn die Schnittstelle oder der Virtual Circuit (VC) nicht überlastet ist, werden keine Warteschlangen aufgelistet. Auf der Cisco Serie 7500 wird der Befehl **show queue** nicht unterstützt.
- **show queueing interface-number [vc [[vpi/] vci]** - Zeigt die Warteschlangenstatistiken einer Schnittstelle oder eines VC an. Auch wenn es keine Überlastung gibt, können Sie hier noch einige Treffer sehen. Der Grund dafür ist, dass prozessübergreifende Pakete immer unabhängig von der Überlastung gezählt werden. Cisco Express Forwarding (CEF) und Fast-Switched-Pakete werden nur bei Überlastung gezählt. Die vorhandenen Warteschlangenmechanismen wie Priority Queueing (PQ), Custom Queueing (CQ) und Weighted Fair Queueing (WFQ) bieten keine Klassifizierungsstatistiken. Diese Statistiken werden nur durch modulare MQC-basierte (Quality of Service Command Line Interface) Funktionen in Bildern nach 12.0(5)T bereitgestellt.
- **show policy interface *{interface}{interface number}* - Der** `Paketzähler` zählt die Anzahl der Pakete, die den Kriterien der Klasse entsprechen. Dieser Zähler erhöht, ob die Schnittstelle überlastet ist oder nicht. Der Zähler `Übereinstimmende Pakete` gibt die Anzahl der Pakete an, die den Kriterien der Klasse entsprechen, wenn die Schnittstelle überlastet wurde. Weitere Informationen zu Paketzählern finden Sie im folgenden Dokument:Verständnis von Paketzählern in Ausgabe der Richtlinienzuordnung anzeigen
- Cisco Class-Based QoS Configuration and Statistics MIB - Stellt SNMP-Überwachungsfunktionen (Simple Network Management Protocol) bereit.

F. RSVP kann zusammen mit Class Based Weighted Fair Queueing (CBWFQ)

verwendet werden. Wenn sowohl das Resource Reservation Protocol (RSVP) als auch der CBWFQ für eine Schnittstelle konfiguriert sind, handeln RSVP und CBWFQ unabhängig voneinander und weisen das gleiche Verhalten auf, wie es bei jeder eigenständigen Anwendung der Fall wäre? RSVP scheint sich so zu verhalten, als ob CBWFQ nicht hinsichtlich der Bandbreitenverfügbarkeit, -bewertung und -zuweisung konfiguriert ist.

Antwort: Bei Verwendung von RSVP und CB-WFQ in Cisco IOS Software, Version 12.1(5)T und höher, kann der Router so betrieben werden, dass RSVP-Datenflüsse und CBWFQ-Klassen die verfügbare Bandbreite einer Schnittstelle oder PVC ohne Überbelegung gemeinsam nutzen.

In der IOS-Softwareversion 12.2(1)T und höher kann RSVP die Zugangskontrolle mithilfe eines eigenen "ip rsvp bandwidth"-Pools durchführen, während CBWFQ die Klassifizierung, Richtlinienvergabe und Planung von RSVP-Paketen durchführt. Dabei wird vorausgesetzt, dass Pakete vom Absender vormarkiert werden und Pakete ohne RSVP unterschiedlich gekennzeichnet werden.

Überlastungsvermeidung Weighted Random Early Detection (WRED)

F. Kann ich gleichzeitig Weighted Random Early Detection (WRED) und Low Latency Queueing (LLQ) oder Class Based Weighted Fair Queueing (CBWFQ) aktivieren?

Antwort: Ja. Die Warteschlange definiert die Reihenfolge der Pakete, die eine Warteschlange verlassen. Dies bedeutet, dass ein Mechanismus für die Paketplanung definiert wird. Sie kann auch verwendet werden, um eine faire Bandbreitenzuweisung und garantierte Mindestbandbreite bereitzustellen. Im Gegensatz dazu definiert Request for Comments (RFC) 2475 das Verwerfen als den "Prozess des Verworfens von Paketen auf der Grundlage festgelegter Regeln". Der Standard-Drop-Mechanismus ist Tail Drop, bei dem die Schnittstelle Pakete verwirft, wenn die Warteschlange voll ist. Ein alternativer Drop-Mechanismus ist Random Early Detection (RED) und Cisco WRED. Hierbei werden Pakete nach dem Zufallsprinzip verworfen, bevor die Warteschlange voll ist, und es wird versucht, eine konsistente durchschnittliche Warteschlangentiefe beizubehalten. WRED verwendet den IP-Rangfolgewert von Paketen, um eine differenzierte Drop-Entscheidung zu treffen. Weitere Informationen finden Sie unter Weighted Random Early Detection (WRED).

F. Wie kann ich die Weighted Random Early Detection (WRED) überwachen und feststellen, dass sie tatsächlich wirksam wird?

Antwort: WRED überwacht die durchschnittliche Warteschlangentiefe und beginnt, Pakete zu verwerfen, wenn der berechnete Wert über den Mindestwert hinausgeht. Geben Sie den Befehl **show policy-map interface** ein, und überwachen Sie die mittlere Warteschlangentiefe, wie im folgenden Beispiel gezeigt:

```
Router# show policy interface s2/1

  Serial2/1
  output : p1
```

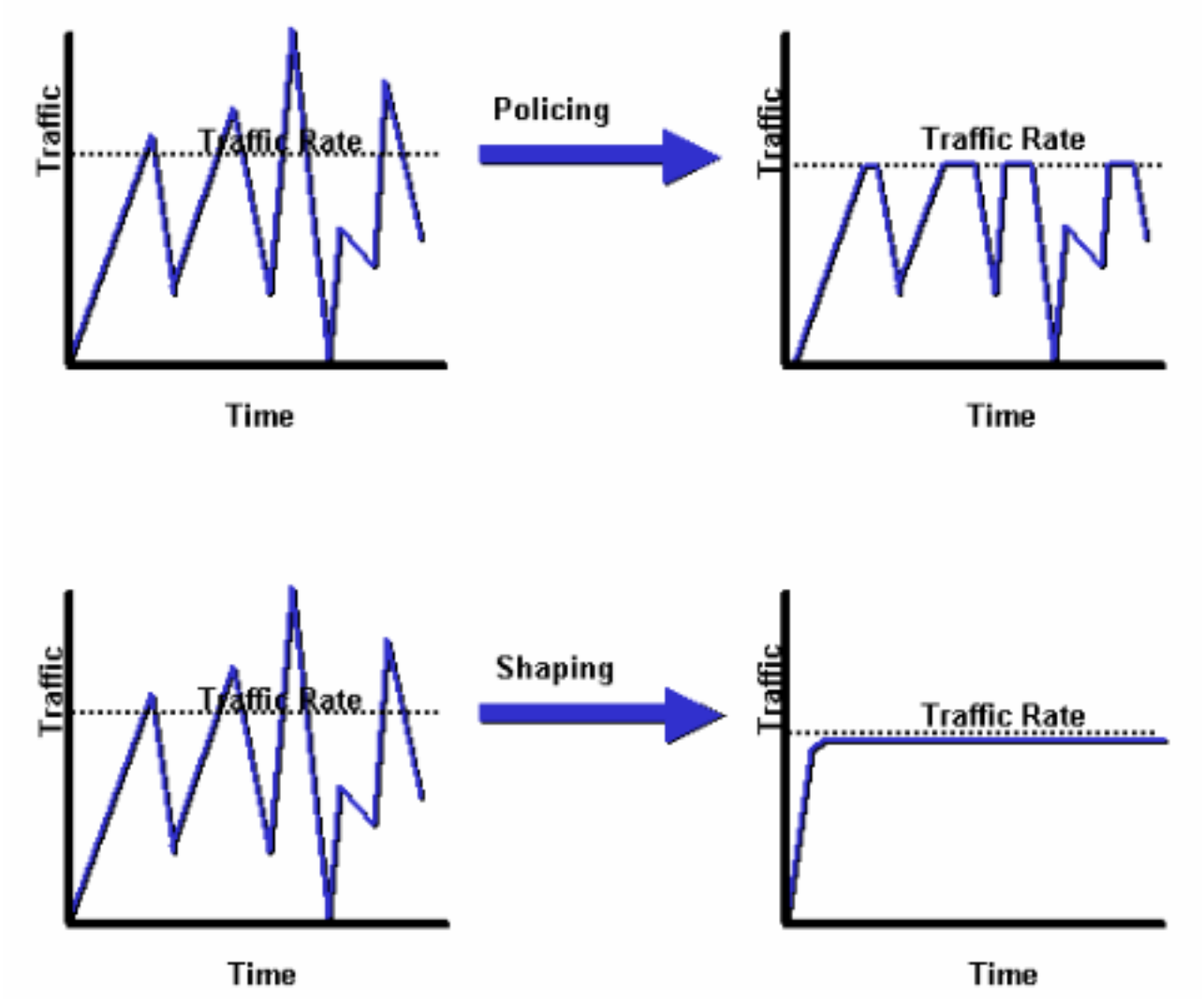
```
Class c1
 Weighted Fair Queueing
     Output Queue: Conversation 265
       Bandwidth 20 (%)
       (pkts matched/bytes matched) 168174/41370804
       (pkts discards/bytes discards/tail drops) 20438/5027748/0
       mean queue depth: 39

  Dscp     Random drop       Tail drop        Minimum   Maximum     Mark
  (Prec)    pkts/bytes        pkts/bytes      threshold threshold probability
    0(0)    2362/581052        1996/491016        20        40       1/10
    1          0/0                0/0             22        40       1/10
    2          0/0                0/0             24        40       1/10
    [output omitted]
```

Policing und Shaping

F. Worin besteht der Unterschied zwischen Richtlinienvergabe und Shaping?

Antwort: Im folgenden Diagramm wird der Hauptunterschied veranschaulicht. Beim Traffic Shaping werden überzählige Pakete in einer Warteschlange gespeichert, und der Überschuss wird dann schrittweise für eine spätere Übertragung festgelegt. Das Ergebnis des Traffic Shaping ist eine optimierte Paketausgaberate. Im Gegensatz dazu verbreitet die Datenverkehrsüberwachung Bursts. Wenn die Datenverkehrsrate die konfigurierte maximale Übertragungsrate erreicht, wird überschüssiger Datenverkehr verworfen (oder neu markiert). Das Ergebnis ist eine Ausgangsrate, die als Sägezahnspur mit Scheiteln und Tiefen erscheint.



Weitere Informationen finden Sie unter Übersicht über das Policing und Shaping.

F. Was ist ein Tokenbucket und wie funktioniert der Algorithmus?

Antwort: Eine Tokenbucket selbst verfügt über keine Rückwurfs- oder Prioritätsrichtlinie. Im Folgenden sehen Sie ein Beispiel für die Funktionsweise der Token-Bucket-Metapher:

- Token werden mit einer bestimmten Geschwindigkeit in den Eimer gelegt.
- Jedes Token ist die Berechtigung für die Quelle, eine bestimmte Anzahl von Bits zu senden.
- Um ein Paket zu senden, muss der Datenverkehrsregler in der Lage sein, eine Anzahl von Token aus der Gruppe zu entfernen, die der Paketgröße entspricht.
- Wenn sich nicht genügend Token im Eimer befinden, um ein Paket zu senden, wartet das Paket entweder, bis der Eimer genügend Token hat (bei einem Shaper), oder das Paket wird verworfen oder ausgezeichnet (bei einem Policer).
- Der Eimer selbst hat eine festgelegte Kapazität. Wenn der Eimer die Kapazität erreicht, werden neu eintreffende Token verworfen und sind für zukünftige Pakete nicht verfügbar. So ist der größte Burst, den eine Quelle in das Netzwerk senden kann, zu jeder Zeit ungefähr proportional zur Größe des Eckels. Ein Token-Eimer erlaubt Burstiness, aber grenzt ihn an.

F. Was bedeuten bei einer Datenverkehrsüberwachung wie klassenbasiertes Policing Committed Burst (BC) und Exzess Burst (Be) und wie sollten diese Werte ausgewählt werden?

Antwort: Eine Datenverkehrsüberwachung puffert keine überzähligen Pakete und leitet sie später weiter, wie dies bei einem Shaper der Fall ist. Stattdessen führt der Policer ein einfaches Senden aus oder sendet keine Richtlinie ohne Pufferung. In Zeiten von Überlastungen, in denen keine Pufferung möglich ist, ist das beste, was Sie tun können, wenn Sie Pakete weniger aggressiv verwerfen, indem Sie den erweiterten Burst korrekt konfigurieren. Daher ist es wichtig, dass Sie verstehen, dass der Policer die normalen Burst- und erweiterten Burst-Werte verwendet, um sicherzustellen, dass die konfigurierte Committed Information Rate (CIR) erreicht wird.

Die Burst-Parameter sind lose auf der allgemeinen Buffering-Regel für Router aufgebaut. Die Regel empfiehlt, eine Pufferung entsprechend der Round-Trip-Zeitbitrate zu konfigurieren, um die ausstehenden TCP-Fenster (Transmission Control Protocol) aller Verbindungen in Zeiten von Überlastung aufzunehmen.

In der folgenden Tabelle werden der Zweck und die empfohlene Formel für die normalen und erweiterten Burst-Werte beschrieben:

Burst-Parameter	Zweck	Empfohlene Formel
normaler Burst	• Implementiert eine standardmäßige Tokenbuchse. • Legt die maximale Größe der Tokenbuchse fest (obwohl Token geliehen werden können, wenn Be größer als	`CIR [BPS] * (1 byte)/(8 bits) * 1.5 seconds` **Hinweis:** 1,5 Sekunden

	BC ist). • Legt fest, wie groß die Tokenbucket sein kann, da neu eintreffende Token verworfen werden und für zukünftige Pakete nicht verfügbar sind, wenn die Eimer die Kapazität erreicht.	ist die typische Round-Trip-Zeit.
erweiterter Burst	• Implementiert eine Tokenbucket mit erweiterter Burst-Funktion. • Deaktiviert, indem BC = Be festgelegt wird. • Wenn BC gleich Be ist, kann sich der Verkehrsleiter keine Token ausleihen und das Paket einfach verwerfen, wenn keine ausreichenden Token verfügbar sind.	**2 * normal burst**

Nicht alle Plattformen verwenden oder unterstützen denselben Wertebereich für einen Policer. Im folgenden Dokument erfahren Sie, welche Werte für Ihre spezifische Plattform unterstützt werden:

- Übersicht über Policing und Shaping

F. Wie entscheidet die Committed Access Rate (CAR) oder klassenbasierte Richtlinienvergabe, ob ein Paket die Committed Information Rate (CIR) erfüllt oder überschreitet? Der Router verwirft Pakete und meldet eine Überschreitungsrate, obwohl die konforme Rate niedriger ist als die konfigurierte CIR.

Antwort: Eine Datenverkehrsüberwachung verwendet die normalen Burst- und erweiterten Burst-Werte, um sicherzustellen, dass die konfigurierte CIR erreicht wird. Um einen guten Durchsatz zu gewährleisten, ist es wichtig, ausreichend hohe Burst-Werte festzulegen. Wenn die Burst-Werte zu niedrig konfiguriert sind, kann die erreichte Rate viel niedriger sein als die konfigurierte Rate. Die Bestrafung temporärer Bursts kann sich stark nachteilig auf den Durchsatz des TCP-Datenverkehrs (Transmission Control Protocol) auswirken. Führen Sie mit CAR den Befehl **show interface rate-limit** aus, um den aktuellen Burst zu überwachen und zu bestimmen, ob der angezeigte Wert durchgehend nahe an den Grenzwerten (BC) und den Werten für erweiterte Grenzwerte (Be) liegt.

```
rate-limit 256000 7500 7500 conform-action continue exceed-action drop
rate-limit 512000 7500 7500 conform-action continue exceed-action drop

router# show interfaces virtual-access 26 rate-limit
    Virtual-Access26 Cable Customers
      Input
        matches: all traffic
          params:  256000 BPS, 7500 limit, 7500 extended limit
          conformed 2248 packets, 257557 bytes; action: continue
```

```
      exceeded 35 packets, 22392 bytes; action: drop
      last packet: 156ms ago, current burst: 0 bytes
      last cleared 00:02:49 ago, conformed 12000 BPS, exceeded 1000 BPS
  Output
    matches: all traffic
      params:  512000 BPS, 7500 limit, 7500 extended limit
      conformed 3338 packets, 4115194 bytes; action: continue
      exceeded 565 packets, 797648 bytes; action: drop
      last packet: 188ms ago, current burst: 7392 bytes
      last cleared 00:02:49 ago, conformed 194000 BPS, exceeded 37000 BPS
```

Weitere Informationen finden Sie in den folgenden Dokumenten:

- Übersicht über Policing und Shaping
- QoS-Richtlinienvergabe für Catalyst 6000
- Quality of Service bei Catalyst 4000 - Häufig gestellte Fragen
- Häufig gestellte Fragen zu Catalyst Switches der G-L3-Serie und WS-X4232-L3 Layer-3-Modulen QoS

F. Sind die Burst- und Warteschlangengrenzen voneinander unabhängig?

Antwort: Ja, die Grenze für Policer-Burst und Warteschlangen ist getrennt und unabhängig voneinander. Sie können den Policer als Gate anzeigen, das eine bestimmte Anzahl von Paketen (oder Byte) und die Warteschlange als *Grenzwert* für die Größe der *Warteschlange* zulässt, der die zugelassenen Pakete vor der Übertragung im Netzwerk enthält. Im Idealfall sollte der Eimer groß genug sein, um einen *Burst* von Bytes/Paketen zu enthalten, der vom Gate zugelassen wird (Policer).

Quality of Service (QoS) Frame-Relay

F. Welche Werte sollten für Committed Information Rate (CIR), Committed Burst (BC), Excess Burst (Be) und Minimum CIR (MinCIR) ausgewählt werden?

Antwort: Frame Relay Traffic Shaping, das Sie durch den Befehl **Frame-Relay Traffic Shaping** aktivieren, unterstützt mehrere konfigurierbare Parameter. Zu diesen Parametern gehören `Frame-Relay-Cir`, `Frame-Relay Mincir` und `Frame-Relay BC`. In den folgenden Dokumenten finden Sie weitere Informationen zum Auswählen dieser Werte und zum Verständnis der zugehörigen Anzeigebefehle:

- Konfigurieren von Frame-Relay-Traffic-Shaping auf Routern der Serie 7200 und untergeordneten Plattformen
- Befehle für Frame-Relay-Traffic-Shaping anzeigen
- VoIP over Frame Relay mit Quality of Service (Fragmentierung, Traffic Shaping, IP-RTP-Priorität)

F. Funktioniert Prioritätswarteschlange auf der Hauptschnittstelle von Frame Relay in Cisco IOS 12.1?

Antwort: Frame Relay-Schnittstellen unterstützen sowohl Schnittstellenwarteschlangen-Mechanismen als auch VC-Warteschlangenmechanismen (Per-Virtual Circuit). Ab Cisco IOS 12.0(4)T unterstützt die Schnittstellenwarteschlange FIFO (First In First Out) oder PIPQ (Per

Interface Priority Queueing) nur dann, wenn Frame Relay Traffic Shaping (FRTS) konfiguriert wird. Daher funktioniert die folgende Konfiguration nicht mehr, wenn Sie ein Upgrade auf Cisco IOS 12.1 durchführen.

```
interface Serial0/0
  frame-relay traffic-shaping
  bandwidth 256
  no ip address
  encapsulation frame-relay IETF
  priority-group 1

 !
 interface Serial0/0.1 point-to-point
  bandwidth 128
  ip address 136.238.91.214 255.255.255.252
  no ip mroute-cache
  traffic-shape rate 128000 7936 7936 1000
  traffic-shape adaptive 32000
  frame-relay interface-dlci 200 IETF
```

Wenn FRTS nicht aktiviert ist, können Sie eine alternative Warteschlangenmethode, z. B. Class Based Weighted Fair Queueing (CBWFQ), auf die Hauptschnittstelle anwenden, die wie eine einzige Bandbreitenpfeife funktioniert. Darüber hinaus können Sie mit Cisco IOS 12.1.1(T) Frame Relay Permanent Virtual Circuits (PVC) Priority Interface Queueing (PIPQ) auf einer Frame Relay-Hauptschnittstelle aktivieren. Sie können PVCs mit hoher, mittlerer, normaler oder niedriger Priorität definieren und den Befehl **Frame-Relay Interface-Queue Priority** auf der Hauptschnittstelle ausführen, wie im folgenden Beispiel gezeigt:

```
interface Serial3/0
 description framerelay main interface
 no ip address
 encapsulation frame-relay
 no ip mroute-cache
 frame-relay traffic-shaping
 frame-relay interface-queue priority

interface Serial3/0.103 point-to-point
 description frame-relay subinterface
 ip address 1.1.1.1 255.255.255.252
 frame-relay interface-dlci 103
  class frameclass

map-class frame-relay frameclass
 frame-relay adaptive-shaping becn
 frame-relay cir 60800
 frame-relay BC 7600
 frame-relay be 22800
 frame-relay mincir 8000
 service-policy output queueingpolicy
 frame-relay interface-queue priority low
```

F. Funktioniert Frame Relay Traffic Shaping (FRTS) mit Distributed Cisco Express Forwarding (dCEF) und Distributed Class Based Weighted Fair Queueing (dCBWFQ)?

Antwort: Ab Cisco IOS 12.1(5)T werden in den VIPs der Cisco Serie 7500 nur die verteilten Versionen der QoS-Funktionen unterstützt. Um Traffic Shaping an Frame-Relay-Schnittstellen zu

aktivieren, verwenden Sie Distributed Traffic Shaping (DTS). Weitere Informationen finden Sie in den folgenden Dokumenten:

- Vielseitige Schnittstellenprozessorbasierte verteilte Versionen FRF.11 und FRF.12 für Cisco IOS Release 12.1 T
- Frame-Relay-Traffic-Shaping mit verteilter QoS auf der Cisco Serie 7500

Quality of Service (QoS) über den asynchronen Übertragungsmodus (ATM)

F. Wo wende ich eine Service-Richtlinie mit Class Based Weighted Fair Queueing (CBWFQ) und Low Latency Queueing (LLQ) auf einer ATM-Schnittstelle (Asynchronous Transfer Mode) an?

Antwort: Ab Cisco IOS 12.2 unterstützen ATM-Schnittstellen Service-Richtlinien auf drei Ebenen oder logischen Schnittstellen: Hauptschnittstelle, Subschnittstelle und Permanent Virtual Circuit (PVC). Wenn Sie die Richtlinie anwenden, ist sie eine Funktion der Quality of Service (QoS)-Funktion, die Sie aktivieren. Warteschlangenrichtlinien sollten pro Virtual Circuit (VC) angewendet werden, da die ATM-Schnittstelle die Überlastungsstufe pro VC überwacht und Warteschlangen für übermäßige Pakete pro VC verwaltet. Weitere Informationen finden Sie in den folgenden Dokumenten:

- Wo wende ich eine QoS-Service-Richtlinie auf eine ATM-Schnittstelle an?
- PRO-VC-Übertragungswarteschlange an den PA-A3- und NM-1A-ATM-Schnittstellen

F. Welche Bytes werden von der Warteschlangenverwaltung von IP zu Asynchronous Transfer Mode (ATM) Class of Service (COs) gezählt?

Antwort: Die in einer Dienstrichtlinie konfigurierten Befehle für Bandbreite und Priorität, um Class-Based Weighted Fair Queueing (CBWFQ) bzw. Low Latency Queueing (LLQ) zu ermöglichen, verwenden einen Kbit/s-Wert, der dieselben Overhead-Bytes zählt wie die Ausgabe des Befehls show interface. Insbesondere zählt das Layer-3-Warteschlangensystem Logical Link Control / Subnetwork Access Protocol (LLC/SNAP). Folgendes wird nicht berücksichtigt:

- ATM Adaptation Layer 5 (AAL5)-Trailer
- Padding, um letzte Zelle zu einem selbst Vielfachen von 48 Byte zu machen
- 5-Byte-Zell-Header
- Welche Byte werden nach IP-zu-ATM-CO-Warteschlangen gezählt?

F. Wie viele Virtual Circuits (VCS) können eine Service-Richtlinie gleichzeitig unterstützen?

Antwort: Das folgende Dokument enthält nützliche Richtlinien zur Anzahl der unterstützten ASM-VCS (Asynchronous Transfer Mode). Etwa 200 bis 300 VBR-nrt Permanent Virtual Circuits (PVCs) wurden sicher bereitgestellt:

- Designleitfaden für IP to ATM Class of Service

Berücksichtigen Sie außerdem Folgendes:

- Verwenden Sie einen leistungsstarken Prozessor. Ein VIP4-80 bietet beispielsweise eine deutlich höhere Leistung als ein VIP2-50.
- Menge des verfügbaren Speicherplatzes Auf dem NPE-400 werden bis zu 32 MB (in einem System mit 256 MB) für den Paket-Puffer reserviert. Bei einem NPE-200 sind bis zu 16 MB für Paketpuffer auf einem System mit 128 MB reserviert.
- Konfigurationen mit WRED (Weighted Random Early Detection) pro VC, die gleichzeitig auf bis zu 200 ATM-PVCs ausgeführt werden, wurden umfassend getestet. Die Paketspeichermenge auf dem VIP2-50, die für die VC-Warteschlangen verwendet werden kann, ist begrenzt. Ein VIP2-50 mit 8 MB SRAM bietet beispielsweise 1085 Paketpuffer für IP-to-ATM-COs pro VC-Warteschlange, auf der WRED ausgeführt wird. Wenn 100 ATM-PVCs konfiguriert wurden und alle VCS gleichzeitig eine übermäßige Überlastung aufwiesen (wie in Testumgebungen simuliert werden könnte, in denen eine nicht TCP-flussgesteuerte Quelle verwendet wird), würde jede PVC im Durchschnitt etwa 10 Pakete puffern, die für einen erfolgreichen Betrieb von WRED zu kurz sein könnten. VIP2-50-Geräte mit großem SRAM werden daher in Designs mit einer hohen Anzahl von ATM-PVCs, die pro VC WRED ausgeführt werden und gleichzeitig Überlastungen verursachen können, dringend empfohlen.
- Je höher die Anzahl der konfigurierten aktiven PVCs, desto niedriger muss ihre Sustained Cell Rate (SCR) sein und desto kürzer ist die Warteschlange, die WRED für den Betrieb auf der PVC benötigt. Wie bei Verwendung der Standard-WRED-Profile der IP-to-ATM Class of Service (COs) Phase 1-Funktion würde die Konfiguration niedrigerer WRED-Drop-Schwellenwerte, wenn pro VC WRED auf einer sehr großen Anzahl von Low-Speed überlasteten ATM-PVCs aktiviert wird, das Risiko von Pufferengpässen im VIP minimieren. Puffer-Engpässe im VIP führen nicht zu Fehlfunktionen. Bei einem Puffermangel im VIP wird die IP-zu-ATM-COs Phase 1-Funktion während des Zeitraums des Pufferknappes einfach auf den First In First Out (FIFO)-Tail-Drop abgebaut (d. h. die gleiche Drop-Policy, die auch dann gilt, wenn die IP-zu-ATM-COs-Funktion auf dieser PVC nicht aktiviert wird).
- Maximale Anzahl gleichzeitiger VCS, die nach vernünftigem Ermessen unterstützt werden kann.

F. Welche ATM-Hardware (Asynchronous Transfer Mode) unterstützt IP-to-ATM Class of Service (COs)-Funktionen wie Class Based Weighted Fair Queueing (CBWFQ) und Low Latency Queueing (LLQ)?

Antwort: IP-zu-ATM-COs bezeichnet eine Reihe von Funktionen, die auf VC-Basis (Virtual Circuit) aktiviert werden. Aufgrund dieser Definition werden IP-zu-ATM-COs nicht von den ATM Interface Processor (AIP)-, PA-A1- oder 4500 ATM-Netzwerkprozessoren unterstützt. Diese ATM-Hardware unterstützt keine VC-Warteschlangen als PA-A3, und die meisten Netzwerkmodule (außer ATM-25) definieren diese. Weitere Informationen finden Sie in folgendem Dokument:

- Grundlagen der ATM-Hardwareunterstützung für IP-to-ATM-COs
- Class-Based, Weighted Fair Queuing auf RSP-basierten Plattformen
- Class-Based, Weighted Fair Queuing (Per-VC CBWFQ) auf den Cisco Routern 7200, 3600 und 2600
- Per-VC Queuing auf dem PA-A3-8T1/E1 IMA ATM-Port-Adapter
- Konfigurieren von ATM Per-VC Queueing auf dem MC3810

Sprache und Quality of Service (QoS)

F. Wie funktionieren Link Fragmentation and Interleaving (LFI)?

Antwort: Interaktiver Datenverkehr wie Telnet und Voice over IP ist anfällig für eine erhöhte Latenz, wenn das Netzwerk große Pakete wie File Transfer Protocol (FTP)-Übertragungen über ein WAN verarbeitet. Die Paketverzögerung für interaktiven Datenverkehr ist erheblich, wenn die FTP-Pakete auf langsameren WAN-Verbindungen in die Warteschlange gestellt werden. Es wurde eine Methode zur Fragmentierung größerer Pakete und zur Warteschlangenverwaltung kleinerer (Sprach-) Pakete zwischen den Fragmenten der größeren Pakete (FTP-Pakete) entwickelt. Cisco IOS-Router unterstützen mehrere Fragmentierungsmechanismen auf Layer 2. Weitere Informationen finden Sie in den folgenden Dokumenten:

- Übersicht über Verbindungseffizienzmechanismen
- VoIP over Frame Relay mit Quality of Service (Fragmentierung, Traffic Shaping, IP-RTP-Priorität)
- VoIP über PPP-Links mit Quality of Service (LLQ/IP RTP-Priorität, LFI, cRTP)

F. Mit welchen Tools kann ich die Voice-over-IP-Leistung überwachen?

Antwort: Cisco bietet derzeit mehrere Optionen zur Überwachung der Quality of Service (QoS) in Netzwerken an, die Voice over IP-Lösungen von Cisco verwenden. Diese Lösungen messen die Sprachqualität nicht mit PSQM (Perceptual Speech Quality Measurement) oder mit einigen der neuen vorgeschlagenen Algorithmen zur Messung der Sprachqualität. Dazu stehen Tools von Agilent (HP) und NetIQ zur Verfügung. Cisco bietet jedoch Tools an, die Ihnen einen Eindruck von der Sprachqualität vermitteln, die sich durch die Messung von Verzögerungen, Jitter und Paketverlusten ergibt. Weitere Informationen finden Sie unter Verwenden von Cisco Service Assurance Agent und Internetwork Performance Monitor zum Verwalten von Quality of Service in Voice over IP-Netzwerken.

F. %SW_MGR-3-CM_ERROR_FEATURE_CLASS: Verbindungsmanager-Funktionsfehler: Klasse-SSS: (QoS) - Installationsfehler, ignorieren.

Antwort: Der Fehler bei der Feature-Installation ist ein erwartetes Verhalten, wenn eine ungültige Konfiguration auf eine Vorlage angewendet wird. Sie weist darauf hin, dass die Service-Richtlinie aufgrund eines Konflikts nicht angewendet wurde. Im Allgemeinen sollten Sie das Shaping nicht auf Klassenstandard der untergeordneten Richtlinie in hierarchischen Richtlinienzuordnungen konfigurieren, sondern stattdessen auf der übergeordneten Richtlinie der Schnittstelle. Diese Nachricht wird zusammen mit der Rückverfolgung ausgedruckt.

Bei sitzungsbasierten Richtlinien muss das Shaping auf Klassenstandard nur auf der Sub-Schnittstellen- oder PVC-Ebene erfolgen. Shaping an der physischen Schnittstelle wird nicht unterstützt. Wenn die Konfiguration auf der physischen Schnittstelle vorgenommen wird, ist das Auftreten dieser Fehlermeldung ein erwartetes Verhalten.

Im Fall von LNS kann ein weiterer Grund sein, dass die Service-Richtlinie beim Starten der Sitzungen über den Radius-Server bereitgestellt werden kann. Geben Sie den Befehl **show tech** aus, um die Radius-Serverkonfiguration anzuzeigen und um illegale Dienstrichtlinien anzuzeigen, die beim Starten der Sitzung über den Radius-Server installiert werden oder die Sitzung berühren.

Zugehörige Informationen

- Grundlegende Leistungsoptimierung
- Quality of Service (QoS)-Unterstützung
- Technischer Support und Dokumentation - Cisco Systems