

# Verständnis und Fehlerbehebung bei Eingabehilfen für Nexus 5600/6000

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Unicast-Datenverkehrsfluss und -pufferung](#)

[Multicast-Datenverkehrsfluss und -pufferung](#)

[Welche Ursachen haben Rückwürfe?](#)

[Problembhebungsszenarien](#)

[Szenerio 1. Eingabeditionen](#)

[Schritt 1: Identifizieren von Ports mit Eingabedickern](#)

[Schritt 2: ASIC-Identifizierung](#)

[Schritt 3: Identifizieren des ausgehenden kongetierten Ports](#)

[Szenerio 2. Eingabehilfen mit HOLB](#)

[HOLB-Eindämmung: VOQ-Grenzwert aktivieren](#)

[HOLB-Eindämmung: Klassifizierung des Datenverkehrs](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie Fehler bei Rückkarten der Cisco Nexus Switches der Serien 5600 und 6000 beheben können.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse der Konfiguration der Cisco Nexus Serie 6000 zu verfügen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Nexus 6001
- 7.1(3)N1(1)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

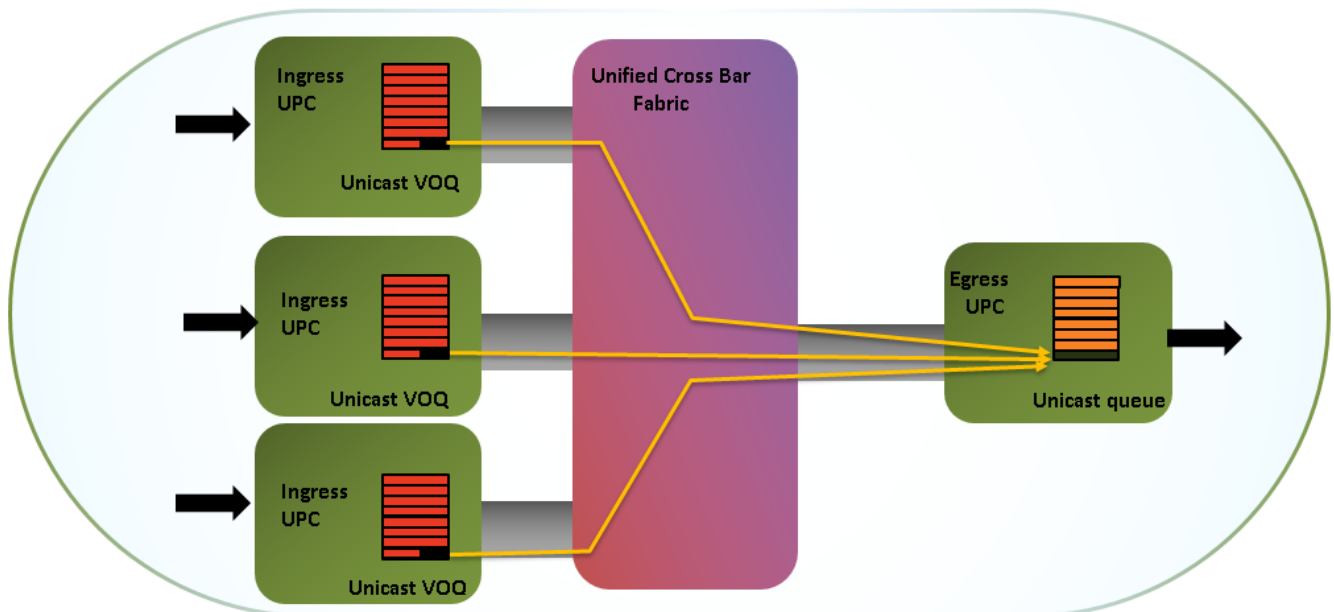
(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Eingabedikarten sind ein Hinweis auf einen überbelegten Ausgangsport. Dies bedeutet auch, dass Sie Unicast-Datenverkehr wahrscheinlich auf diesem bestimmten Port verwerfen. In diesem Artikel erfahren Sie, wie Unicast- und Multicast-Datenverkehr auf dieser Plattform gepuffert wird und wie Eingabedikarten zusammen mit den Eindämmungsschritten auftreten können.

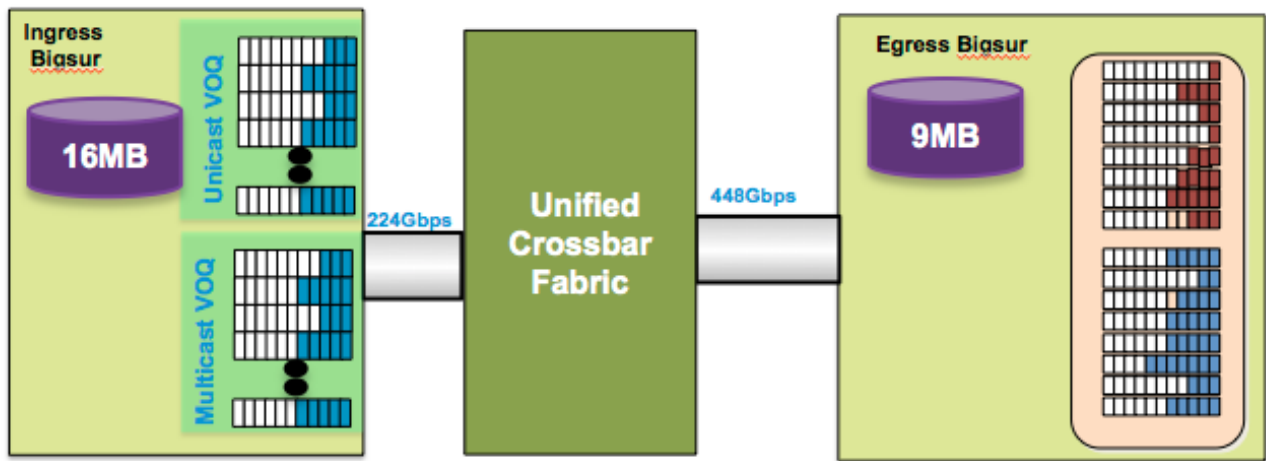
## Unicast-Datenverkehrsfluss und -pufferung

Unicast-Datenverkehr wird zuerst beim Ausgangspufferpool in die Warteschlange gestellt, und dann, nachdem die Ausgangswarteschlange voll ist, wie im Bild gezeigt.



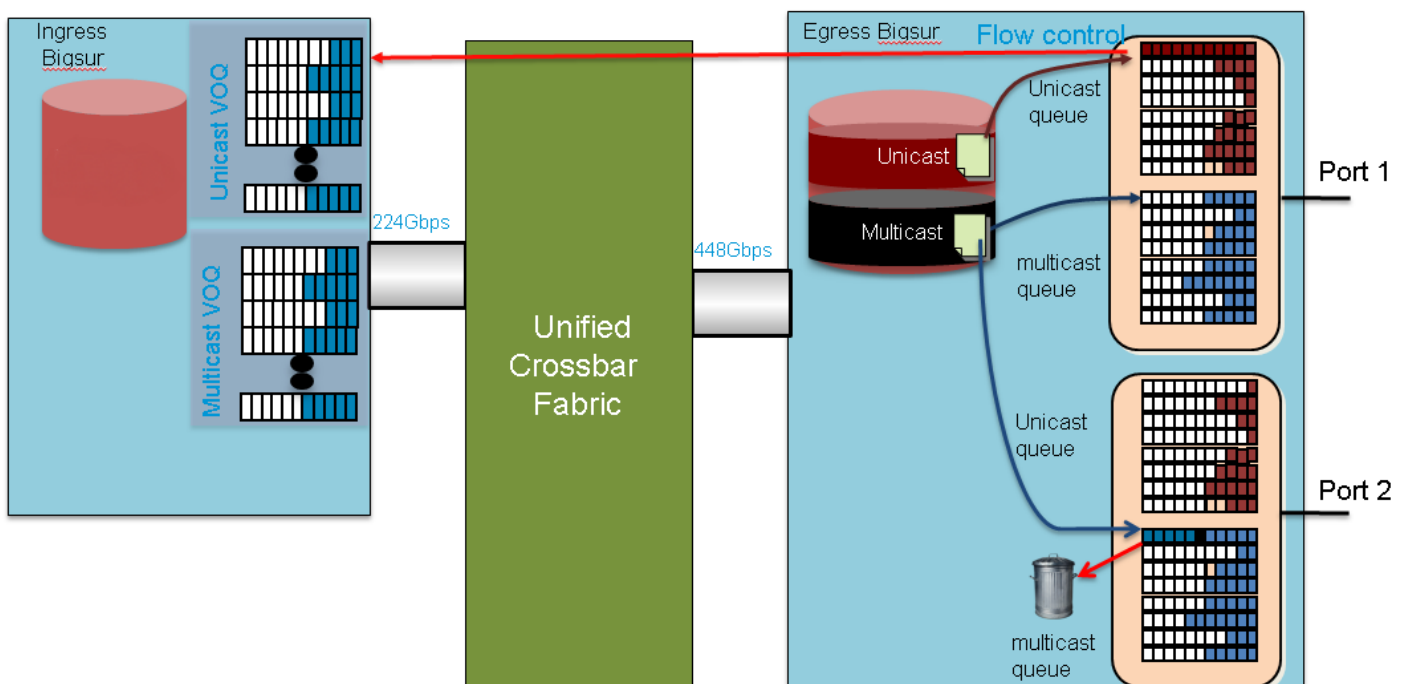
Es gibt einen gemeinsamen Eingangspuffer mit 16 MB und einen gemeinsamen Ausgangspuffer mit 9 MB. Die Puffer werden von 12 x 10-Gig-Ports oder 3 x 40-Gig-Ports gemeinsam genutzt. Gemeinsam genutzter Puffer eignet sich gut für die Burst-Absorption.

Es folgt eine visuelle Darstellung der Speicherzuweisung für Ihre Referenz (BigSur ist der Name des ASIC/Unified Port Controller), wie im Bild gezeigt.



## Multicast-Datenverkehrsfluss und -pufferung

- Multicast-Pakete werden gepuffert und am Ausgang verworfen
- Verwerfen Sie das Multicast-Paket nahe dem Überlastungspunkt, um die Head of Line Blocking (HOLB) zu vermeiden.
- Verwalten Sie verlustfreies Fabric für Unicast, wie im Bild gezeigt.



In den meisten Fällen sind Ausgangs-Datenverluste immer auf Multicast-/Broadcast-/Unknow-  
Unicast-Datenverkehr zurückzuführen.

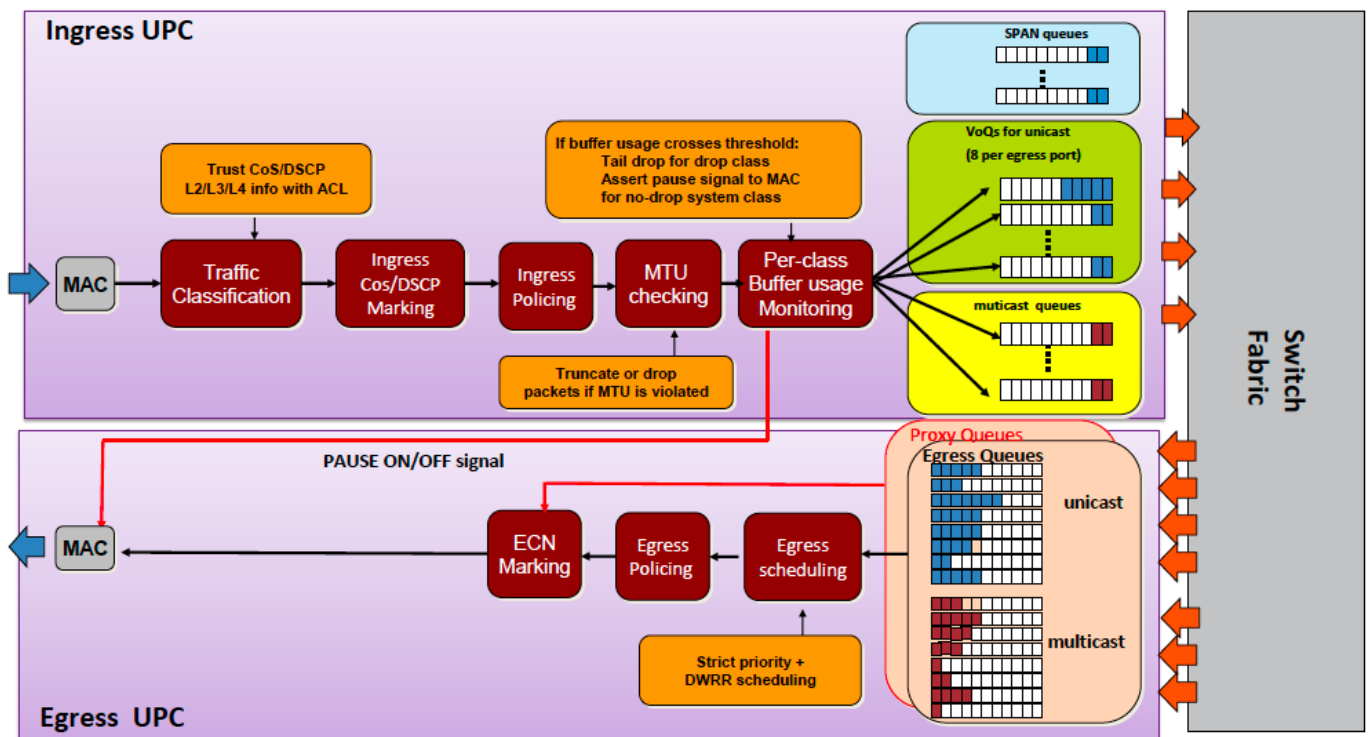
## Welche Ursachen haben Rückwürfe?

Ein überlasteter Ausgangs-Port verursacht die Ausgangs-Puffer, um zuerst aufzufüllen und dann den Rückendruck auf den Eingang zu verursachen. Dies gilt nur für Unicast-Datenverkehr. Wenn die Eingangspuffer voll sind, können Sie möglicherweise Datenverkehr beim Eingang verwerfen, was zu Rückwürfen bei der Eingabe führt.

Diese Erläuterung ist sehr allgemein gehalten und leicht zu verarbeiten, aber sie enthält noch ein

wenig mehr, insbesondere wenn Sie verschiedene Klassen von Datenverkehr, Warteschlangen usw. betrachten. Es gibt ein Konzept für Virtual Output Queue (VOQ), das häufig auf der Nexus-Plattform verwendet wird. VOQ ist eine Zuweisung von Eingangspuffern für alle IEEE 802.1p Class of Service (CoS) pro Ausgangsport. Es gibt also 8 VOQ pro Ausgangsport.

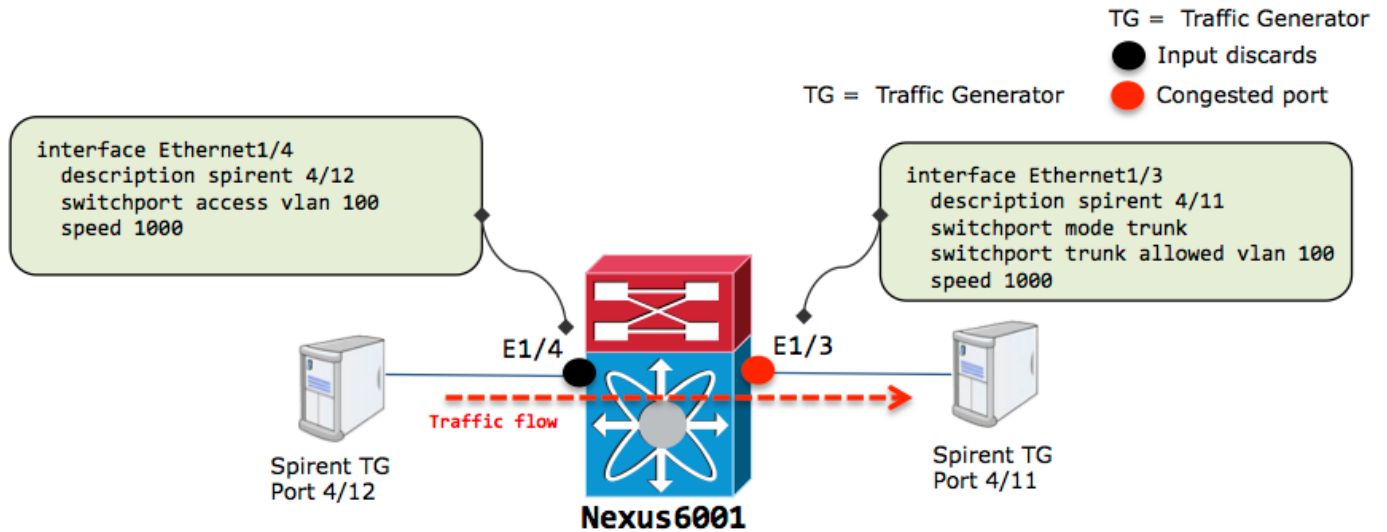
Eine Überlastung an einem Ausgangsport in einer CoS führt schließlich zur Überlastung des entsprechenden VOQs am Eingangsport. Sobald das Limit erreicht ist, wird der Datenverkehr verworfen. Sie betrifft jedoch keinen Datenverkehr, der für andere CoSs oder andere Ausgangsschnittstellen bestimmt ist, und vermeidet so HOLB, das sonst zu einer Überlastung führen würde. Der Datenverkehrsfluss vom Eingangs- zum Ausgangs-Port und die verschiedenen abgebildeten Blöcke werden im Bild dargestellt.



## Problembhebungsszenarien

### Szenario 1. Eingabeditionen

Übungseinrichtung:



Datenverkehr mit Leitungsgeschwindigkeit steigt an e1/3 und mögliche Überbelegung:

```

nexus6001# sh int e1/3
Ethernet1/3 is up
Dedicated Interface
Hardware: 1000/10000 Ethernet, address: 002a.6a56.7a8a (bia 002a.6a56.7a8a)
Description: spirent 4/11
MTU 1500 bytes, BW 1000000 Kbit,, BW 1000000 Kbit, DLY 10 usec
reliability 255/255, txload 251/255, rxload 25/255
Encapsulation ARPA, medium is broadcast
Port mode is trunk
full-duplex, 1000 Mb/s
Beacon is turned off
Input flow-control is off, output flow-control is off
Switchport monitor is off
EtherType is 0x8100
Last link flapped 11:39:20
Last clearing of "show interface" counters 00:00:15
0 interface resets
30 seconds input rate 98683696 bits/sec, 8223 packets/sec
30 seconds output rate 986853640 bits/sec, 82019 packets/sec
Load-Interval #2: 5 minute (300 seconds)
  input rate 98.68 Mbps, 8.22 Kpps; output rate 986.85 Mbps, 82.01 Kpps
RX
 124003 unicast packets  0 multicast packets  0 broadcast packets
 124003 input packets  186004500 bytes
 0 jumbo packets  0 storm suppression bytes
 0 runs  0 giants  0 CRC  0 no buffer
 0 input error  0 short frame  0 overrun  0 underrun  0 ignored
 0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
 0 input with dribble  0 input discard
 0 Rx pause
TX
 1236745 unicast packets  9 multicast packets  0 broadcast packets
 1236754 output packets  1860065401 bytes
 0 jumbo packets
 0 output error  0 collision  0 deferred  0 late collision
 0 lost carrier  0 no carrier  0 babble 0 output discard
 0 Tx pause
  
```

```

nexus6001# sh int e1/4
Ethernet1/4 is up
Dedicated Interface

Hardware: 1000/10000 Ethernet, address: 002a.6a56.7a8b (bia 002a.6a56.7a8b)
Description: spirent 4/12
MTU 1500 bytes, BW 1000000 Kbit,, BW 1000000 Kbit, DLY 10 usec
reliability 255/255, txload 25/255, rxload 251/255
Encapsulation ARPA, medium is broadcast
Port mode is access
full-duplex, 1000 Mb/s
Beacon is turned off
Input flow-control is off, output flow-control is off
Switchport monitor is off
EtherType is 0x8100
Last link flapped 10:53:31
Last clearing of "show interface" counters 00:00:04
0 interface resets
30 seconds input rate 986840376 bits/sec, 82236 packets/sec
30 seconds output rate 98421072 bits/sec, 8223 packets/sec
Load-Interval #2: 5 minute (300 seconds)
  input rate 986.84 Mbps, 82.23 Kpps; output rate 98.42 Mbps, 8.22 Kpps
RX
  326332 unicast packets  0 multicast packets  0 broadcast packets
  326332 input packets  489496500 bytes
  0 jumbo packets  0 storm suppression bytes
  0 runts  0 giants  0 CRC  0 no buffer
  0 input error  0 short frame  0 overrun  0 underrun  0 ignored
  0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
  0 input with dribble  863 input discard >>>>>
  0 Rx pause
TX
  32633 unicast packets  2 multicast packets  0 broadcast packets
  32635 output packets  48819096 bytes
  0 jumbo packets
  0 output error  0 collision  0 deferred  0 late collision
  0 lost carrier  0 no carrier  0 babble 0 output discard
  0 Tx pause

```

In einer simulierten Konfiguration, wie hier beschrieben, kennen Sie die Ursache der Überbelegung, aber in einer Produktionsumgebung, in der das Datenverkehrsprofil ausgebrochen ist und es eine Herausforderung sein kann, die überlasteten Ausgangs-Ports mithilfe dieser Befehle zu erkennen.

Mit den hier aufgeführten Schritten können Sie die überlasteten Ausgangs-Ports identifizieren.

## Schritt 1: Identifizieren von Ports mit Eingabedickern

Rückwürfe für Eingänge an Port e1/4 sichtbar:

```

nexus6001# sh int e1/4 | in i disc
  0 input with dribble  3024 input discard
  0 lost carrier  0 no carrier  0 babble 0 output discard

nexus6001# sh queuing int e1/4
Ethernet1/4 queuing information:
TX Queuing
  qos-group  sched-type  oper-bandwidth
  0          WRR        100

```

## RX Queuing

### qos-group 0 >>>> Drops in QOS 0

q-size: 100160, q-size-40g: 100160, HW MTU: 1500 (1500 configured)

drop-type: drop, xon: 0, xoff: 0

#### Statistics:

```
Pkts received over the port           : 9612480
Ucast pkts sent to the cross-bar      : 9587016
Mcast pkts sent to the cross-bar      : 0
Ucast pkts received from the cross-bar : 961249
Pkts sent to the port                 : 961261
Pkts discarded on ingress           : 3024 >>>>>
Per-priority-pause status             : Rx (Inactive), Tx (Inactive)
```

## Schritt 2: ASIC-Identifizierung

- Ordnen Sie die Schnittstelle der internen ASIC-Nummer (UPC) dieser Ausgabe zu.
- Finden Sie die Eingangs-ASIC-ID aus der Eingangs-Port-ID heraus, auf der Sie bemerkt haben, dass sie verworfen wurde.

```
nexus6001# sh hard internal bigsur all-ports
```

#### Bigsur Port Info:

Port name	asic idx	inst slot	inst asic	inst eport	inst logi	inst flag	inst adm	inst opr	inst if_index	inst diag	inst ucVer
sup1	0	0	0	0 -	48	b3	en	dn	15010000	pass	0.00
sup0	0	0	0	1 -	49	b3	en	dn	15020000	pass	0.00
lgb1/1	1	0	1	2 -	0	b3	en	up	1a000000	pass	0.00
lgb1/2	1	0	1	3 -	1	b3	en	up	1a001000	pass	0.00
lgb1/3	1	0	1	0 -	2	b3	en	up	1a002000	pass	0.00
<b>lgb1/4</b>	<b>1**</b>	<b>0</b>	<b>1</b>	<b>1 -</b>	<b>3</b>	<b>b3</b>	<b>en</b>	<b>up</b>	<b>1a003000</b>	<b>pass</b>	<b>0.00 &gt;&gt;&gt;&gt;** is the asic number</b>
lgb1/5	1	0	1	6 -	4	b3	en	up	1a004000	pass	0.00
lgb1/6	1	0	1	7 -	5	b3	en	up	1a005000	pass	0.00
lgb1/7	1	0	1	4 -	6	b3	en	up	1a006000	pass	0.00
lgb1/8	1	0	1	5 -	7	b3	en	up	1a007000	pass	0.00
lgb1/9	1	0	1	10 -	8	b3	en	up	1a008000	pass	0.00
lgb1/10	1	0	1	11 -	9	b3	en	up	1a009000	pass	0.00
lgb1/11	1	0	1	8 -	10	b3	en	up	1a00a000	pass	0.00
xgb1/12	1	0	1	9 -	11	b3	en	dn	1a00b000	pass	0.00
xgb1/13	2	0	2	2 -	12	b3	en	dn	1a00c000	pass	0.00
xgb1/14	2	0	2	3 -	13	b3	en	dn	1a00d000	pass	0.00
xgb1/15	2	0	2	0 -	14	b3	en	dn	1a00e000	pass	0.00
xgb1/16	2	0	2	1 -	15	b3	en	dn	1a00f000	pass	0.00
xgb1/17	2	0	2	6 -	16	b3	en	dn	1a010000	pass	0.00
xgb1/18	2	0	2	7 -	17	b3	en	dn	1a011000	pass	0.00
xgb1/19	2	0	2	4 -	18	b3	en	dn	1a012000	pass	0.00
xgb1/20	2	0	2	5 -	19	b3	en	dn	1a013000	pass	0.00
xgb1/21	2	0	2	10 -	20	b3	en	dn	1a014000	pass	0.00
xgb1/22	2	0	2	11 -	21	b3	en	dn	1a015000	pass	0.00
xgb1/23	2	0	2	8 -	22	b3	en	dn	1a016000	pass	0.00
xgb1/24	2	0	2	9 -	23	b3	en	dn	1a017000	pass	0.00
xgb1/25	3	0	3	2 -	24	b3	en	dn	1a018000	pass	0.00
xgb1/26	3	0	3	3 -	25	b3	en	dn	1a019000	pass	0.00
xgb1/27	3	0	3	0 -	26	b3	en	dn	1a01a000	pass	0.00
xgb1/28	3	0	3	1 -	27	b3	en	dn	1a01b000	pass	0.00
xgb1/29	3	0	3	6 -	28	b3	en	dn	1a01c000	pass	0.00
xgb1/30	3	0	3	7 -	29	b3	en	dn	1a01d000	pass	0.00
xgb1/31	3	0	3	4 -	30	b3	en	dn	1a01e000	pass	0.00
xgb1/32	3	0	3	5 -	31	b3	en	dn	1a01f000	pass	0.00

```

xgb1/33 | 3 | 0 | 3 | 10 - | 32 | b3 | en | dn | 1a020000 | pass | 0.00
xgb1/34 | 3 | 0 | 3 | 11 - | 33 | b3 | en | dn | 1a021000 | pass | 0.00
xgb1/35 | 3 | 0 | 3 | 8 - | 34 | b3 | en | dn | 1a022000 | pass | 0.00
xgb1/36 | 3 | 0 | 3 | 9 - | 35 | b3 | en | dn | 1a023000 | pass | 0.00
xgb1/37 | 4 | 0 | 4 | 2 - | 36 | b3 | en | dn | 1a024000 | pass | 0.00
xgb1/38 | 4 | 0 | 4 | 3 - | 37 | b3 | en | dn | 1a025000 | pass | 0.00
xgb1/39 | 4 | 0 | 4 | 0 - | 38 | b3 | en | dn | 1a026000 | pass | 0.00
xgb1/40 | 4 | 0 | 4 | 1 - | 39 | b3 | en | dn | 1a027000 | pass | 0.00
xgb1/41 | 4 | 0 | 4 | 6 - | 40 | b3 | en | dn | 1a028000 | pass | 0.00
xgb1/42 | 4 | 0 | 4 | 7 - | 41 | b3 | en | dn | 1a029000 | pass | 0.00
xgb1/43 | 4 | 0 | 4 | 4 - | 42 | b3 | en | dn | 1a02a000 | pass | 0.00
xgb1/44 | 4 | 0 | 4 | 5 - | 43 | b3 | en | dn | 1a02b000 | pass | 0.00
xgb1/45 | 4 | 0 | 4 | 10 - | 44 | b3 | en | dn | 1a02c000 | pass | 0.00
xgb1/46 | 4 | 0 | 4 | 11 - | 45 | b3 | en | dn | 1a02d000 | pass | 0.00
xgb1/47 | 4 | 0 | 4 | 8 - | 46 | b3 | en | dn | 1a02e000 | pass | 0.00
xgb1/48 | 4 | 0 | 4 | 9 - | 47 | b3 | en | dn | 1a02f000 | pass | 0.00
40gb2/1 | 5 | 1 | 0 | 2 - | 0 | b3 | dis | dn | 1a0f0000 | pass | 0.00
40gb2/2 | 5 | 1 | 0 | 1 - | 1 | b3 | dis | dn | 1a0f1000 | pass | 0.00
40gb2/3 | 6 | 1 | 1 | 2 - | 2 | b3 | dis | dn | 1a0f2000 | pass | 0.00
40gb2/4 | 6 | 1 | 1 | 1 - | 3 | b3 | dis | dn | 1a0f3000 | pass | 0.00
Done.

```

### Schritt 3: Identifizieren des ausgehenden kongetierten Ports

- Identifizieren Sie den überlasteten Ausgangsport mit VOQ-Zählern.
- Verwenden Sie die ASIC-Nummer in den **Zählern voq asic-num**, um herauszufinden, welcher Ausgangsport zu den Verlusten beiträgt.

```

nexus6001# sh plat soft qd info counters voq asic-num 1
+-----+-----+-----+-----+
| port | TRANSMIT | TAIL DROP | HEAD DROP |
+-----+-----+-----+-----+
Eth1/3
  QUEUE-3          3222876464          8545008          0
Eth1/4
  QUEUE-3          323451170              0              0
Eth1/6
  QUEUE-3          871362                0              0
SUP_HI
  QUEUE-0          2041                  0              0
+-----+-----+-----+-----+

```

### Szenerio 2. Eingabehilfen mit HOLB

Übungseinrichtung:





port	TRANSMIT	TAIL DROP	HEAD DROP
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+			
<b>Eth1/3</b>			
QUEUE-3	3893719464	164782171	0

Der Fluss, der beeinflusst werden muss, bewegt sich in Richtung 10.10.10.50. Der Strom zwischen 10.10.10.101 und 10.10.10.102 muss sauber sein.

Dies ist jedoch nicht der Fall. Ein festgeklemmter oder langsam ablaufender Ausgangsport kann dazu führen, dass alle Puffer an einem oder mehreren Eingangsports, die Datenverkehr an den Ausgangsport senden, ausgeschöpft werden, was sich auf den gesamten Datenverkehr dieser Eingangsports auswirkt. Das ist das klassische HOLB-Problem.

Spirent Traffic Generators zeigen, dass die Flüsse verworfen werden. Die Portnummern sind Spirent-Portnummern, wie im Bild gezeigt.

Traffic Aggregate View: Results 1

Streams > Detailed Stream Results | Change Result View | 1 of 1 | Select Tx Ports: All Ports | Select Rx Ports: All Ports

Change Counter Mode: Basic Mode | Resample

**Drops towards non congested ports**

Name/ID	Tx Port Name	Rx Port Names	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)	Reordered Count (Frames)
StreamBloc...	Port //4/11	Port //4/12	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	N/A	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	Port //4/11	1,307,568	1,100,070	223,516	16.887	1,100,070	0
StreamBloc...	Port //7/11	Port //7/12	461,229	275,398	172,495	38.512	275,398	0
StreamBloc...	Port //7/11	Port //4/11	1,844,950	1,100,058	664,699	37.665	1,100,058	0

## HOLB-Eindämmung: VOQ-Grenzwert aktivieren

Um dieses Szenario zu vermeiden, können die VOQs (nur für Unicast-Datenverkehr) mit einem festgelegten Grenzwert konfiguriert werden.

```
nexus6001(config)# hard unicast voq-limit
```

Nach der Konfiguration sind die Datenflüsse zu nicht überlasteten Ports nicht betroffen.

Die Spirent Traffic Generator-Ansicht nach der VOQ-Limit-Konfiguration ist wie im Bild gezeigt.

Streams > Detailed Stream Results | Change Result View | 1 of 1 | Select Tx Ports: All Ports | Select Rx Ports: All Ports

Change Counter Mode: Basic Mode | Resample

**There are no dropped packets**

Name/ID	Tx Port Name	Rx Port Names	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)	Reordered Count (Frames)
StreamBloc...	Port //4/11	Port //4/12	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	N/A	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	Port //4/11	1,348,359	1,133,953	230,398	16.887	1,133,953	0
StreamBloc...	Port //7/11	Port //7/12	474,821	461,488	0	0.000	461,488	0
StreamBloc...	Port //7/11	Port //4/11	1,899,318	1,133,940	685,182	37.665	1,133,940	0

Obwohl diese Konfiguration einen klaren Vorteil bietet, um Verwerfungen aufgrund von HOLB zu verhindern. Warum ist dies nicht die Standardkonfiguration?

In der Regel kann der Datenverkehr in einer Produktionsumgebung explodieren. Durch die Deaktivierung des VOQ-Grenzwerts können die Eingangspuffer einen Traffic-Microburst

absorbieren, ohne dass diese verloren gehen müssen.

Sofern die Situation die Aktivierung des VOQ-Limit nicht erfordert, wird empfohlen, den Standardwert zu verwenden, bei dem die VOQ deaktiviert bleibt.

## HOLB-Eindämmung: Klassifizierung des Datenverkehrs

Es gibt eine andere Methode, um HOLB durch die Verwendung der QoS-Konfiguration zu reduzieren. Da eingehende Rückwürfe nur eine bestimmte VOQ betreffen, die wiederum eine bestimmte QoS-Klasse ist, können Sie den betroffenen Datenverkehr einer anderen QoS-Gruppe einem nicht überlasteten Port zuordnen. In dieser Ausgabe wirken sich die eingehenden Rückwürfe auf die QoS-Gruppe 0-Klasse aus.

```
nexus6001# sh queuing int e1/4
Ethernet1/4 queuing information:
TX Queuing
  qos-group sched-type oper-bandwidth
    0         WRR         100

RX Queuing
qos-group 0 >>>> Drops in QOS 0
q-size: 100160, q-size-40g: 100160, HW MTU: 1500 (1500 configured)
drop-type: drop, xon: 0, xoff: 0
Statistics:
  Pkts received over the port          : 9612480
  Ucast pkts sent to the cross-bar     : 9587016
  Mcast pkts sent to the cross-bar     : 0
  Ucast pkts received from the cross-bar : 961249
  Pkts sent to the port                : 961261
Pkts discarded on ingress            : 3024 >>>>>>
  Per-priority-pause status           : Rx (Inactive), Tx (Inactive)
```

Die Konfiguration hier ordnet wichtigen Datenverkehr der QoS-Gruppe 2 zu.

1. Definieren Sie ACL für Datenverkehr, der nicht verworfen werden darf. Ziel ist es, diesen Datenverkehr in eine andere QoS-Gruppe zu klassifizieren, sodass er nicht beeinträchtigt wird.

```
ip access-list SINGLEFLOW
 statistics per-entry
 10 permit ip 10.10.10.101/32 10.10.10.102/32
```

## 2. QoS-Klassifizierung:

```
class-map type qos match-all FIX_AFFECTED_FLOW
 match access-group name SINGLEFLOW
policy-map type qos QOS_POLICY_FIX_AFFECTED_FLOW
 class FIX_AFFECTED_FLOW
   set qos-group 2
```

## 3. Netzwerk-QoS-Konfiguration:

```
class-map type network-qos QOSGRP2
 match qos-group 2
policy-map type network-qos NQOS-GRP2
 class type network-qos QOSGRP2
 class type network-qos class-default
```

4. Wenden Sie die verschiedenen Richtlinien an. Die Netzwerk-QoS ist systemweit, während die Klassifizierungsrichtlinie auf eine einzige Schnittstelle angewendet werden kann.

```
system qos
service-policy type network-qos NQOS-GRP2
```

```
interface Ethernet1/1
service-policy type qos input QOS_POLICY_FIX_AFFECTED_FLOW
```

5. Die Verwerfungen sind für die Klasse QoS-Gruppe-2 nicht sichtbar:

```
nexus6001(config-if)# sh queuing int e1/1
Ethernet1/1 queuing information:
TX Queuing
  qos-group  sched-type  oper-bandwidth
    0         WRR        100
    2         WRR        0
RX Queuing
qos-group 0
q-size: 100160, q-size-40g: 100160, HW MTU: 1500 (1500 configured)
drop-type: drop, xon: 0, xoff: 0
Statistics:
  Pkts received over the port          : 525111
  Ucast pkts sent to the cross-bar     : 327510
  Mcast pkts sent to the cross-bar     : 0
  Ucast pkts received from the cross-bar : 0
  Pkts sent to the port                : 0
  Pkts discarded on ingress           : 197868 >>>>
  Per-priority-pause status            : Rx (Inactive), Tx (Inactive)
qos-group 2
q-size: 100160, q-size-40g: 100160, HW MTU: 1500 (1500 configured)
drop-type: drop, xon: 0, xoff: 0
Statistics:
  Pkts received over the port          : 131413
  Ucast pkts sent to the cross-bar     : 132096
  Mcast pkts sent to the cross-bar     : 0
  Ucast pkts received from the cross-bar : 0
  Pkts sent to the port                : 0
  Pkts discarded on ingress           : 0 >>> No Drops
  Per-priority-pause status            : Rx (Inactive), Tx (Inactive)
```

## Zugehörige Informationen

- [Nexus Switches der Serie 6000 - QoS-Konfigurationsbeispiel](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)