

Veelgestelde vragen - Output Drops op Cisco Catalyst 9000 Series Switches

Inleiding

In dit document worden antwoorden gegeven op veelgestelde vragen over het verlagen van de uitvoer van switches uit de Cisco Catalyst 9000-reeks.

Voorwaarden

Vereisten

Cisco raadt u aan om een fundamenteel begrip te hebben van schakelconcepten, waaronder interface buffering en Quality of Service (QoS) configuraties.

Gebruikte componenten

Dit document is van toepassing op alle Cisco Catalyst 9000 Series-switches en is niet beperkt tot specifieke hardware- of softwareversies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Uitgangsdalingen treden op wanneer een interface-uitgang buffer is uitgeput, wat resulteert in pakketverlies en verslechterde netwerkprestaties. Veelvoorkomende oorzaken zijn netwerkcongestie, microbursts in het verkeer, verkeerde configuraties of hardwarebeperkingen. In dit document met veelgestelde vragen wordt ingegaan op veelgestelde vragen over het verlagen van de uitvoer van switches uit de Cisco Catalyst 9000-reeks. Het biedt richtlijnen voor het identificeren van onderliggende oorzaken, methoden voor probleemoplossing en aanbevolen praktijken om de efficiëntie en betrouwbaarheid van het netwerk te herstellen.

V. Wat zijn outputdalingen?

A. Output drops op Cisco Catalyst 9000-switches verwijzen naar het aantal pakketten dat wordt gedropt en niet wordt verzonden vanuit een interface, hoewel de pakketten door het apparaat zijn verwerkt. Dit gebeurt wanneer de uitvoerwachtrij van de interface vol wordt. De switch-interface heeft hardwarebuffers die pakketten tijdelijk opslaan voordat ze worden verzonden of doorgestuurd uit de poort. Wanneer de snelheid van het uitgaande verkeer hoger is dan de snelheid waarmee de hardware het kan verzenden, worden de buffers vol en worden eventuele extra pakketten die in de wachtrij aankomen, weggelaten.

V. Welke opdracht kan worden gebruikt om de uitvoer te controleren?

A. Gebruik de opdracht `show interfaces <interface>` en zoek naar de totale output drops counter, die het aantal pakketten aangeeft dat op de output queue van die interface is gevallen.

Voorbeeld:

```
<#root>
```

```
GigabitEthernet1/0/1 is up, line protocol is up (connected)  
  Input queue: 0/2000/0/0 (size/max/drops/flushes);
```

```
Total output drops: 3089
```

```
  Queueing strategy: fifo  
  Output queue: 0/40 (size/max)
```

V. Wat zijn de meest voorkomende oorzaken van de daling van de productie?

A. Uitgangsdalingen op Catalyst 9000-switches treden meestal op wanneer pakketten worden weggegooid voordat ze worden verzonden vanwege verschillende congestie- of configuratieproblemen. De meest voorkomende oorzaken zijn:

- Micro-bursts: plotselinge pieken in het verkeer met hoge intensiteit die zich gedurende milliseconden voordoen. Omdat standaard netwerkbewakingstools (zoals SNMP) vaak peilen met intervallen van 1 minuut of 5 minuten, zijn deze uitbarstingen vaak onzichtbaar

voor beheerssoftware, maar voldoende om de hardware-uitstroombuffers uit te putten.

- Overinschrijving: Wanneer de totale bandbreedte van het inkomende verkeer de capaciteit van de uitgaande interface aanzienlijk overschrijdt, is congestie onvermijdelijk. Dit komt vaak voor in scenario's waarbij meerdere hogesnelheidspoorten (bijvoorbeeld 10G) verkeer naar een enkele lagere snelheidspoort sturen (bijvoorbeeld 1G).
- Buffer Constraints: Elke interface heeft een eindige hoeveelheid hardware buffer ruimte. Wanneer de uitrijwachtrij zijn maximale capaciteit bereikt als gevolg van aanhoudende congestie, voert de switch 'tail-dropping' uit, waarbij alle volgende inkomende pakketten worden weggegooid totdat ruimte beschikbaar komt.
- Quality of Service (QoS) Misconfiguratie: verkeerd geconfigureerd QoS-beleid - met name agressief politiewerk of restrictieve vormgeving - kan leiden tot dalingen. Als een beleid is geconfigureerd om het verkeer onder de werkelijke koppelingcapaciteit te beperken, worden pakketten die die drempel overschrijden, verwijderd, zelfs als de fysieke koppeling niet is overbelast.
- Snelheid- en duplexmismatches: hoewel dit minder vaak voorkomt bij autoonderhandeling, kan een mismatch tussen de switch-poort en het aangesloten apparaat leiden tot inefficiënte transmissie, verhoogde botsingen (in half-duplex) en daaropvolgende wachtrijverzadiging.
- Flow Control (IEEE 802.3x): Als Flow Control (Stroomregeling) is ingeschakeld, kan de switch worden geïnstrueerd om de transmissie door het ontvangende apparaat te pauzeren. Als de pauzeframes vaak voorkomen, kan de uitgang van de switch buffers vullen, wat leidt tot druppels als de switch wacht om de transmissie te hervatten.
- Onbalans tussen poort en kanaal: als het verkeer in een EtherChannel/Port-Channel niet gelijkmatig over de koppelingen van de leden is verdeeld, kan één interface overbelast raken terwijl andere onderbenut blijven.

V. Wat zijn micro-uitbarstingen?

A. Micro-bursts zijn hoge intensiteit, korte duur verkeerspieken die zich voordoen over microseconden of milliseconden. Ze zorgen voor een daling van de uitvoer door de uitstroombuffers op Catalyst 9000-switches onmiddellijk uit te putten. Omdat standaard monitoringtools gemiddeld verkeer over langere intervallen verwerken, blijven deze bursts vaak onzichtbaar. Dit resulteert in pakketverlies, zelfs wanneer het gemiddelde gebruik van een interface ruim binnen de capaciteit lijkt. Bijgevolg zijn deze voorbijgaande pieken een primaire oorzaak van congestie in snelle netwerkomgevingen.

V. Zijn outputdalingen altijd een probleem?

A. Nee, output drops kunnen optreden tijdens korte verkeersexplosies, zelfs in gezonde netwerken. Moderne switches gebruiken buffergebaseerde wachtrijen en incidentele dalingen kunnen optreden zonder dat dit van invloed is op toepassingen. Druppels worden meestal problematisch wanneer:

- Druppels nemen voortdurend toe
- Toepassingen ervaren latentie of pakketverlies
- Toename TCP-hertransmissies
- Realtime toepassingen (VoIP/video) worden beïnvloed

V. Waarom treden er uitvoerdalingen op, zelfs als de interface niet volledig wordt gebruikt?

A. Er kunnen uitvoerdalingen optreden, zelfs wanneer het interfacegebruik ver onder de maximale bandbreedte van de koppeling ligt (bijvoorbeeld onder 1000 MBPS op een Gigabit-interface). Dit gebeurt omdat netwerkverkeer niet in een perfect vloeiende en continue stroom wordt verzonden. In een ideaal scenario wordt elke bit gelijkmatig over de link verzonden en verzenden alle apparaten verkeer met precies gesynchroniseerde intervallen. In echte netwerken verzenden apparaten echter verkeer wanneer ze dat nodig hebben. Als gevolg hiervan kunnen meerdere pakketten tegelijkertijd bij de switch aankomen en moeten ze via dezelfde uitgaande interface worden verzonden. Om deze situatie het hoofd te bieden, gebruiken switches hardwarebuffers op elke interface. Deze buffers slaan tijdelijk pakketten op die tegelijkertijd aankomen, zodat ze sequentieel over de link kunnen worden verzonden. Als het aantal pakketjes dat op een bepaald moment op de interface aankomt de beschikbare buffercapaciteit overschrijdt, kan de switch ze niet allemaal opslaan. Wanneer dit gebeurt, worden de overtollige pakketten weggelaten, wat resulteert in uitvoerdalingen.

Dit is de reden waarom het mogelijk is om outputdalingen te observeren, zelfs wanneer het gemiddelde bandbreedtegebruik relatief laag is (bijvoorbeeld 300 MBPS op een 1 GBPS-interface). Het gemiddelde gebruik kan laag lijken, maar korte uitbarstingen van verkeer kunnen tijdelijk het vermogen van de interface om pakketten te verzenden overschrijden of de beschikbare buffercapaciteit overschrijden.

Het is ook belangrijk op te merken dat de waarden van het interfacegebruik die worden weergegeven via SNMP-bewakingsprogramma's of de opdracht interface tonen gebaseerd zijn op gemiddelde verkeersmetingen over intervallen zoals 30 seconden of 5 minuten. Deze gemiddelden geven geen zeer korte verkeerspieken weer die binnen milliseconden kunnen optreden.

V. Hoe kan ik uitvoerdalingen controleren zonder de verbindingssnelheid te verhogen?

A. U kunt uitvoerdalingen op Catalyst 9000-switches beheren en verminderen met behulp van

verschillende technieken zonder de werkelijke verbindingssnelheid te verhogen:

- Verhoog de SoftMax Multiplier (Quick Mitigation): Om het aantal buffers te verhogen dat een wachtrij kan aanvragen uit de gedeelde bufferpool, kunt u de SoftMax-drempel aanpassen met behulp van de globale configuratie opdracht `qos queue-softmax-multiplier <100-1200>`. De standaardwaarde is 100. Als u deze waarde instelt op 1200, wordt het vermogen van de wachtrij om microbursts te absorberen met een factor 12 verhoogd in vergelijking met de standaardconfiguratie.

Met deze opdracht worden de drempelwaarden voor de poortwachtrij verhoogd, zodat de wachtrij extra buffereenheden uit de gedeelde bufferpool kan gebruiken wanneer dat nodig is. Dit wordt vaak gebruikt als een snelle mitigatietechniek om outputdalingen veroorzaakt door verkeersuitbarstingen te verminderen. Omdat buffers echter gedeelde bronnen zijn, gaat de configuratie ervan uit dat microbursts niet gelijktijdig op alle poorten voorkomen.

Wijziging van de buffer per wachtrij (afstemming van het QoS-beleid): als de SoftMax-multiplier onvoldoende is, kan de toewijzing van de buffer op het wachtrijniveau worden afgestemd met behulp van QoS-beleidskaarten. Hierdoor kunnen beheerders meer bufferruimte toewijzen aan specifieke verkeersklassen, bufferverhoudingen in wachtrijen wijzigen en prioriteitswachtrijen voor kritisch verkeer configureren. Deze aanpak is nuttig wanneer specifieke verkeerstypen speciale bufferbronnen vereisen of wanneer verkeersprofielen aanzienlijk variëren.

Voorbeeld:

```
policy-map QOS-POLICY
class VOICE
  priority level 1
  queue-buffers ratio 50
class class-default
  queue-buffers ratio 50
```

- Implementeer Quality of Service (QoS): het helpt pakketdalingen te beheersen door prioriteit te geven aan kritisch netwerkverkeer tijdens perioden van congestie. Het stelt netwerken in staat om prioriteit te geven aan latentiegevoelig verkeer zoals spraak en video, het verkeer van het controlevliegtuig te beschermen en ervoor te zorgen dat belangrijke gegevens worden verzonden voordat verkeer met een lagere prioriteit wordt verzonden. Typische QoS-mechanismen omvatten verkeersclassificatie, prioritering van wachtrijen, toewijzing van wachtrijbuffers en congestiebeheer. Door deze technieken toe te passen, kan het netwerk ervoor zorgen dat minder belangrijk verkeer eerst wordt weggelaten, waardoor bedrijfskritieke toepassingen worden beschermd en de algehele netwerkprestaties worden gehandhaafd.
- Verkeersvorming: Configureer de vormgeving van de uitgang op de interface om

verkeersbreuken glad te strijken. Door de transmissiesnelheid iets onder de fysieke lijnsnelheid te beperken, dwingt u het verkeer te bufferen en met een consistente, voorspelbare snelheid te verzenden. Dit voorkomt het staartvalgedrag veroorzaakt door plotselinge, snelle micro-uitbarstingen.

Voorbeeld:

```
policy-map SHAPE-POLICY
class class-default
shape average
```

- Load Distribution optimaliseren (Port-Channel Balancing): in een EtherChannel- of Port-Channel-configuratie kan ongelijke hashing ervoor zorgen dat specifieke lidlinks overbelast raken, terwijl andere links onderbenut blijven. Door het optimaliseren van load-balancing algoritmen, zorgt u ervoor dat het verkeer gelijkmatig wordt verdeeld over alle lid links, die congestie op individuele interfaces voorkomt en vermindert output drops.

Voorbeeld:

```
port-channel load-balance src-dst-ip
```

V. Wat is de ultieme oplossing voor outputdruppels?

A. De meest effectieve oplossingen om outputdruppels te elimineren zijn:

- Verhoog de lijnsnelheid van de interface: Upgrade de interfacesnelheid om een hogere bandbreedte voor uitstappen te bieden en overinschrijving te verminderen. Ga bijvoorbeeld van een 1G-interface naar een 10G-interface, indien beschikbaar op de switch.
- Port Bundling (EtherChannel) gebruiken: Meerdere fysieke koppelingen aggregeren in één logische koppeling met behulp van poortbundeling, op voorwaarde dat het aangesloten apparaat deze functie ondersteunt. Dit verhoogt de totale bandbreedte en helpt de verkeersbelasting te verdelen.
- Hardware-upgrade indien nodig: als er geen hogere-snelheidsinterface beschikbaar is op de switch en de poortbundeling niet wordt ondersteund door het aangesloten apparaat, overweeg dan om het hardwareplatform te upgraden naar een met een hogere opslagcapaciteit of grotere buffers.

V. Hoe kunnen wachtrijstatistieken worden gecontroleerd op een interface?

A. Voor Catalyst 9000-switches kunnen gedetailleerde hardwarestatistieken worden gecontroleerd met de opdracht Toon platformhardware gevoed door actieve Qos-wachtrijstatusinterface <poort>. Deze opdracht biedt gedetailleerde statistieken, waaronder buffergebruik, het aantal wachtrijen en valtelers per wachtrij op de opgegeven interface, waardoor de prestaties van de wachtrij kunnen worden bewaakt en congestie of pakketdalingen kunnen worden geïdentificeerd.

Voorbeeld:

<#root>

```
show platform hardware fed switch active qos queue stats interface Gig 1/0/1
```

DATA Port:0 Enqueue Counters

Q	Buffers (Count)	Enqueue-TH0 (Bytes)	Enqueue-TH1 (Bytes)	Enqueue-TH2 (Bytes)	Qpolicer (Bytes)
---	-----------------	---------------------	---------------------	---------------------	------------------

0	0	0	0		
---	---	---	---	--	--

384251797

1	0	0	0		
---	---	---	---	--	--

488393930284

0

...

DATA Port:0 Drop Counters

Q	Drop-TH0 (Bytes)	Drop-TH1 (Bytes)	Drop-TH2 (Bytes)	SBufDrop (Bytes)
---	------------------	------------------	------------------	------------------

0	0	0	0	0
---	---	---	---	---

1	0	0		
---	---	---	--	--

192308101

0

0

0

...

V. Hoe kunt u bevestigen of QoS de oorzaak is van een daling van de uitvoer?

A. Om te controleren of QoS verantwoordelijk is voor de output drops, controleert u de QoS-beleidsstatistieken met behulp van de opdracht `show policy-map interface <interface>` en wachrijtellers. Als valtellers toenemen onder een specifieke QoS-klasse, kunnen de dalingen worden veroorzaakt door QoS-wachtrijlimieten of politiewerk. Verwijder, indien mogelijk, tijdens een onderhoudsvenster tijdelijk het QoS-beleid uit de interface met behulp van de opdracht `no service-policy <naam van het beleid>` en controleer of de uitvoerdalingen doorgaan. Als druppels stoppen na het verwijderen van het beleid, is het waarschijnlijk dat de QoS-configuratie bijdraagt aan de druppels.

Voorbeeld:

```
<#root>
```

```
sh policy-map interface gigabitEthernet 1/0/1
```

```
GigabitEthernet1/0/1
Service-policy output: TEST
Class-map: class-default (match-any)
 0 packets
Match: any
Queueing
```

```
(total drops) 587230
```

```
(bytes output) 834545
```

```
...
```

V. Kunnen er uitvoerdalingen optreden op hogesnelheidsinterfaces zoals 10G of 40G?

A. Ja, zelfs hogesnelheidsinterfaces zoals 10G of 40G kunnen uitvoerdalingen ervaren wanneer meerdere stromen met hoge snelheid op één poort convergeren, waardoor de interfacebuffers overweldigd raken. Bovendien kunnen microbursts - korte uitbarstingen van verkeer die de interfacebandbreedte overschrijden - snel poortbuffers uitputten en leiden tot pakketdruppels.

V. Kunnen uitvoerdalingen worden veroorzaakt door hardwarefouten?

A. Uitgangsdalingen worden over het algemeen niet veroorzaakt door hardwarefouten. Ze zijn meestal het gevolg van verkeersopstoppingen, waarbij de interfacebuffers overweldigd raken door hoge verkeerssnelheden of microbursts. Hardwaregerelateerde dalingen kunnen optreden, maar zijn meestal gekoppeld aan specifieke foutcondities, die zeldzaam zijn in vergelijking met congestiegerelateerde dalingen. Daarom worden outputdalingen meestal geassocieerd met netwerkverkeersomstandigheden in plaats van hardwarestoringen. Fouten in de bewakingsinterface, zoals FCS/CRC-fouten, kunnen helpen hardwareproblemen te identificeren indien aanwezig, maar deze verschillen van uitvoerdalingen die worden veroorzaakt door congestie.

V. Kunnen softwarebugs leiden tot een daling van de uitvoer?

A. Outputdalingen als gevolg van softwarefouten zijn zeer zeldzaam en meestal cosmetisch en hebben geen substantiële invloed op het verkeer. De meeste output dalingen worden voornamelijk veroorzaakt door verkeerscongestie en buffer uitputting.

V. Kan ECMP of load balancing de congestie verminderen?

A. Ja, Equal-Cost Multi-Path (ECMP)-routing en taakverdeling verminderen congestie door het verkeer gelijkmatig te verdelen over meerdere paden met gelijke kosten naar een bestemming. Deze aanpak verhoogt het bandbreedtegebruik en voorkomt dat één pad een knelpunt wordt.

V. Hebben outputdalingen een andere invloed op het UDP-verkeer dan op TCP?

A. Ja, uitvoerdalingen hebben een andere invloed op UDP-verkeer dan TCP, omdat UDP een verbindingsloos protocol is dat verloren pakketten niet opnieuw verzendt, dus elk pakketverlies heeft directe invloed op toepassingen zoals spraak of video, die afhankelijk zijn van tijdige levering. TCP bevat daarentegen retransmissiemechanismen die proberen verloren pakketten te herstellen, waardoor de impact van druppels wordt beperkt. Daarom kunnen outputdalingen een meer merkbare verslechtering veroorzaken in UDP-gebaseerde realtime toepassingen, omdat verloren pakketten niet worden hersteld en kunnen leiden tot kwaliteitsproblemen.

V. Wat is het verschil tussen invoerdruppels en uitvoerdruppels?

A. Input drops op interfaces treden meestal op wanneer de invoerwachtrijen overweldigd raken en pakketten niet snel genoeg kunnen verwerken, waardoor selectief pakketverlies ontstaat op basis van het wachtrijalgoritme. Uitgangsdalingen gebeuren wanneer pakketten worden weggelaten

terwijl ze een interface verlaten vanwege congestie in de uitvoerwachtrij of bufferuitputting. Inputdalingen zijn gerelateerd aan ingresverwerkingslimieten, terwijl outputdalingen voornamelijk worden veroorzaakt door egrescongestie en bufferoverloop. Deze dalingen kunnen worden beïnvloed door factoren zoals verkeersexplosies, platformbeperkingen en Quality of Service (QoS)-configuraties die congestie en buffertoewijzing beheren.

V. Kunnen grote back-uptaken leiden tot een daling van de uitvoer?

A. Ja, grote back-uptaken, zoals back-ups van gegevens, replicatie of bulkoverdrachten, genereren vaak bursty-verkeer dat interfacebuffers kan overweldigen, wat leidt tot uitvoerdalingen. Deze uitbarstingen kunnen tijdelijke congestie op de uitgang interface veroorzaken, vooral wanneer de uitgaande bandbreedte lager is dan de inkomende verkeerssnelheid of wanneer meerdere hoge snelheid stromen convergeren op een enkele poort.

V. Hoe kan ik vaststellen of verkeersbreuken leiden tot een daling van de output?

A. Om te bevestigen dat de uitvoer is gedaald als gevolg van verkeersexplosies, kunt u een SPAN-sessie in combinatie met Wireshark gebruiken om het uitgaand verkeer op de betreffende interface vast te leggen en te analyseren terwijl de uitvoer daalt. Observeer deze stappen om te controleren of de uitvoer daalt als gevolg van verkeersinfarcten.

- Sluit een laptop waarop Wireshark is geïnstalleerd aan op een ongebruikte poort op de switch.
- Configureer SPAN op de switch om het inkomverkeer van de uitvoer te weerspiegelen naar de poort waarop de laptop is aangesloten.

```
monitor session 1 source interface
```

```
Tx
```

```
monitor session 1 destination interface
```

```
Replace
```

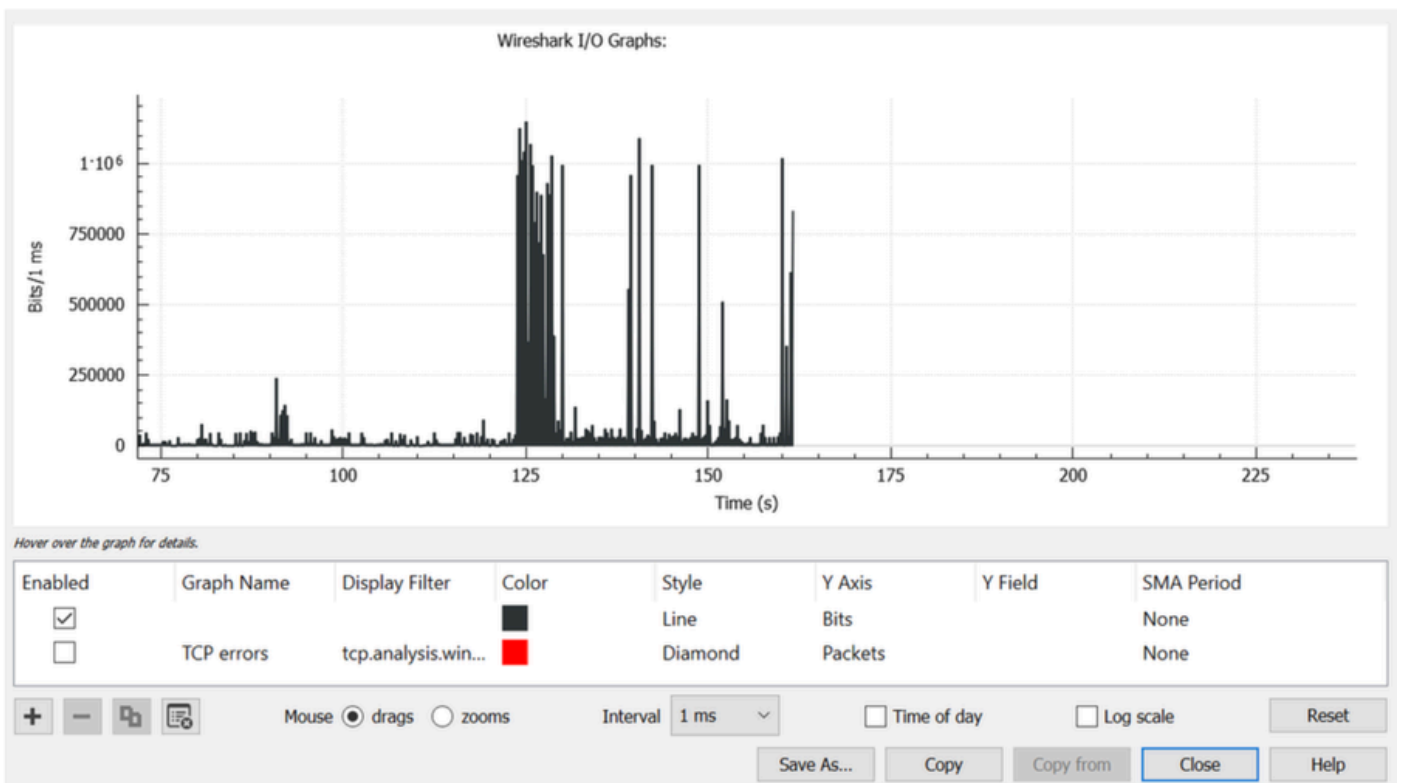
```
with the interface where output drops are seen for the source.
```

Replace

with the interface connected to the laptop for the destination.

- Start de SPAN-opname op de switch terwijl de uitvoerdalingen actief worden verhoogd om ervoor te zorgen dat relevant verkeer wordt vastgelegd.
- Open het opnamebestand in Wireshark en ga vervolgens naar Statistieken > I/O-grafiek.
- Wijzig het interval van de standaard 1 seconde in 1 milliseconde (1 ms).
- Klik op Reset om de grafiek met het nieuwe interval te vernieuwen.
- De grafiek geeft het verkeer weer in bits per milliseconde.

Zoek naar verkeerspieken die de doorstuursnelheid van de interface op een schaal van milliseconden overschrijden (bijvoorbeeld 1.000.000 bits/ms voor een 1 GBPS-interface). Wanneer het verkeer deze doorstuursnelheid overschrijdt, buffert de switch pakketten, wat congestie en uitvoerdalingen kan veroorzaken. Identificeer verkeerspieken (microbursts) door pieken te observeren gevolgd door perioden van weinig of geen verkeer. In Wireshark selecteert het klikken op een piek de bijbehorende pakketten, waardoor verdere analyse van het verkeer dat de druppels heeft veroorzaakt mogelijk wordt. De volgende afbeelding toont de bijgewerkte I / O-grafiek voor een interface die uitvoerdalingen heeft ervaren.



Belangrijke overwegingen

- Zorg ervoor dat de SPAN-bron- en bestemmingspoorten dezelfde of compatibele snelheden hebben om te voorkomen dat er extra druppels worden toegevoegd.
- Leg verkeer vast terwijl de outputdalingen actief toenemen om relevante uitbarstingen vast te leggen.
- Embedded Packet Capture (EPC) wordt niet aanbevolen voor dit doel, omdat het de opnamesnelheden beperkt en bursts kan missen.

Veel voorkomende misvattingen over outputdalingen

Misvatting: Elke output drop betekent dat het netwerk niet goed functioneert.

Realiteit: Een klein aantal uitvoerdalingen is normaal in hogesnelheidsnetwerken als gevolg van microbursts of korte verkeerspieken.

Misvatting: Als het gebruik van de interface laag is, mogen er geen druppels gebeuren.

Realiteit: Het gebruik wordt gemeten als een gemiddelde over de tijd. Microbursts kunnen tijdelijk de interfacebandbreedte overschrijden, waardoor er zelfs dalingen optreden wanneer het gemiddelde gebruik laag is.

Misvatting: Uitgangsdalingen betekenen dat de hardware van de switch defect is.

Realiteit: Outputdalingen worden meestal veroorzaakt door verkeerscongestie of bursty-verkeer, niet door hardwareproblemen.

Misvatting: Het verhogen van de buffertoewijzing zal alle dalingen voorkomen.

Realiteit: Buffers absorberen slechts tijdelijke uitbarstingen. Aanhoudende congestie zal nog steeds resulteren in pakketdruppels.

Misvatting: Alleen 1G-interfaces ervaren uitvoerdalingen.

Realiteit: Drops kunnen optreden op 10G-, 25G-, 40G- of hogere snelheidsinterfaces wanneer het verkeer de beschikbare bandbreedte of buffercapaciteit overschrijdt.

Misvatting: QoS moet alle druppels elimineren / pakketverlies voorkomen.

Realiteit: QoS geeft prioriteit aan belangrijk verkeer, maar het kan opzettelijk verkeer met een lagere prioriteit laten vallen tijdens congestie.

Misvatting: Elke daling van de uitvoer zal de impact van de gebruiker veroorzaken.

Realiteit: Veel toepassingen maken gebruik van TCP-hertransmissie, die kan herstellen van incidentele pakketdruppels zonder merkbare impact.

Misvatting: Drops treden alleen op wanneer interfaces 100% gebruik bereiken.

Realiteit: Drops kunnen optreden tijdens korte uitbarstingen van verkeer, zelfs als het gemiddelde gebruik laag blijft.

Misvatting: QoS-configuratie is altijd de oorzaak van dalingen.

Realiteit: De meeste dalingen worden veroorzaakt door verkeerspatronen of overinschrijving, niet door QoS-beleid.

Misvatting: Een gezond netwerk mag nooit een daling van de output hebben.

Realiteit: In krachtige switchomgevingen worden incidentele dalingen verwacht en normaal.

Gidsen voor probleemoplossing

- [Afwijzingen in de uitvoer op Catalyst 9000-switches oplossen](#)
- [Inzicht in wachtrijbuffertoewijzing op Catalyst 9000-Switches](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.