Fehlerbehebung bei Netzwerklatenz und Paketverlusten auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument wird eine detaillierte Methodik zur Behebung von Problemen mit Netzwerklatenz und Paketverlusten bei Cisco Catalyst Switches der Serie 9000 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit Netzwerkkonzepten wie TCP/IP, VLANs und Spanning Tree Protocols (STPs) zu befassen. Die Kenntnis der Cisco Catalyst Switches der Serie 9000 und der Cisco IOS® XE CLI ist äußerst wichtig. Außerdem müssen Sie mit den Netzwerküberwachungstools und den Zugriffsberechtigungen für Konfiguration und Diagnose vertraut sein.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Catalyst Switches der Serie 9000 mit allen Versionen. Dieses Dokument ist nicht auf bestimmte Software- oder Hardwareversionen 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

Dieses Dokument richtet sich an Netzwerkadministratoren und -techniker und bietet Hilfestellung bei der effizienten Identifizierung, Isolierung und Lösung dieser Probleme in Netzwerkumgebungen von Unternehmen. Netzwerklatenz und Paketverluste können die Leistung und Zuverlässigkeit in Unternehmensumgebungen beeinträchtigen. Diese Probleme resultieren häufig aus Netzwerküberlastungen, Fehlkonfigurationen oder Umgebungsfaktoren. Cisco Catalyst Switches der Serie 9000 wurden für hohe Leistung und Ausfallsicherheit konzipiert. Dieses Dokument enthält gezielte Schritte zur Fehlerbehebung, damit Netzwerkexperten Latenz- und Paketverluste bei der Verwendung dieser Switches erkennen und beheben können.

Netzwerklatenz und Paketverluste

Netzwerklatenz

Netzwerklatenz ist die Messung der Verzögerung, die auftritt, wenn Daten ein Netzwerk von der

Quelle bis zum Ziel durchlaufen. In der Regel wird die Latenz als Round-Trip Time (RTT) ausgedrückt - die Zeit, die ein Paket benötigt, um von der Quelle zum Ziel und zurück zu gelangen.

Die Latenz wird in der Regel in Millisekunden (ms) gemessen.

Auswirkungen: Eine hohe Latenz kann die Anwendungsleistung beeinträchtigen, insbesondere bei Protokollen wie TCP, die für eine effiziente Datenübertragung auf rechtzeitige Bestätigungen angewiesen sind.

Paketverlust

Paketverluste treten auf, wenn Netzwerkgeräte Pakete nicht an ihr beabsichtigtes Ziel weiterleiten können, was häufig auf Überlastungen, Pufferüberläufe, Fehlkonfigurationen oder fehlerhafte Hardware zurückzuführen ist. Paketverluste werden in der Regel als Prozentsatz verlorener Pakete über ein bestimmtes Intervall gemessen.

Auswirkungen: Paketverluste reduzieren den Durchsatz, verursachen Neuübertragungen und können die Anwendungszuverlässigkeit beeinträchtigen.

Erwartete Latenz-Benchmarks

Netzwerktyp	Typische RTT
Gleiches VLAN (Access Layer)	< 1 ms
Campus Core-Traversal	1-5 ms
Metro-WAN	5-30 ms
Internet/WAN	30-150 ms

Anmerkung: Die geografische Entfernung zwischen Netzwerk-Hops kann die RTT erhöhen und zu einer höheren Latenz beitragen.

Messung der Netzwerklatenz

Beginnen Sie mit einem umfassenden Verständnis Ihres Netzwerks und seiner Topologie. Wenn Ihr Netzwerk auf deterministische Variablen und minimale Unvorhersehbarkeit ausgelegt ist, wird der Prozess der Erkennung und Behebung von Latenz- und Paketverlusten erheblich einfacher.

Zur Messung der Netzwerklatenz werden in der Regel zwei Tools verwendet.

Ping

Es wird ausgegeben, ob ein Ziel erreichbar ist, zusammen mit Statistiken zu Paketverlusten und RTT. Sobald Sie die problematischen Hops identifizieren, können Sie versuchen, direkt zwischen ihnen zu pingen und die Geräte einzuchecken, um das Problem zu finden.

<#root>

Switch#ping 8.8.8.8

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!.!!.
```

Success rate is 60 percent (3/5),

round-trip min/avg/max = 12/

15

/22 ms

<===== 2 dropped out of 5 packets, Average RTT 15 ms

Routenverfolgung

Die Traceroute zeigt alle Hops im Routing-Pfad von der Quelle zum Ziel sowie die RTT-Ergebnisse für jeden Hop. Eine Traceroute kann beispielsweise anzeigen, wo im Netzwerk (in welchem Hop im Routing-Pfad) die Verzögerung vorhanden ist oder beginnt. Ein solches Beispiel ist in der nächsten Ausgabe der Traceroute dargestellt.

<#root>

Switch#traceroute 8.8.8.8

```
Type escape sequence to abort.
Tracing the route to 8.8.8.8

1 2 ms 2 ms 2 ms   [10.10.10.10]
2 2 ms 1 ms 1 ms   [20.20.20.20]
```

3 7 ms 45 ms 40 ms [30.30.30.30]

<===== High latency at this hop

```
4 7 ms 3 ms 1 ms   [40.40.40.40]

Note: The IP addresses shown for each hop are provided for demonstration purposes only.
```

Diese Ausgabe deutet auf eine wahrscheinliche Verzögerung an Hop 3 hin, was sich in einem deutlichen Anstieg der RTT zwischen Hop 2 und Hop 3 zeigt. Der relativ geringe Zeitunterschied zwischen Hop 3 und Hop 4 deutet darauf hin, dass das Problem auf das Segment zwischen 20.20.20.20 und 30.30.30 lokalisiert ist.

Häufige Ursachen von Latenz und Paketverlusten

Probleme mit Layer 1 (physischer Layer)

Layer-1-Probleme sind eine häufige Ursache für Netzwerklatenz und Paketverluste. Auf der physischen Ebene müssen folgende Aspekte überprüft werden:

- Überprüfen Sie, ob die Duplex- und Geschwindigkeitseinstellungen an allen Schnittstellen richtig konfiguriert sind.
- Überprüfen Sie die Schnittstellen auf CRC-Eingabefehler, die auf Probleme auf der physischen Schicht hinweisen können.
- Fehlerhafte Netzwerkkabel, Glasfaserverbindungen, SFP-Module oder Switch-Ports können ebenfalls zu Paketverzögerungen und -verlusten führen.


```
Switch#show interface gi1/0/1


GigabitEthernet1/0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 70b3.171d.c101
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,


Full-duplex, 1000Mb/s,

 media type is 10/100/1000BaseTX
  ...
  5 minute input rate 2000 bits/sec, 5 packets/sec
  5 minute output rate 3000 bits/sec, 8 packets/sec
     250000 packets input, 22000000 bytes, 0 no buffer
     Received 300 broadcasts (200 multicasts)
     0 runts, 0 giants, 0 throttles


85 input errors, 85 CRC,

 0 frame, 0 overrun, 0 ignored

<===== Input errors and CRC


     0 watchdog, 0 multicast, 0 pause input
```

```
  ...
     260000 packets output, 23000000 bytes, 0 underruns
     5 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
```

Switch# show interfaces counters errors

Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize	OutDiscards
Gi1/0/1	**0**	**0**	**0**	**0**	**0**	**0**
Gi1/0/2	0	0	0	0	0	0

```
...
```

Ausgabekürzungen

Wenn eine Senderwarteschlange einer Switch-Schnittstelle voll ist und keine weiteren Pakete weiterleiten kann, treten Ausgabeunterbrechungen auf. Dies kann zu einer höheren Latenz führen, wenn Pakete in der Warteschlange warten, und bei einem Überlauf der Warteschlange zu Paketverlusten führen, was sich auf die Anwendungsleistung und die Netzwerkzuverlässigkeit auswirkt.

<#root>

Switch#show interface gi1/0/1

```
GigabitEthernet1/0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 70b3.171d.c101
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
...
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 2d00h
  Input queue: 0/2000/0/0 (size/max/drops/flushes)
```

; Total output drops: 4216760900

```
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 389946000 bits/sec, 84175 packets/sec
  5 minute output rate 694899000 bits/sec, 106507 packets/sec
     7885666654 packets input, 4677291827948 bytes, 0 no buffer
...
```

Der Zähler für die Gesamtausgabe verworfene Pakete zeigt eine große Anzahl verworfener

Pakete an. Dies weist auf eine Überlastung oder einen Warteschlangenüberlauf an dieser Schnittstelle hin. Dies kann zu erhöhter Latenz und Paketverlusten führen und die Netzwerk- und Anwendungsleistung beeinträchtigen.

STP-Stabilität

Eine STP-Instabilität kann zu Netzwerklatenz und Paketverlusten beitragen. In einem stabilen Netzwerk müssen die Topologieänderungen minimal sein. Häufige Topologieänderungen können auf zugrunde liegende Probleme hinweisen und den normalen Weiterleitungsvorgang stören.

Wichtige Überlegungen zur Minimierung der STP-Latenz:

Topologieänderungen (TCNs): Übermäßige STP-Topologieänderungen können dazu führen, dass die MAC-Adresse der Switch-Tabelle (CAM) häufig geleert wird, was den Broadcast-Datenverkehr und die Latenz erhöht, da die Switches unbekannte Unicast-Pakete überfluten, bis die Tabelle neu aufgefüllt wird.

Edge-Port-Konfiguration: Stellen Sie sicher, dass alle Edge-Ports mit PortFast konfiguriert sind. Durch die Aktivierung von PortFast wird verhindert, dass Benachrichtigungen zu STP-Topologieänderungen (TCNs) generiert werden, wenn Clients oder Server eine Verbindung herstellen oder trennen. Dadurch wird die unnötige Veralterung der CAM-Tabelle verringert und die Stabilität verbessert.

Planung der Root Bridge: Manuelle Planung und Zuweisung von STP-Root-Bridges und -Prioritäten, um eine planbare Netzwerktopologie zu erhalten und unnötige Topologieänderungen zu minimieren

Bei einer Topologieänderung (z. B. einem Port-Übergangsstatus) sendet der Switch eine TCN-BPDU an die Root-Bridge. Die Root-Bridge gibt dann TCN-BPDUs an alle Switches weiter und fordert sie auf, die Alterungszeit ihrer MAC-Adressen vom Standardwert (300 Sekunden) auf den Wert für die Weiterleitungsverzögerung (in der Regel 15 Sekunden) zu verkürzen. Dies führt dazu, dass kürzlich nicht verwendete Einträge gelöscht werden, was zu mehr unbekannten Unicasts und zu erhöhten Überschwemmungen im gesamten Netzwerk führt.

<#root>

```
Switch#show spanning-tree detail | include ieee|from|occur|is exec


VLAN0705 is executing the ieee compatible Spanning Tree protocol

Number of topology changes 6233

last change occurred 00:00:03 ago

     <===== Topology Changes


from GigabitEthernet1/0/25                                  <===== From Gi1/0/25
```

MAC Flapping/Layer 2 Loops

MAC-Flapping/Layer-2-Schleifen verursachen Netzwerklatenz und Paketverluste, indem die MAC-Adresstabelle mit derselben Quell-MAC an verschiedenen Ports kontinuierlich aktualisiert wird. Diese ständige Änderung unterbricht die Datenweiterleitung und führt zu Unterbrechungen und Paketverlusten. Layer-2-Schleifen verschlimmern das Problem, da sie dafür sorgen, dass Broadcast-Pakete endlos zirkulieren. Dadurch wird das MAC-Flapping verstärkt und die Netzwerkleistung weiter herabgesetzt. Die Implementierung von Schleifenvermeidungsprotokollen wie STP ist für einen stabilen Netzwerkbetrieb und zur Vermeidung dieser Probleme unerlässlich.

Um die MAC-Verschiebungsbenachrichtigung zu konfigurieren, verwenden Sie den Befehl mac address-table notification mac-move im globalen Konfigurationsmodus.

<#root>

Mac Flapping logs:

```
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po1 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host b0f1.ec27.69ea in vlan 154 is flapping between port Po9 and port Po
```

Flusssteuerung

Wenn die Flusssteuerung aktiviert ist und sich ein Empfangspuffer eines Switch-Ports der Kapazität nähert, sendet der Switch Pausen-Frames, um den eingehenden Datenverkehr vorübergehend anzuhalten. Dieser Prozess kann die Latenz erhöhen, da die Datenübertragung zeitweise angehalten wird. Wenn die Datenflusskontrolle dagegen nicht aktiviert ist oder Upstream-Geräte Pausen-Frames nicht berücksichtigen, kann der eingehende Datenverkehr die Pufferkapazität überschreiten, was zu Pufferüberläufen und Paketverlusten führt.

Die Flusskontrolle muss unter Berücksichtigung der Funktionen aller Geräte im Datenverkehrspfad sorgfältig konfiguriert werden. Eine unsachgemäße Verwendung oder Fehlkonfiguration kann die Latenz erhöhen und zu Paketverlusten führen, was sich negativ auf die Anwendungsleistung auswirkt.

<#root>

Switch#show interfaces gigabitEthernet 1/0/1

```
GigabitEthernet1/0/1 is up, line protocol is up (connected)
□
```

input flow-control is on,

```
 output flow-control is unsupported
```

<===== Input Flow Control is ON

Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 6530
5 minute input rate 8000 bits/sec, 8 packets/sec
5 minute output rate 0 bits/sec, 0 packets/s
0 watchdog, 5014620 multicast,

1989 pause input

<===== Pause Input

0 unknown protocol drops 0 babbles, 0 late collision,
0 deferred 0 lost carrier, 0 no carrier, 0 pause output

Switch#show controllers ethernet-controller gigabitEthernet 1/0/1

Transmit GigabitEthernet1/0/1 Receive
0 MacUnderrun frames 0 MacOverrun frames
0 Pause frames

1878 Pause frames <===== Pause frames in RX

CPU-Auslastung

Eine hohe CPU-Auslastung kann die Netzwerklatenz erhöhen und Paketverluste verursachen. Wenn die CPU stark ausgelastet ist, kann der Switch den Datenverkehr auf der Kontrollebene, Routing-Updates oder Managementfunktionen nicht effizient verarbeiten. Dies kann die Paketweiterleitung verzögern, Timeouts für Protokolle wie ARP oder Spanning Tree verursachen und zu Paketverlusten führen, insbesondere bei Datenverkehr, der einen CPU-Eingriff erfordert.

<#root>

Switch#show processes cpu sorted

CPU utilization for five seconds:

95%/8%;

one minute: 92%; five minutes: 90%

<===== CPU utilization 93%

PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process

439 3560284 554004 6426 54.81% 55.37% 48.39% 0 SISF Main Thread

438 2325444 675817 3440 22.67% 28.17% 27.15% 0

SISF Switcher Th

104 548861 84846 6468 10.76% 8.17% 7.51% 0 Crimson flush tr

```
 119      104155      671081        155  1.21%  1.27%  1.26%   0 IOSXE-RP Punt Se
```

Speichernutzung

Eine hohe Speichernutzung kann zu Latenz und Paketverlusten führen, da die CPU- und Kontrollebenenprozesse überlastet werden. Diese Überlastung verzögert die Bearbeitung von Routing-Updates, QoS-Richtlinien und dem Puffermanagement, was zu einer Überlastung in der Paketverarbeitungs-Pipeline führt. Daher können Pakete verworfen oder verzögert werden. Eine hohe Speichernutzung wirkt sich daher negativ auf die Netzwerkleistung aus, da die Effizienz des Switches bei der Verwaltung des Datenverkehrs sinkt.

<#root>

Switch#show platform resources

```
Resource                  Usage                    Max             Warning         Critical
-------------------------------------------------------------------------------------------
Control Processor       25.00%                     100%            90%             95%
  DRAM
```

3656MB(94%)

```
            866MB           90%             95%             W
```

High memory logs:

```
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
```

ICMP-Umleitungen und nicht erreichbare Nachrichten

Wenn ein Paket an einer Layer-3-Schnittstelle ankommt und von derselben Schnittstelle weitergeleitet wird, generiert der Switch eine ICMP-Umleitungsnachricht, um die Quelle über einen effizienteren nächsten Hop im gleichen Subnetz zu informieren. Dies führt dazu, dass das ursprüngliche Paket zweimal das vLAN passiert, was die Bandbreitennutzung erhöht. Darüber hinaus beansprucht das ICMP-Umleitungspaket selbst Bandbreite und erfordert CPU-Verarbeitung, was zu CPU-Unterbrechungen und erhöhter Latenz führen kann. Wenn viele solcher Umleitungen erfolgen, insbesondere bei starkem Datenverkehr, kann die CPU-Last erheblich ansteigen, was möglicherweise Paketverluste zur Folge hat.

Die häufige Generierung und Verarbeitung von nicht erreichbaren ICMP-Nachrichten kann ebenfalls die CPU-Auslastung erhöhen und so die Netzwerkleistung beeinträchtigen. Hohes Volumen an nicht erreichbarem ICMP-Datenverkehr beansprucht CPU-Ressourcen, was zu Latenz und Paketverlusten führen kann.

Um diese Auswirkungen zu minimieren, empfiehlt Cisco die Deaktivierung von nicht erreichbaren ICMP-Meldungen und ICMP-Weiterleitungen an Switch Virtual Interfaces (SVIs) und Layer 3-Schnittstellen mithilfe der Befehle no ip unreachables und no ip redirects. Dieses Best Practice-Verfahren reduziert die CPU-Last und verbessert die Netzwerkstabilität.

<#root>

Switch#show ip traffic | in unreachable

```
...
  Rcvd: 194943 format errors, 369707 checksum errors,
3130 redirects,
734412 unreachable

  Sent: 29265 redirects, 14015958 unreachable, 196823 echo, 786959149 echo reply
...
```

Switch#show platform hardware fed active qos queue stats internal cpu policer

```
           CPU Queue Statistics
============================================================================================
                                                (default) (set)     Queue        Queue
QId PlcIdx  Queue Name                 Enabled   Rate     Rate      Drop(Bytes)  Drop(Frames)
--------------------------------------------------------------------------------------------
0    11     DOT1X Auth                  Yes     1000      1000     0            0
1    1      L2 Control                  Yes     2000      2000     0            0
2    14     Forus traffic               Yes     4000      4000     3296567      2336
3    0      ICMP GEN                    Yes     750       750      0            0
4    2      Routing Control             Yes     5500      5500     1085196      12919
5    14     Forus Address resolution    Yes     4000      4000     51723336     760639

6    0      ICMP Redirect               Yes     750       750      8444220485535  6978564145

...
```

Stürme im Datenverkehr

Ein Datenstrom tritt auf, wenn übermäßige Broadcast-, Multicast- oder Unicast-Pakete ein LAN überfluten, die Ressourcen des Switches überlasten und die Netzwerkleistung herabsetzen.

Die Sturmkontrolle auf Switches überwacht Broadcast-, Multicast- und Unicast-Datenverkehr an physischen Schnittstellen und vergleicht diesen mit konfigurierten Schwellenwerten. Wenn der Datenverkehr diese Grenzwerte überschreitet, blockiert der Switch den übermäßigen

Datenverkehr vorübergehend, um eine Beeinträchtigung des Netzwerks zu verhindern. Dies schützt Switch-Ressourcen und gewährleistet die Stabilität und Leistung des gesamten Netzwerks.

<#root>

Switch#show interfaces counters

```
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1        125487955     550123004     250123555     105234788

Gi1/0/2           500123        100123          5123          1024
Gi1/0/3           250123         50123          1024           512
```

Switch#show platform hardware fed switch active qos queue stats internal cpu policer

```
                          CPU Queue Statistics
============================================================================================
                                                  (default) (set)     Queue         Queue
QId PlcIdx  Queue Name                 Enabled    Rate      Rate      Drop(Bytes)   Drop(Frames)
--------------------------------------------------------------------------------------------
11   13     L2 LVX Data Pack             Yes      1000      1000      0             0

12   0      BROADCAST                    Yes      750       750       32529067      186363

13   10     Openflow                     Yes      250       250       0             0

14   13     Sw forwarding                Yes      1000      1000      48317658492   245507344

15   8      Topology Control             Yes      13000     16000     0             0
```

CAM- und ARP-Alterungszeit

Die Veraltungszeit von CAM (MAC Address Table) und ARP (Address Resolution Protocol) kann ebenfalls zu Netzwerklatenz und Paketverlusten führen. Dies liegt daran, dass die CAM-Tabelle, in der MAC-Adressen zu Port-Zuordnungen gespeichert sind, Einträge in der Regel schneller altert (Standard: ca. fünf Minuten) als die ARP-Tabelle, in der Zuordnungen von IP- zu MAC-Adressen gespeichert werden (Standard: ca. vier Stunden). Wenn eine MAC-Adresse aus der CAM-Tabelle entfernt wird, aber noch in der ARP-Tabelle vorhanden ist, kennt der Switch den jeweiligen Port nicht mehr, um Unicast-Datenverkehr für diese MAC-Adresse weiterzuleiten. Der Switch flutet daher den Unicast-Datenverkehr an alle Ports im VLAN und verursacht Netzwerküberlastungen und potenzielle Paketverluste.

Wie der CAM im Vergleich zur ARP-Veraltungszeit zu Latenz und Paketverlusten führt

- Wenn der CAM-Tabelleneintrag vor dem ARP-Eintrag veraltet ist, überflutet der Switch Unicast-Pakete, da keine MAC-Port-Zuordnung möglich ist.
- Diese Überlastung erhöht die CPU-Last und beansprucht unnötigerweise Bandbreite, was zu Netzwerklatenz und Paketverlusten führt.
- Die Diskrepanz kann auch zu einer ineffizienten Weiterleitung und einer verstärkten Verarbeitung auf Kontrollebene führen.

<#root>

Switch#show mac address-table aging-time

Global Aging Time:

300 <===== MAC aging

Vlan Aging Time
---- ----------

Switch#show ip arp

Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.95.1

124

Incomplete ARPA

<===== Arp age

...

Switch#show interface vlan1

Vlan1 is up, line protocol is up , Autostate Enabled
Hardware is Ethernet SVI, address is 10b3.d6f0.1347 (bia 10b3.d6f0.1347)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
ARP type: ARPA,

ARP Timeout 04:00:00

Last input never, output never, output hang never

Configuring MAC Aging and ARP Timeout:

```
Switch#confure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Switch(config)#mac-address-table aging-time ?

```
  <0-0>         Enter 0 to disable aging
  <10-1000000>  Aging time in seconds
```

Switch(config)#mac-address-table aging-time 14400 ?

```
  routed-mac  Set RM Aging interval
  vlan        VLAN Keyword
```

Switch(config)#interface vlan 1

```
Switch(config-if)#arp timeout 300

Switch(config-if)#do show interface vlan 1

Vlan1 is up, line protocol is up , Autostate Enabled
  Hardware is Ethernet SVI, address is 10b3.d6f0.1347 (bia 10b3.d6f0.1347)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA,
```

ARP Timeout 00:05:00

```
  Last input never, output never, output hang never
```

Sitzung überwachen

Wenn aktive Monitoring-Sitzungen (SPAN) auf einem Switch mit mehreren Quell- und Ziel-Ports konfiguriert werden, können sie zu Netzwerklatenz und Paketverlusten beitragen.

<#root>

Example:

```
Session 1

---------

Type                  : Local Session
Source Ports          :

    Both              : Po101,Po105,Po109,Po125,Po161,Po170      <===== Multiple source ports

Destination Ports     : Te9/8

Egress SPAN Replication State:
Operational mode      : Centralized
Configured mode       : Centralized (default)

Session 2

---------

Type                  : Local Session
Source Ports          :

    Both              : Po161,Po170

Destination Ports     : Te9/1

Egress SPAN Replication State:
Operational mode      : Centralized
Configured mode       : Centralized (default)
```

Funktionsweise von SPAN

SPAN (Switched Port Analyzer) ist eine hardwaregestützte Funktion, die den Datenverkehr von Quell-Ports auf Ziel-Ports spiegelt, ohne dass CPU-Abfragen erforderlich sind. Der Replikations-ASIC auf dem Supervisor-Modul übernimmt die Paketspiegelung, während die Weiterleitungs-Engine die gespiegelten Pakete an die Ziel-Ports umleitet. Gespiegelte Pakete werden mit der gleichen Zeit wie regulärer Datenverkehr weitergeleitet.

Auswirkungen mehrerer Quell- und Ziel-Ports:

Im vorherigen Beispiel muss der Switch Datenverkehr von allen Quellschnittstellen auf die Zielschnittstellen replizieren. Der Datenverkehr des Po170-Schnittstellenmoduls wird beispielsweise gespiegelt und zweimal an zwei verschiedene Ziele weitergeleitet. Diese Replikation erhöht die Last für die Weiterleitungs-Engine und kann zu Überlastungen in der Switch-Backplane führen.

- Wenn auf einem Port-Channel ein Datenverkehr mit drei Gbit/s übertragen wird, kann die Replikation dieses Datenverkehrs an mehrere Ziele zu mehr als 15 Gbit/s gespiegeltem Datenverkehr führen.
- Die Last des Replikations-ASIC nimmt proportional zur Datenverkehrsrate an den Quellschnittstellen zu.
- Bei niedrigeren Datenverkehrsraten sind die Auswirkungen auf die Latenz minimal. Mit steigendem Datenverkehr nehmen Latenz und Überlastungen jedoch zu.

Ausnahmen auf ASIC-Ebene

Verwenden Sie diesen Befehl, um die Schnittstelle auf ASIC-Zuordnungen zu überprüfen, die die ASIC-Instanz anzeigen, in der sich die Schnittstelle befindet.

<#root>

```
Switch#show platform software fed switch active ifm mappings

Interface                IF_ID    Inst Asic Core Port SubPort Mac  Cntx LPN  GPN  Type Active

GigabitEthernet2/0/12    0x13
 1     0    1
     11     0      20    17   12   108  NIF   Y
<===== ASIC Instance 1 (Asic 0/Core 1)
```

Sobald die ASIC-Instanz identifiziert ist, führen Sie den nächsten Befehl aus, um die Weiterleitungs-ASIC-Drop-Ausnahmen für diese ASIC anzuzeigen.

<#root>

```
Switch#show platform hardware fed switch active fwd-asic drops exceptions asic
```

```
Example output snippet for ASIC instance 1:

****EXCEPTION STATS ASIC INSTANCE 1 (asic/core 0/1)****
================================================================================
 Asic/core |                NAME                  |   prev       |  current  |  delta

================================================================================
0       1  NO_EXCEPTION                            2027072618   2028843223    1770605
0       1  ROUTED_AND_IP_OPTIONS_EXCEPTION        735          735           0
0       1  PKT_DROP_COUNT                         14556203    14556203        0
0       1  BLOCK_FORWARD                         14556171    14556171        0
0       1  IGR_EXCEPTION_L5_ERROR                 1            1             0
...
```

Software-Bugs

Softwarefehler können manchmal direkt oder indirekt unbeabsichtigte und unerwartete Verhaltensweisen verursachen. Diese Fehler können zu Problemen wie Netzwerklatenz, Paketverlusten oder anderen Leistungseinbußen führen. Um diese Probleme zu beheben, besteht ein gängiger erster Schritt darin, den Switch neu zu laden. Dadurch können vorübergehende Fehler behoben und der Normalbetrieb wiederhergestellt werden. Darüber hinaus ist es wichtig, Ihre Geräte durch regelmäßige Anwendung der neuesten Firmware- und Software-Updates auf dem neuesten Stand zu halten. Diese Updates beinhalten häufig Korrekturen für bekannte Fehler und Verbesserungen, die die Stabilität und Leistung von Geräten verbessern und so dazu beitragen, Probleme im Zusammenhang mit Softwarefehlern zu vermeiden.

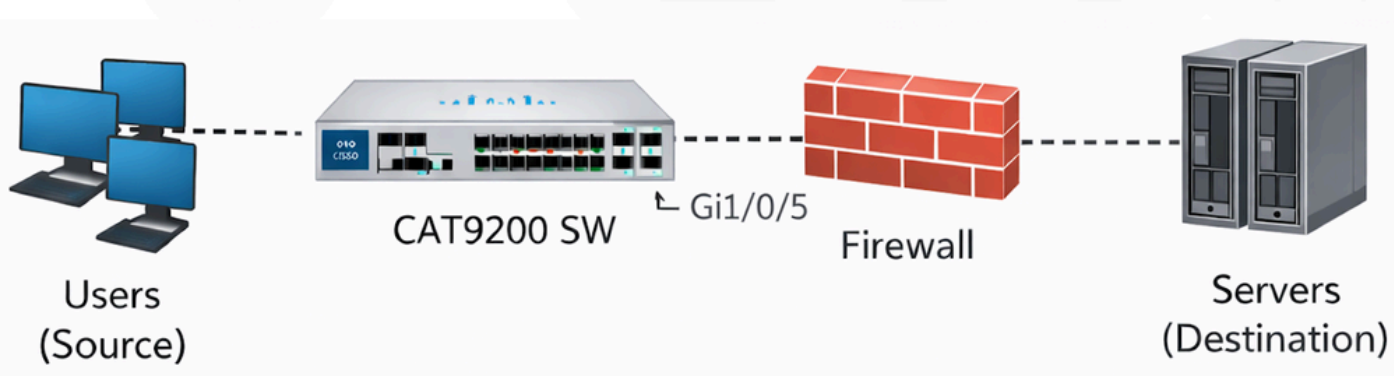
Cisco Bug Search-Tool

Anwenderbericht

Problemdetails

Bei Versuchen, große Datenmengen über vLANs zu übertragen, z. B. bei Dateiübertragungen mit hoher Kapazität, kommt es zu gelegentlichen Netzwerkverbindungsverlusten. Diese Unterbrechungen werden als sporadische Fehler bei der Datenübertragung trotz mehrerer erfolgreicher Versuche deutlich, die die Netzwerkzuverlässigkeit und die Anwendungsleistung erheblich beeinträchtigen. Das Problem wird durch erneutes Laden des Switches vorübergehend behoben.

Topologie



Symptome

- Die Dateiübertragung zwischen Quelle und Ziel schlägt nach mehreren erfolgreichen Versuchen immer wieder fehl.
- Bei Ausfällen wird die Verbindung zum Firewall unterbrochen.
- Die 802.1X-Authentifizierung bleibt während des gesamten Vorfalls funktionsfähig.
- Der Switch reagiert über die Konsole während der Incidents.
- Der verbundene Port der Firewall zeigt während der Ausfallzeiten nur Broadcast-Datenverkehr an.
- Diagnosetests (DiagGoldPktTest) schlagen an der Schnittstelle Gi1/0/5 durchweg fehl und weisen auf ein Datenpfad-Problem hin.

Fehlerbehebung durchgeführt

- Die Schnittstellenzähler und die Pufferstatistiken auf Plattformebene werden überprüft.
- Die Switch-Schnittstelle Gi1/0/5 zeigt ein sehr hohes Volumen von 802,3x Pause-Frames, die von der Firewall empfangen werden.
- Output-Drops und Statistiken zu Pausen-Frames werden genau überwacht.
- Die Warteschlangenstatistiken der Forwarding-Engine der Plattformsoftware werden überprüft, um das Pufferverhalten zu identifizieren.
- Die Flusssteuerungseinstellungen an der Switch-Schnittstelle werden überprüft.

Relevante Schnittstellenstatistiken

<#root>

```
Switch#show interfaces GigabitEthernet 1/0/5

GigabitEthernet1/0/5 is up, line protocol is up (connected)
□
input flow-control is on,
 output flow-control is unsupported
<===== Input Flow-control is ON

Input queue: 0/2000/0/0 (size/max/drops/flushes);
```

Total output drops: 78444

5 minute input rate 8000 bits/sec, 8 packets/sec□

5 minute output rate 0 bits/sec, 0 packets/s **<===== Output rate**

0 watchdog, 5014620 multicast,

1989 pause input

0 unknown protocol drops□0 babbles, 0 late collision,
...

Switch#show controllers ethernet-controller GigabitEthernet 1/0/5

Transmit GigabitEthernet1/0/5. Receive
0 MacUnderrun frames 0 MacOverrun frames
0 Pause frames

1878 Pause frames

<===== Pause Frames In RX

...

Switch#diagnostic start switch 1 test DiagGoldPktTest port 5

Switch#show diagnostic result switch 1 test DiagGoldPktTest detail

□Test results: (. = Pass, F = Fail, U = Untested)
_____
1) DiagGoldPktTest:
Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24□
U U U U

F

U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U.

<===== DiagGoldPktTest Failed For Port 5

Port 25 26 27 28□----------□U U U U

Switch#show flowcontrol interface GigabitEthernet 1/0/

Port Send FlowControl Receive FlowControl RxPause TxPause
admin oper admin Oper
---------- -------- -------- -------- -------- ------- -------
Gi1/0/5 Unsupp. Unsupp. on on.

13256

```
          0
<===== Pause Frames In RX


Switch#show platform hardware fed switch active qos queue stats interface GigabitEthernet 1/0/5


Asic:0 Core:0 DATA Port:8 Hardware Drop Counters□
------------------------------------------------------------
Q   Drop-TH0     Drop-TH1      Drop-TH2      SBufDrop          QebDrop
□   (Bytes)        (Bytes)       (Bytes)       (Bytes)              (Bytes)□
------------------------------------------------------------
0     0               0

18106020

           0               0
```

Ursachenermittlung

Die Ursache wurde als Puffersperre identifiziert, da übermäßige 802.3x-Pausen-Frames von der Firewall an die Switch-Schnittstelle gesendet wurden. Ethernet-Pausen-Frames weisen den Switch an, die Übertragung zu unterbrechen, damit sich das Empfangsgerät von einer Überlastung erholen kann. Wenn Pausen-Frames jedoch wiederholt oder für eine längere Dauer gesendet werden:

- Die Ausgabewarteschlange des Switch-Puffers für die Schnittstelle ist voll ausgelastet.
- Der Switch akzeptiert weiterhin eingehende Pakete, die für die angehaltene Schnittstelle bestimmt sind und sich in der Ausgabewarteschlange akkumulieren.
- Die Sättigung der Warteschlangen führt zu Ausgabeverlusten und Blackholing des Datenverkehrs.
- In diesem Fall wurden die Puffer gesperrt, und die Weiterleitung wurde auch nach der Verringerung der Pausen-Framerate nicht fortgesetzt.
- Ein erneutes Laden des Switches war erforderlich, um den gesperrten Pufferstatus zu löschen.

Dieses Verhalten wird im Cisco Bug CSCwm14612 dokumentiert, der beschreibt, wie überwältigende Pausen-Frames dazu führen, dass die Schnittstelle fälschlicherweise Puffer hält, was zu Ausgabeverringerungen führt.

Auflösung

Die Eingangsflusskontrolle wurde an der betroffenen Switch-Schnittstelle mithilfe des folgenden Befehls deaktiviert:

<#root>

```
Switch#configure terminal
```

```
Switch(config)#interface GigabitEthernet 1/0/5
Switch(config-if)#
```

```
flowcontrol receive off
```

Schlussfolgerung

Die zeitweiligen Netzwerkverbindungsfehler und Paketverluste zwischen dem Cisco C9200L-Switch und der Firewall wurden durch ein Blockieren der Softwarewarteschlange verursacht, das durch ein übermäßiges Volumen von 802,3x Pause-Frames ausgelöst wurde. Durch Deaktivieren der Eingangsflusssteuerung an der Switch-Schnittstelle wurde das Problem behoben, indem verhindert wurde, dass die Warteschlange voll ausgelastet und gesperrt wurde.

Zugehörige Informationen

- Fehlerbehebung für verworfene Ausgangspakete auf Switches der Catalyst 9000-Serie
- Fehlerbehebung bei STP-Problemen mit Catalyst Switches
- Fehlerbehebung bei MAC Flaps/Loop auf Cisco Catalyst Switches
- 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.