Erläuterungen zu den Paketzählern in der Befehlsausgabe mit Committed Access Rate (CAR) mit der Anzeigeschnittstellenrate

Inhalt

Einführung

Committed Access Rate (CAR) ist eine Funktion zur Ratenbegrenzung, die zur Bereitstellung von Klassifizierungs- und Richtliniendiensten verwendet werden kann. CAR kann verwendet werden, um Pakete anhand bestimmter Kriterien zu klassifizieren, z. B. IP-Adressen und Port-Werte, die Zugriffslisten verwenden. Die Aktion für Pakete, die dem Durchsatzgrenzwert entsprechen und den Wert überschreiten, kann definiert werden. Weitere Informationen zur CAR-Konfiguration finden Sie unter Konfigurieren der zugewiesenen Zugriffsrate.

In diesem Dokument wird erläutert, warum die Ausgabe des Befehls **show interface x/x rate-limit** einen Wert von `nicht 0 % über dem Bbit/s` anzeigt, wenn der `konforme Bbit/s`-Wert kleiner als die konfigurierte Committed Information Rate (CIR) ist.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips

Conventions (Technische Tipps zu Konventionen von Cisco).

Befehlsausgabe mit der Anzeigeschnittstellenrate

In der Ausgabe dieses Befehls sind drei Bedingungen für die Überschreitung von 0 (null) zu sehen:

- Burst-Werte werden zu niedrig eingestellt, um eine ausreichende Durchsatzrate zu ermöglichen. Ein Beispiel hierfür ist die Cisco Bug-ID CSCdw42923 (nur registrierte Kunden).
- Problem mit doppelter Buchführung in der Cisco IOS®-Software behoben
- Softwarefehler in Cisco IOS

Sehen Sie sich die Beispielausgabe von einer Virtual-Access-Schnittstelle an. In dieser Konfiguration wird RADIUS verwendet, um der dynamisch erstellten virtuellen Zugriffsschnittstelle eine Ratenbeschränkung zuzuweisen.

```
AV Pair from Radius
Cisco-AVPair = "lcp:interface-config#1=rate-limit input 256000 7500 7500
conform-action continue
exceed-action drop",
Cisco-AVPair = "lcp:interface-config#2=rate-limit output 512000 7500 7500
conform-action continue
exceed-action drop",
```

Verwenden Sie den Befehl **show interface x rate-limit**, um die Leistung des Cisco Legacy Policer, CAR, zu überwachen. In diesem Beispiel enthält die Ausgabe dieses Befehls Hinweise darauf, warum es eine Nicht-0-Überschreitung von bps gibt. Der aktuelle Burst-Wert beträgt 7.392 Byte, während der durch den Grenzwert angegebene bestätigte Burst-Wert (Bc) auf 7.500 Byte festgelegt wird.

```
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
```

Wenn Sie die CAR oder eine neuere Richtlinienvergabe von Cisco konfigurieren, müssen Sie klassenbasierte Richtlinienvergabe ausreichend hohe Burst-Werte konfigurieren, um den erwarteten Durchsatz sicherzustellen und sicherzustellen, dass die Überwachung Pakete nur verwirft, um kurzfristige Überlastungen zu verhindern.

Bei der Auswahl von Burst-Werten ist es wichtig, vorübergehende Erhöhungen der Warteschlangengröße zu berücksichtigen. Sie können nicht einfach annehmen, dass Pakete gleichzeitig eintreffen und abgehen. Sie können auch nicht davon ausgehen, dass sich die

Warteschlange von leer zu ein Paket ändert und dass die Warteschlange bei einem Paket bleibt, das auf einer konsistenten Ein-/Ausgangs-Ankunftszeit basiert. Wenn der typische Datenverkehr relativ stark belastet ist, müssen die Burst-Werte entsprechend groß sein, damit die Verbindungsauslastung auf einem akzeptabel hohen Niveau gehalten werden kann. Eine zu niedrige Burst-Größe oder ein zu niedriger Mindestabstand können zu einer inakzeptabel niedrigen Verbindungsauslastung führen.

Ein Burst kann einfach als eine Reihe von Back-to-Back-Frames mit MTU-Größe definiert werden, z. B. Frames mit 1500 Byte, die aus einem Ethernet-Netzwerk stammen. Wenn ein Burst solcher Frames an einer Ausgabeschnittstelle eintrifft, kann er die Ausgabepuffer überlasten und die konfigurierte Tiefe des Tokenbuckets zu einem bestimmten Zeitpunkt überschreiten. Bei Verwendung eines Token-Messsystems entscheidet ein Policer binär, ob ein ankommendes Paket die konfigurierten Richtlinienwerte einhält, übertrifft oder verletzt. Beim Burst-Datenverkehr, z. B. einem FTP-Stream, kann die sofortige Ankunftsrate dieser Pakete die konfigurierten Burst-Werte überschreiten und zu CAR-Verlusten führen.

Darüber hinaus variiert der Gesamtdurchsatz in Zeiten von Überlastungen je nach Art des Datenverkehrs, der von der Richtlinie ausgewertet wird. Während der TCP-Datenverkehr auf eine Überlastung reagiert, ist dies bei anderen Datenströmen nicht der Fall. Beispiele für nicht reagierende Datenflüsse sind UDP- und ICMP-basierte Pakete.

TCP basiert auf einer positiven Bestätigung mit erneuter Übertragung. TCP verwendet ein gleitendes Fenster als Teil des positiven Bestätigungsmechanismus. Sliding Window-Protokolle verwenden die Netzwerkbandbreite besser, da sie dem Absender ermöglichen, mehrere Pakete zu übertragen, bevor er auf eine Bestätigung wartet. In einem Gleitfensterprotokoll mit einer Fenstergröße von 8 darf der Sender beispielsweise 8 Pakete übertragen, bevor er eine Bestätigung erhält. Wenn Sie die Fenstergröße erhöhen, wird die Zeit im Leerlauf im Netzwerk weitgehend eliminiert. Ein durchdachtes Schiebetreuprotokoll hält das Netzwerk vollständig ausgelastet mit Paketen und hält einen hohen Durchsatz aufrecht.

Da die Endpunkte den spezifischen Überlastungsstatus des Netzwerks nicht kennen, wurde TCP als Protokoll entwickelt, um bei Überlastungen im Netzwerk durch die Reduzierung der Übertragungsraten zu reagieren. Im Einzelnen werden dabei zwei Techniken eingesetzt:

Technik	Beschreibung
Multiplikative Verringerung der Überlastungsvermeidung	Reduzieren Sie nach Verlust eines Segments (das entspricht einem Paket TCP) das Überlastungsfenster um die Hälfte. Das Überlastungsfenster ist ein zweiter Wert oder ein zweites Fenster, das verwendet wird, um die Anzahl der Pakete zu begrenzen, die ein Absender an das Netzwerk senden kann, bevor er auf eine Bestätigung wartet.
Langsame Wiederherstellung	Wenn Sie den Datenverkehr über eine neue Verbindung starten oder den Datenverkehr nach einer Überlastungsphase erhöhen, starten Sie das Überlastungsfenster in der Größe eines einzelnen Segments und erhöhen das Überlastungsfenster jedes Mal um ein Segment, wenn eine Bestätigung eingeht.

	TCP initialisiert das Überlastungsfenster auf 1, sendet ein erstes Segment und wartet. Wenn die Bestätigung eingeht, erhöht sie das Überlastungsfenster auf 2, sendet zwei Segmente und wartet darauf. Weitere Informationen finden Sie unter RFC 2001 .

Pakete können verloren gehen oder vernichtet werden, wenn Übertragungsfehler Daten stören, Netzwerkhardware ausfällt oder Netzwerke zu stark ausgelastet sind, um die anfallende Last zu bewältigen. TCP geht davon aus, dass verlorene Pakete oder Pakete, die aufgrund extremer Verzögerungen nicht innerhalb des Zeitintervalls bestätigt werden, auf eine Überlastung im Netzwerk hinweisen.

Das Token-Bucket-Messsystem eines Policers wird bei jeder Paketankündigung aufgerufen. Insbesondere werden der konforme Satz und der Überschreitungssatz auf der Grundlage dieser einfachen Formel berechnet:

```
(conformed bits since last clear counter)/(time in seconds elapsed since last clear counter)
```

Da die Formel die Raten für einen Zeitraum ab dem letzten Clearing der Zähler berechnet, empfiehlt Cisco, die Zähler zu löschen, um die aktuelle Rate zu überwachen. Wenn die Zähler nicht gelöscht werden, bedeutet die vorherige Berechnungsrate tatsächlich, dass die Ausgabe des Befehls **show** einen über einen potenziell sehr langen Zeitraum berechneten Durchschnitt anzeigt und die Werte bei der Bestimmung des aktuellen Zinssatzes möglicherweise nicht von Bedeutung sind.

Der durchschnittliche Durchsatz muss mit der konfigurierten Committed Information Rate (CIR) über einen bestimmten Zeitraum übereinstimmen. Burst-Größen ermöglichen eine maximale Burst-Dauer zu einem bestimmten Zeitpunkt. Wenn kein Datenverkehr oder weniger als der CIR-Wert vorliegt und der Token-Eimer nicht gefüllt wird, ist ein sehr großer Burst immer noch auf eine bestimmte Größe beschränkt, die auf normalen Burst und längerem Burst basiert.

Die Drop-Rate ergibt sich aus diesem Mechanismus.

1. Notieren Sie sich die aktuelle Uhrzeit.
2. Aktualisieren Sie die Tokenbuchse mit der Anzahl der Token, die sich seit der letzten Ankunft eines Pakets kontinuierlich angesammelt haben.
3. Die Gesamtzahl der akkumulierten Token darf den Wert für die maximale Anzahl von Token nicht überschreiten. Legen Sie überschüssige Token ab.
4. Überprüfen Sie die Paketkonformität.

Die Ratenbegrenzung kann auch mithilfe von Policing erreicht werden. Dies ist eine Beispielkonfiguration, um eine Ratenbegrenzung für die Ethernet-Schnittstelle bereitzustellen, die klassenbasierte Richtlinienvergabe verwendet.

```
class-map match-all rtp1
   match ip rtp 2000 10
!
   policy-map p3b
   class rtp1
   police 200000 6250 6250 conform-action transmit exceed-action drop violate-action    drop
policy-map p2
```

```
   class rtp1
   police 250000 7750 7750 conform-action transmit exceed-action drop violate-action    drop
   !
interface Ethernet3/0
   service-policy output p3b
   service-policy input p2
```

Diese Beispielausgabe aus dem Befehl **show policy-map interface** veranschaulicht die korrekt berechneten und synchronisierten Werte für die angebotene Rate und die angebotene Abfallrate sowie die konfigurierten bzw. die Überschreitung der Bitraten.

```
router#show policy-map interface ethernet 3/0
  Ethernet3/0

   Service-policy input: p2

     Class-map: rtp1 (match-all)
       88325 packets, 11040625 bytes
       30 second offered rate 400000 bps, drop rate 150000 bps
       Match: ip rtp 2000 10
       police:
         250000 bps, 7750 limit, 7750 extended limit
         conformed 55204 packets, 6900500 bytes; action: transmit
         exceeded 33122 packets, 4140250 bytes; action: drop
         conformed 250000 bps, exceed 150000 bps violate 0 bps

       Service-policy : p3b

         Class-map: rtp1 (match-all)
           88325 packets, 11040625 bytes
           30 second offered rate 400000 bps, drop rate 50000 bps
           Match: ip rtp 2000 10
           police:
             200000 bps, 6250 limit, 6250 extended limit
             conformed 44163 packets, 5520375 bytes; action: transmit
             exceeded 11041 packets, 1380125 bytes; action: drop
             conformed 200000 bps, exceed 50000 bps violate 0 bps

         Class-map: class-default (match-any)
           0 packets, 0 bytes
           30 second offered rate 0 bps, drop rate 0 bps
           Match: any
```

Bekannte Probleme mit CAR und klassenbasierten Richtlinienzählern

In dieser Tabelle sind die gelösten Probleme mit den Zählern aufgeführt, die in den Befehlen **show policy-map** oder **show interface rate-limit** angezeigt werden. Registrierte Kunden, die angemeldet sind, können die Fehlerinformationen im Bug Search Tool einsehen.

Symptom	Beheben von Bug-IDs und Problemumgehungen
Geringere Drop-Zähler als erwartet	• Cisco Bug-ID CSCdv41231 (nur registrierte Kunden)Wenn eine hierarchische Eingabehilfenrichtlinie den **polizeilichen** Befehl auf der übergeordneten und der untergeordneten Ebene verwendet, kann der Policer weniger als die erwartete Anzahl von Paketen verwerfen, da der übergeordnete

	Policer überlastet werden muss, bevor die Pakete verworfen werden. Dies ist ein Beispiel für eine solche Richtlinie:
	`policy-map child`
	`class dscp1`
	`police cir 100000 bc 3000 conform-action transmit exceed-action drop`
	`!`
	`policy-map parent`
	`class rtp1`
	`police cir 250000 bc 7750 conform-action transmit exceed-action drop`
	`service-policy child`
	Erstellen Sie als Problemumgehung separate Richtlinien, und wenden Sie eine für eingehende und eine für ausgehende Richtlinien an, um die Konfiguration einer hierarchischen Richtlinie zu vermeiden.

Verdoppeln Sie die erwartete Rate von Verlusten und Durchsatz.	• Cisco Bug ID CSCds23924 (nur registrierte Kunden)Cisco Express Forwarding (CEF) definiert einen IOS-Switching-Mechanismus, der Pakete von der Eingangs- zur Ausgangsschnittstelle weiterleitet. Vor den Änderungen, die mithilfe dieser Bug-ID implementiert wurden, erhöhten sowohl CEF als auch konfigurierte QoS-Mechanismen wie CAR oder klassenbasierte Richtlinienvergabe die Paketzähler. Das Ergebnis sind so genannte doppelte Abrechnung, überhöhte Pakete und überhöhte Paketverluste. • Cisco Bug-ID CSCdr40598 (nur registrierte Kunden)Wenn bei der Cisco Serie 1200 die CAR für die Ausgabe aktiviert ist und die Eingangs-Linecard die Engine 2 ist, werden die Ausgangszähler verdoppelt. Diese doppelte Abrechnung ergibt sich aus der Behandlung von Ausgabecomputern. • Cisco Bug-ID CSCdv84259 (nur registrierte Kunden)Wenn Sie den Befehl **ip cef distributed** auf einem Router der Cisco 7500-Serie global aktivieren, wird eine VIP-Kartenschnittstelle (Non-Versatile Interface Processor) angezeigt, wobei der Befehl **ip route-cache distributed** standardmäßig aktiviert ist. Nicht-VIPs unterstützen kein verteiltes CEF, und ein seltener Nebeneffekt dieses Befehls, der auf Nicht-VIPs angezeigt wird, ist die doppelte Buchhaltung.
Keine Verlus	Im Allgemeinen besteht der erste Schritt bei der Fehlerbehebung bei der Anwendung

trate oder Nullabfallrate	klassenbasierter QoS-Funktionen darin, sicherzustellen, dass der QoS-Klassifizierungsmechanismus ordnungsgemäß funktioniert. Mit anderen Worten: Stellen Sie sicher, dass die in den Match-Anweisungen in der Klassenzuordnung angegebenen Pakete die richtigen Klassen treffen.
	`router#show policy-map interface ATM4/0.1`
	`Service-policy input: drop-inbound-http-hacks (1061)`
	`Class-map: http-hacks (match-any) (1063/2)`
	`149 packets, 18663 bytes`
	`5 minute offered rate 2000 bps, drop rate 0 bps`
	`Match: protocol http url "*cmd.exe*" (1067)`
	`145 packets, 18313 bytes`
	`5 minute rate 2000 bps`
	`Match: protocol http url "*.ida*" (1071)`
	`0 packets, 0 bytes`
	`5 minute rate 0 bps`
	`Match: protocol http url "*root.exe*" (1075)`
	`4 packets, 350 bytes`
	`5 minute rate 0 bps`
	`Match: protocol http url "*readme.eml*" (1079)`
	`0 packets, 0 bytes`
	`5 minute rate 0 bps`
	`police:`
	`1000000 bps, 31250 limit, 31250 extended limit`
	`conformed 0 packets, 0 bytes; action: drop`
	`exceeded 0 packets, 0 bytes; action: drop`
	`violated 0 packets, 0 bytes; action: drop`
	`conformed 0 bps, exceed 0 bps violate 0 bps`
	• Cisco Bug ID CSCds34478 (nur registrierte Kunden)Die Klassifizierung schlägt fehl, wenn CEF und nicht DCEF aktiviert ist und eine Eingangsrichtlinie an eine ATM-PVC angeschlossen ist. In der Cisco IOS Software, Version 12.1T, schlägt die Ausgabenklassifizierung fehl, wenn CEF und nicht DCEF aktiviert ist und eine Ausgaberichtlinie an eine ATM-PVC angeschlossen ist.

Anomalische oder inkonsistente	• Cisco Bug ID CSCdw50583 (nur registrierte Kunden)Die in der Klassenzuordnung angezeigte Droprate stimmt nicht mit den von der Polizeiaktion angegebenen Dropraten

Fallrate	überein. In dieser Beispielausgabe beträgt die Abfallrate für die Klasse 745000 bps, während die Abfallrate für Polizeiaktionen 1072000 bps beträgt.
	`router#show policy-map interface`
	`  Serial3/0.1: DLCI 13 -`
	
	`   Service-policy output: out`
	
	`     Class-map: c2 (match-all)`
	`       172483 packets, 91760956 bytes`
	`       30 second offered rate 1384000 bps, drop rate 745000 bps`
	`       Match: ip precedence 0`
	`       police:`
	`         384000 bps, 1500 limit, 1500 extended limit`
	`         conformed 38903 packets, 20696396 bytes; action: transmit`
	`         exceeded 133580 packets, 71064560 bytes; action: drop`
	`         conformed 311000 bps, exceed 1072000 bps violate 0 bps`

Zugehörige Informationen

- Konfigurieren der zugewiesenen Zugriffsrate
- Richtlinienvergabe mit CAR
- Verwendung von CAR bei DOS-Angriffen
- Support-Seite für QoS-Technologie
- Support-Seite für IP Routed Protocols
- Support-Seite für IP-Routing
- Technischer Support und Dokumentation - Cisco Systems