Häufig gestellte Fragen - Ausgabekürzungen bei Cisco Catalyst Switches der Serie 9000

Einleitung

Dieses Dokument enthält Antworten auf häufig gestellte Fragen zu Ausgabekürzungen bei Cisco Catalyst Switches der Serie 9000.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit den Switching-Konzepten vertraut zu machen, einschließlich Schnittstellenpufferung und Quality of Service (QoS)-Konfigurationen.

Verwendete Komponenten

Dieses Dokument gilt für alle Cisco Catalyst Switches der Serie 9000 und ist nicht auf bestimmte Hardware- oder Softwareversionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Wenn der Ausgangspuffer einer Schnittstelle erschöpft ist, geht die Ausgabe verloren, was zu Paketverlusten und einer Beeinträchtigung der Netzwerkleistung führt. Häufige Ursachen sind Netzwerküberlastungen, Microbursts im Datenverkehr, Fehlkonfigurationen oder Hardware-Einschränkungen. Dieses FAQ-Dokument beantwortet häufige Fragen zu Ausgängen bei Cisco Catalyst Switches der Serie 9000. Es bietet Hilfestellung bei der Identifizierung von Ursachen, Fehlerbehebungsmethoden und empfohlenen Vorgehensweisen zur Wiederherstellung der Netzwerkeffizienz und -zuverlässigkeit.

F. Was sind Ausgabefehler?

A.: Ausgabe-Drops auf Cisco Catalyst Switches der Serie 9000 beziehen sich auf die Anzahl der Pakete, die verworfen und nicht über eine Schnittstelle übertragen werden, obwohl die Pakete vom Gerät verarbeitet wurden. Dies geschieht, wenn die Ausgabewarteschlange der Schnittstelle voll wird. Die Switch-Schnittstelle verfügt über Hardware-Puffer, die Pakete vorübergehend speichern, bevor sie übertragen oder über den Port weitergeleitet werden. Wenn die Rate des ausgehenden Datenverkehrs die Rate übersteigt, mit der die Hardware den Datenverkehr übertragen kann, sind die Puffer voll, und alle zusätzlichen Pakete, die in der Warteschlange ankommen, werden verworfen.

Frage: Welcher Befehl kann verwendet werden, um Ausgabeverwerfungen zu überprüfen?

A. Verwenden Sie den Befehl show interfaces <Schnittstelle> und suchen Sie nach dem Zähler für die Gesamtzahl verworfener Pakete, der die Anzahl der in der Ausgabewarteschlange dieser Schnittstelle verworfenen Pakete angibt.

Beispiel:

<#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)
```

F. Was sind die häufigsten Ursachen für Leistungseinbrüche?

A.: Die Ausgabe auf Catalyst 9000-Switches fällt in der Regel dann aus, wenn Pakete vor der Übertragung aufgrund verschiedener Engpässe oder Konfigurationsprobleme verworfen werden. Zu den häufigsten Ursachen gehören:

- Datenverkehr-Microbursts: Plötzliche, besonders intensive Spitzen im Datenverkehr, die über Millisekunden auftreten. Da Standard-Netzwerküberwachungstools (wie SNMP)

Abfragen häufig in Intervallen von einer Minute oder von fünf Minuten durchführen, sind diese Bursts für die Managementsoftware häufig nicht sichtbar, reichen aber aus, um die Hardware-Ausgangspuffer zu erschöpfen.

- Überbelegung: Wenn die Gesamtbandbreite des eingehenden Datenverkehrs die Kapazität der ausgehenden Schnittstelle deutlich übersteigt, ist eine Überlastung unvermeidlich. Dies ist in Szenarien üblich, in denen mehrere Hochgeschwindigkeits-Ports (z. B. 10G) Datenverkehr an einen einzelnen Port mit geringerer Geschwindigkeit senden (z. B. 1G).
- Pufferbeschränkungen: Jede Schnittstelle verfügt über eine begrenzte Menge an Hardware-Pufferspeicher. Wenn die maximale Kapazität der Ausgangswarteschlange aufgrund anhaltender Überlastung erreicht ist, führt der Switch ein Tail-Dropping durch, bei dem alle nachfolgenden eingehenden Pakete verworfen werden, bis Speicherplatz verfügbar ist.
- Falsche QoS-Konfiguration (Quality of Service): Falsch konfigurierte QoS-Richtlinien - insbesondere aggressives Policing oder restriktives Shaping - können zu Drops führen. Wenn eine Richtlinie so konfiguriert ist, dass der Datenverkehr unterhalb der tatsächlichen Verbindungskapazität begrenzt wird, werden Pakete, die diesen Grenzwert überschreiten, verworfen, selbst wenn die physische Verbindung nicht überlastet ist.
- Geschwindigkeits- und Duplexdiskrepanzen: Obwohl dies bei modernen Auto-Negotiation-Verfahren seltener der Fall ist, kann eine Diskrepanz zwischen dem Switch-Port und dem angeschlossenen Gerät zu ineffizienter Übertragung, verstärkten Kollisionen (im Halbduplex-Modus) und einer nachfolgenden Warteschlangensättigung führen.
- Flusskontrolle (IEEE 802.3x): Wenn die Flusssteuerung aktiviert ist, kann der Switch angewiesen werden, die Übertragung vom Empfangsgerät anzuhalten. Wenn die Pausen-Frames häufig auftreten, kann sich der Ausgang der Switch-Puffer füllen, was dazu führt, dass der Switch abwartet, bis die Übertragung wieder aufgenommen wird.
- Port-Channel-Ungleichgewicht: Wenn der Datenverkehr in einem EtherChannel/Port-Channel nicht gleichmäßig auf die Mitglieder-Links verteilt wird, kann es an einer Schnittstelle zu Überlastungen kommen, während andere nicht voll ausgelastet sind.

F. Was sind Mikro-Bursts?

Antwort: Mikro-Bursts sind Datenverkehrsspitzen mit hoher Intensität und kurzer Dauer, die sich über Mikrosekunden oder Millisekunden erstrecken. Sie verursachen Leistungseinbußen, indem die Ausgangshardwarepuffer der Catalyst Switches der Serie 9000 sofort ausgelastet werden. Da Standard-Überwachungstools den Datenverkehr über längere Zeiträume hinweg durchschnittlich überwachen, bleiben diese Spitzen oft unsichtbar. Dies führt zu Paketverlusten, selbst wenn die durchschnittliche Auslastung einer Schnittstelle deutlich unter der Kapazität zu liegen scheint. Daher sind diese vorübergehenden Spitzen eine der Hauptursachen für Überlastungen in Hochgeschwindigkeits-Netzwerkumgebungen.

F. Sind Ausgabefehler immer ein Problem?

Antwort: Nein, die Ausgabe kann selbst in intakten Netzwerken bei kurzen Datenverkehrsspitzen

absinken. Moderne Switches verwenden pufferbasierte Warteschlangen, und gelegentliche Unterbrechungen können auftreten, ohne dass Anwendungen beeinträchtigt werden. Drops werden in der Regel dann problematisch, wenn:

- Tropfen nehmen kontinuierlich zu
- Bei Anwendungen treten Latenz oder Paketverlust auf
- TCP-Neuübertragungen nehmen zu
- Echtzeitanwendungen (VoIP/Video) sind betroffen

F. Warum werden die Ausgaben auch dann verworfen, wenn die Schnittstelle nicht voll ausgelastet ist?

Antwort: Die Ausgabe fällt auch dann ab, wenn die Schnittstellennutzung deutlich unter der maximalen Bandbreite der Verbindung liegt (z. B. unter 1000 Mbit/s an einer Gigabit-Schnittstelle). Dies liegt daran, dass der Netzwerkverkehr nicht reibungslos und ohne Unterbrechung übertragen wird. Im Idealfall wird jedes Bit gleichmäßig über die Verbindung übertragen, und alle Geräte senden den Datenverkehr in genau synchronisierten Intervallen. In realen Netzwerken übertragen Geräte jedoch Datenverkehr, wann immer sie dies benötigen. Dadurch können mehrere Pakete gleichzeitig am Switch ankommen und müssen über dieselbe ausgehende Schnittstelle übertragen werden. Um diese Situation zu bewältigen, verwenden die Switches auf jeder Schnittstelle einen Hardwarepuffer. Diese Puffer speichern vorübergehend Pakete, die gleichzeitig eintreffen, sodass sie sequenziell über die Verbindung übertragen werden können. Wenn die Paketmenge, die zu einem bestimmten Zeitpunkt an der Schnittstelle eingeht, die verfügbare Pufferkapazität überschreitet, kann der Switch nicht alle Pakete speichern. In diesem Fall werden die überschüssigen Pakete verworfen, was zu Ausgabeverringerungen führt.

Aus diesem Grund können auch bei einer relativ geringen durchschnittlichen Bandbreitennutzung (z. B. 300 Mbit/s an einer 1-GBIT/s-Schnittstelle) Leistungseinbrüche beobachtet werden. Die durchschnittliche Auslastung kann gering erscheinen, aber kurze Datenverkehrsspitzen können die Fähigkeit der Schnittstelle zum Übertragen von Paketen vorübergehend überschreiten oder die verfügbare Pufferkapazität überschreiten.

Außerdem ist zu beachten, dass die Schnittstellennutzungswerte, die über SNMP-Überwachungstools oder den Befehl show interface angezeigt werden, auf durchschnittlichen Datenverkehrsmessungen in Intervallen von z. B. 30 Sekunden oder 5 Minuten basieren. Diese Durchschnittswerte spiegeln keine sehr kurzen Datenverkehrsspitzen wider, die innerhalb von Millisekunden auftreten können.

F. Wie kann ich die Ausgabeverringerungen kontrollieren, ohne

die Verbindungsgeschwindigkeit zu erhöhen?

A.: Sie können die Ausfallzeiten auf Catalyst 9000-Switches mithilfe verschiedener Techniken verwalten und reduzieren, ohne die Geschwindigkeit der physischen Verbindung zu erhöhen:

- Increase the SoftMax Multiplier (Quick Mitigation): Um die Anzahl der Puffer zu erhöhen, die eine Warteschlange vom gemeinsamen Pufferpool anfordern kann, können Sie den SoftMax-Schwellenwert mit dem globalen Konfigurationsbefehl qos queue-softmax-multiplier <100-1200> anpassen. Der Standardwert ist 100. Wenn Sie diesen Wert auf 1200 setzen, kann die Warteschlange im Vergleich zur Standardkonfiguration um den Faktor 12 Microbursts absorbieren.

  Mit diesem Befehl werden die Schwellenwerte für Portwarteschlangen erhöht, sodass die Warteschlange bei Bedarf zusätzliche Puffereinheiten aus dem gemeinsamen Pufferpool nutzen kann. Diese Methode wird häufig als Methode zur schnellen Abwehr verwendet, um die durch Datenverkehrsspitzen verursachten Verluste bei der Ausgabe zu reduzieren. Da Puffer jedoch gemeinsam genutzte Ressourcen sind, wird in der Konfiguration davon ausgegangen, dass die Mikrospitzen nicht auf allen Ports gleichzeitig auftreten.

Per-Queue Buffer Modification (QoS Policy Tuning): Wenn der SoftMax-Multiplikator nicht ausreicht, kann die Pufferzuweisung mithilfe von QoS Policy-Maps auf Warteschlangenebene optimiert werden. Auf diese Weise können Administratoren mehr Pufferspeicher bestimmten Datenverkehrsklassen zuweisen, die Warteschlangenpufferverhältnisse ändern und Prioritätswarteschlangen für kritischen Datenverkehr konfigurieren. Dieser Ansatz ist nützlich, wenn bestimmte Datenverkehrstypen dedizierte Pufferressourcen benötigen oder wenn sich die Datenverkehrsprofile erheblich unterscheiden.

Beispiel:

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

- Implementierung von Quality of Service (QoS): Sie hilft, Paketverluste zu kontrollieren, indem sie kritischen Netzwerkverkehr während Zeiten der Überlastung priorisiert. Es ermöglicht Netzwerken, latenzempfindlichen Datenverkehr wie Sprache und Video zu priorisieren, den Steuerungsebenen-Datenverkehr zu schützen und sicherzustellen, dass wichtige Daten vor Datenverkehr mit geringerer Priorität übertragen werden. Typische QoS-Mechanismen umfassen die Klassifizierung des Datenverkehrs, die Priorisierung von

Warteschlangen, die Zuweisung von Warteschlangenpuffern und das Engpassmanagement. Durch die Anwendung dieser Techniken kann das Netzwerk sicherstellen, dass weniger wichtiger Datenverkehr zuerst verworfen wird. Dies trägt zum Schutz geschäftskritischer Anwendungen und zur Aufrechterhaltung der Netzwerkleistung bei.

- Traffic Shaping: Konfigurieren Sie das Egress-Shaping an der Schnittstelle, um Datenverkehrsspitzen zu glätten. Wenn Sie die Übertragungsrate geringfügig unter der physischen Leitungsrate begrenzen, erzwingen Sie eine Pufferung des Datenverkehrs und die Übertragung mit einer konsistenten, vorhersehbaren Geschwindigkeit. Dadurch wird das durch plötzliche Hochgeschwindigkeits-Mikro-Bursts verursachte Tail-Drop-Verhalten verhindert.

Beispiel:

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

- Optimierung der Lastverteilung (Port-Channel-Ausgleich): In einer EtherChannel- oder Port-Channel-Konfiguration kann uneinheitliches Hashing zu Engpässen bei bestimmten Mitglieds-Links führen, während andere nicht ausgelastet sind. Durch die Optimierung von Load-Balancing-Algorithmen stellen Sie sicher, dass der Datenverkehr gleichmäßig auf alle Member-Links verteilt wird, wodurch Engpässe an einzelnen Schnittstellen vermieden und Ausgabekürzungen reduziert werden.

Beispiel:

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

F. Was ist die ultimative Lösung für Output Drops?

A. Die effektivsten Lösungen zum Eliminieren von Output-Drops sind:

- Increase Interface Line Speed: Aktualisieren Sie die Schnittstellengeschwindigkeit, um eine höhere Ausgangsbandbreite bereitzustellen und die Überbelegung zu reduzieren. So können Sie beispielsweise von einer 1G-Schnittstelle zu einer 10G-Schnittstelle wechseln, sofern diese auf dem Switch verfügbar ist.

- Verwendung von Port-Bündelung (EtherChannel): Bündelung mehrerer physischer Verbindungen zu einer einzigen logischen Verbindung unter Verwendung von Port-Bündelung, vorausgesetzt, das angeschlossene Gerät unterstützt diese Funktion. Dies erhöht die Gesamtbandbreite und verteilt die Datenverkehrslast.
- Falls erforderlich Hardware-Upgrade: Wenn auf dem Switch keine Schnittstelle mit höherer Geschwindigkeit verfügbar ist und die Port-Bündelung vom angeschlossenen Gerät nicht unterstützt wird, sollten Sie ein Upgrade der Hardwareplattform auf eine Plattform mit höherer Kapazität oder größeren Puffern in Erwägung ziehen.

F. Wie können Warteschlangenstatistiken auf einer Schnittstelle überprüft werden?

A.: Für Catalyst 9000-Switches können detaillierte Statistiken zu Hardwarewarteschlangen mit dem Befehl show platform hardware fed active qos queue stats interface <Port> überprüft werden. Dieser Befehl stellt detaillierte Statistiken bereit, einschließlich der Puffernutzung, der Anzahl von Warteschlangen und der Zähler für Verwerfungen pro Warteschlange an der angegebenen Schnittstelle, die dabei helfen, die Leistung der Warteschlange zu überwachen und Überlastungen oder Paketverluste zu identifizieren.

Beispiel:

<#root>

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

```
DATA Port:0 Enqueue Counters
-------------------------------------------------------------------------------------------
Q Buffers          Enqueue-TH0          Enqueue-TH1          Enqueue-TH2             Qpolicer
  (Count)              (Bytes)              (Bytes)              (Bytes)              (Bytes)
- ------- -------------------- -------------------- -------------------- --------------------
0       0                    0                    0

384251797

                  0
1       0                    0                    0

488393930284

                  0
...
DATA Port:0 Drop Counters
-------------------------------------------------------------------------------------------
Q             Drop-TH0             Drop-TH1             Drop-TH2             SBufDrop
```

```
               (Bytes)              (Bytes)              (Bytes)              (Bytes)
- -------------------- -------------------- -------------------- -------------------- ----------
0                     0                    0                    0                    0
1                     0                    0

192308101

                    0                    0                    0
...
```

Frage: Wie kann überprüft werden, ob die Ausgabe durch QoS beeinträchtigt wird?

A. Um zu überprüfen, ob QoS für die Verwerfung von Ausgaben verantwortlich ist, überprüfen Sie die QoS-Richtlinienstatistiken mit dem Befehl show policy-map interface <Schnittstelle> und den Warteschlangenzählern. Wenn die Anzahl der Verwerfungszähler unter einer bestimmten QoS-Klasse ansteigt, können die Verwerfungen durch QoS-Warteschlangenbegrenzungen oder Richtlinienzuweisung verursacht werden. Entfernen Sie die QoS-Richtlinie nach Möglichkeit während eines Wartungsfensters vorübergehend über die Schnittstelle Befehl no service-policy output <Policy-name> und überwachen, ob die Ausgabe weiterhin verworfen wird. Wenn das Verwerfen nach dem Entfernen der Richtlinie aufhört, trägt wahrscheinlich die QoS-Konfiguration zu den Verwerfungen bei.

Beispiel:

<#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
...
```

Frage: Können Ausgabeverringerungen an Hochgeschwindigkeitsschnittstellen wie 10G oder 40G auftreten?

A. Ja, selbst Hochgeschwindigkeits-Schnittstellen wie 10G oder 40G können bei der Zusammenführung mehrerer Hochgeschwindigkeits-Datenflüsse auf einem einzelnen Port Ausgabekürzungen erleben, die zu einer Überlastung der Schnittstellenpuffer führen. Zudem können Microbursts - kurze Datenverkehrsspitzen, die die Schnittstellenbandbreite überschreiten - Portpuffer schnell ausschöpfen und zu Paketverlusten führen.

F. Können Ausgabestörungen durch Hardwarefehler verursacht werden?

A. Leistungseinbrüche sind in der Regel nicht auf Hardwarefehler zurückzuführen. Sie resultieren in der Regel aus einer Überlastung des Datenverkehrs, bei der die Schnittstellenpuffer aufgrund hoher Datenverkehrsraten oder Microbursts überlastet sind. Hardwarebedingte Ausfälle können auftreten, sind jedoch in der Regel mit bestimmten Fehlerbedingungen verbunden, die im Vergleich zu überlastungsbedingten Ausfällen selten sind. Daher sind Leistungsverluste in erster Linie auf Netzwerkverkehrsbedingungen und nicht auf Hardwarefehler zurückzuführen. Die Überwachung von Schnittstellenfehlern wie FCS-/CRC-Fehlern kann dabei helfen, Hardwareprobleme zu identifizieren, sofern vorhanden. Diese unterscheiden sich jedoch von durch Überlastung verursachten Ausgabekürzungen.

F. Können Softwarefehler dazu führen, dass die Ausgabe verloren geht?

A. Durch Softwarefehler verursachte Ausgabekürzungen sind sehr selten und größtenteils kosmetischer Natur und haben keine wesentlichen Auswirkungen auf den Datenverkehr. Die meisten Ausgabeverluste werden in erster Linie durch Datenverkehrsengpässe und eine Erschöpfung des Puffers verursacht.

Frage: Können ECMP oder Lastenausgleich Engpässe reduzieren?

A. Ja, Equal-Cost Multi-Path (ECMP) Routing und Lastenausgleich reduzieren Engpässe, indem der Datenverkehr gleichmäßig über mehrere Pfade mit gleichen Kosten auf ein Ziel verteilt wird. Dieser Ansatz erhöht die Bandbreitennutzung und verhindert, dass einzelne Pfade zu Engpässen werden.

Frage: Beeinträchtigen Ausgabefehler den UDP-Datenverkehr anders als TCP?

A. Ja, der UDP-Datenverkehr wird anders als bei TCP durch Ausgabekürzungen beeinflusst, da es sich bei UDP um ein verbindungsloses Protokoll handelt, das verlorene Pakete nicht erneut überträgt. Ein Paketverlust wirkt sich also direkt auf Anwendungen wie Sprache oder Video aus, die auf eine rechtzeitige Übermittlung angewiesen sind. TCP hingegen umfasst Weiterleitungsmechanismen, die versuchen, verlorene Pakete wiederherzustellen, wodurch die Auswirkungen von Paketverlusten gemindert werden. Aus diesem Grund kann ein Verwerfen der Ausgabe zu einer deutlicheren Verschlechterung in UDP-basierten Echtzeitanwendungen führen, da verlorene Pakete nicht wiederhergestellt werden und dies zu Qualitätsproblemen führen kann.

F. Was ist der Unterschied zwischen Input- und Output-Drops?

A.: Eingangsverluste an Schnittstellen treten in der Regel dann auf, wenn die Eingangswarteschlangen überlastet sind und Pakete nicht schnell genug verarbeiten können. Dies führt dazu, dass Pakete basierend auf dem Warteschlangenalgorithmus selektiv verworfen werden. Ausgabeausfälle treten auf, wenn Pakete aufgrund einer Überlastung in der Ausgabewarteschlange oder einer Pufferüberlastung beim Verlassen einer Schnittstelle verworfen werden. Eingabetropfen hängen mit den Grenzwerten für die Verarbeitung des Eingangs zusammen, während Ausgabetropfen in erster Linie durch eine Überlastung des Ausgangs und einen Pufferüberlauf verursacht werden. Faktoren wie Datenverkehrsspitzen, Plattformbeschränkungen und QoS-Konfigurationen (Quality of Service), die Engpässe und die Pufferzuweisung verwalten, können diese Verwerfungen beeinflussen.

Frage: Können große Backup-Jobs zu einem Verlust der Ausgabe führen?

A. Ja, große Backup-Jobs, wie z. B. Daten-Backups, Replikation oder Massenübertragungen, erzeugen häufig Datenverkehrsspitzen, die die Schnittstellenpuffer überlasten können, was zu Ausgabeverringerungen führen kann. Diese Bursts können eine vorübergehende Überlastung der Ausgangsschnittstelle verursachen, insbesondere wenn die ausgehende Bandbreite geringer als die eingehende Datenverkehrsrate ist oder wenn mehrere Flüsse mit hoher Rate an einem einzelnen Port konvergieren.

Frage: Wie kann ich feststellen, ob Datenverkehrsspitzen zu Ausgabekürzungen führen?

A. Zur Bestätigung von durch Datenverkehrsspitzen verursachten Ausgabeverlusten können Sie eine SPAN-Sitzung in Kombination mit Wireshark verwenden, um den ausgehenden Datenverkehr an der betroffenen Schnittstelle zu erfassen und zu analysieren, während Ausgabeverluste auftreten. Befolgen Sie diese Schritte, um zu überprüfen, ob die Ausgabe aufgrund von

Datenverkehrsspitzen verloren geht.

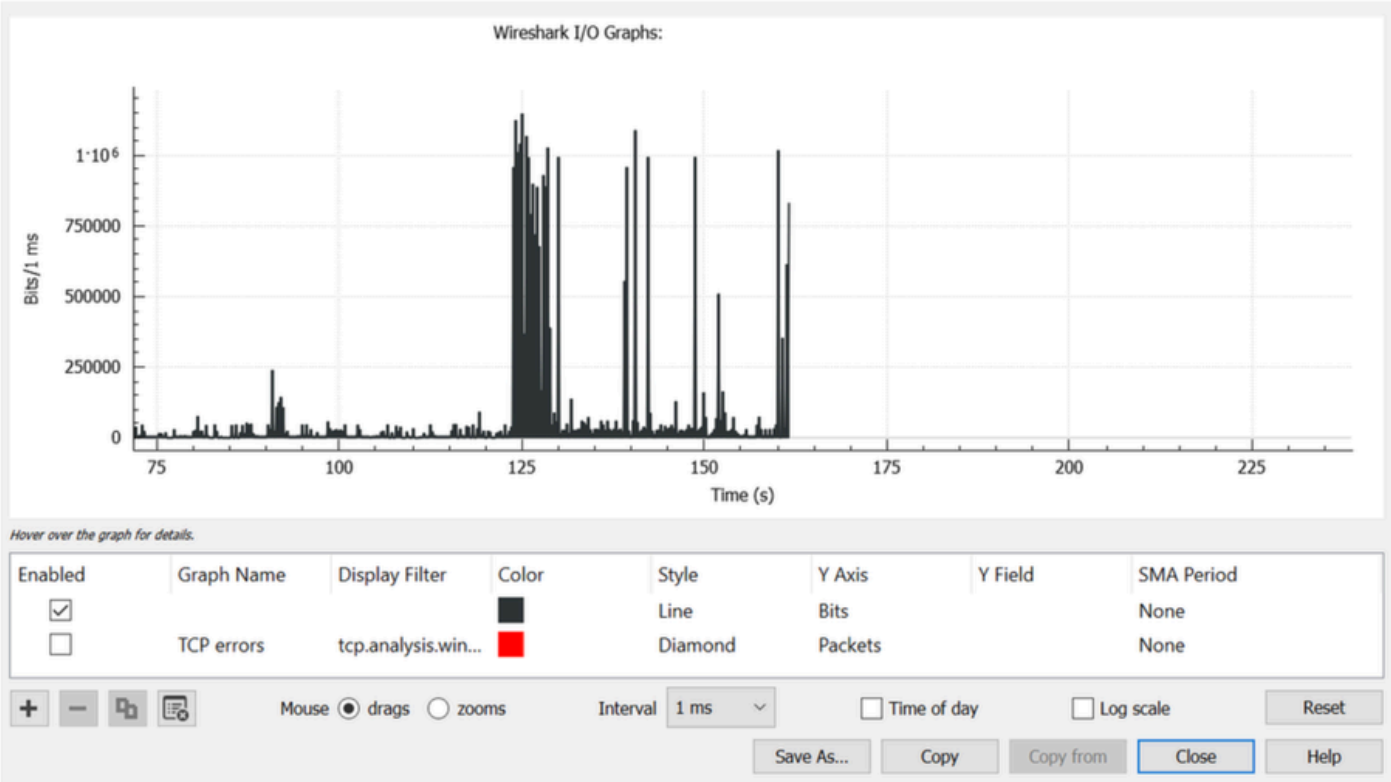
- Schließen Sie einen Laptop mit installiertem Wireshark an einen nicht verwendeten Port des Switches an.
- Konfigurieren Sie SPAN auf dem Switch, um den ausgehenden Datenverkehr der Schnittstelle zu spiegeln, bei der es zu Ausgabefehlern an dem Port kommt, an dem der Laptop angeschlossen ist.

```
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.
```

- Starten Sie die SPAN-Erfassung auf dem Switch, während die Ausgangsunterbrechungen aktiv zunehmen, um sicherzustellen, dass der relevante Datenverkehr erfasst wird.
- Öffnen Sie die Erfassungsdatei in Wireshark, und navigieren Sie dann zu Statistics > I/O Graph.
- Ändern Sie die Einstellung für Interval (Intervall) von der Standardeinstellung 1 Sekunde auf 1 Millisekunde (1 ms).
- Klicken Sie auf Zurücksetzen, um das Diagramm mit dem neuen Intervall zu aktualisieren.
- Das Diagramm zeigt den Datenverkehr in Bits pro Millisekunde an.

Achten Sie auf Datenverkehrsspitzen, die die Weiterleitungsgeschwindigkeit der Schnittstelle im Millisekundenbereich übersteigen (z. B. 1.000.000 Bit/ms bei einer 1-GBIT/s-Schnittstelle). Wenn der Datenverkehr diese Weiterleitungsgeschwindigkeit übersteigt, puffert der Switch Pakete, was

zu Überlastungen und Ausgabeverlusten führen kann. Identifizieren Sie Datenverkehrsspitzen (Microbursts), indem Sie Spitzen und dann Phasen mit geringem oder ohne Datenverkehr beobachten. In Wireshark werden durch Klicken auf einen Spike die entsprechenden Pakete ausgewählt, wodurch eine weitere Analyse des Datenverkehrs möglich ist, der die Löschungen ausgelöst hat. Das nächste Bild zeigt das aktualisierte E/A-Diagramm für eine Schnittstelle, bei der die Ausgabe verloren ging.



Wichtige Überlegungen

- Stellen Sie sicher, dass die SPAN-Quell- und -Zielports die gleichen oder kompatiblen Geschwindigkeiten aufweisen, um zusätzliche Datenverluste zu vermeiden.
- Erfassung von Datenverkehr bei gleichzeitig steigender Anzahl von Ausgabedateien zur Erfassung relevanter Spitzen.
- Embedded Packet Capture (EPC) wird für diesen Zweck nicht empfohlen, da es die Erfassungsraten begrenzt und Bursts verpassen kann.

Häufige Missverständnisse über Ausgabefälle

Irrtum: Jeglicher Output Drop bedeutet, dass das Netzwerk defekt ist.

Realität: In Hochgeschwindigkeitsnetzwerken ist aufgrund von Microbursts oder kurzen Datenverkehrsspitzen eine geringe Anzahl von Leistungseinbrüchen normal.

Irrtum: Wenn die Schnittstellennutzung gering ist, dürfen keine Verluste auftreten.

Realität: Die Auslastung wird als Durchschnittswert über der Zeit gemessen. Microbursts können die Schnittstellenbandbreite vorübergehend überschreiten und selbst bei geringer durchschnittlicher Auslastung zu Verlusten führen.

Irrtum: Wenn die Ausgabe ausfällt, ist die Switch-Hardware fehlerhaft.

Realität: Leistungsabfälle werden in der Regel durch Datenverkehrsüberlastung oder Burst-Datenverkehr verursacht, nicht durch Hardwareprobleme.

Irrtum: Durch eine erhöhte Pufferzuweisung werden alle Verluste vermieden.

Realität: Puffer absorbieren nur vorübergehende Spitzen. Eine anhaltende Überlastung führt weiterhin dazu, dass Pakete verworfen werden.

Irrtum: Nur bei 1G-Schnittstellen treten Ausgabekürzungen auf.

Realität: Verluste können an Schnittstellen mit 10G, 25G, 40G oder höheren Geschwindigkeiten auftreten, wenn Datenverkehrsspitzen die verfügbare Bandbreite oder Pufferkapazität übersteigen.

Irrtum: QoS muss alle Paketverluste ausschließen/verhindern.

Realität: QoS priorisiert wichtigen Datenverkehr, kann aber bei Überlastungen absichtlich Datenverkehr mit niedrigerer Priorität verwerfen.

Irrtum: Jeglicher Output Drop hat Auswirkungen auf den Benutzer.

Realität: Viele Anwendungen verwenden die TCP-Neuübertragung, mit der sich gelegentliche Paketverluste ohne nennenswerte Auswirkungen beheben lassen.

Irrtum: Verluste treten nur auf, wenn die Schnittstellen eine Auslastung von 100 % erreichen.

Realität: Verluste können bei kurzen Datenverkehrsspitzen auftreten, selbst wenn die durchschnittliche Auslastung niedrig bleibt.

Irrtum: Die QoS-Konfiguration ist immer die Ursache für Unterbrechungen.

Realität: Die meisten Datenverluste werden durch Datenverkehrsmuster oder Überbelegung verursacht, nicht durch QoS-Richtlinien.

Irrtum: In einem intakten Netzwerk darf es nie zu Leistungseinbußen kommen.

Realität: In leistungsstarken Switching-Umgebungen ist mit gelegentlichen Ausfällen zu rechnen.

Leitfäden zur Fehlerbehebung

- Fehlerbehebung für verworfene Ausgangspakete auf Switches der Catalyst 9000-Serie
- Analyse der Warteschlangenpufferzuweisung bei Catalyst Switches der Serie 9000
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.