Problemen oplossen Netwerklatentie en pakketdrops op Catalyst 9000-Switches

Inleiding

In dit document wordt een uitgebreide methodologie beschreven voor het oplossen van problemen met netwerklatentie en pakketverlies op switches uit de Cisco Catalyst 9000-reeks.

Voorwaarden

Vereisten

Cisco raadt u aan een fundamenteel begrip te hebben van netwerkconcepten, waaronder TCP / IP, VLAN's en Spanning Tree Protocols (STP's). Kennis van Cisco Catalyst 9000 Series switches en de Cisco IOS® XE CLI is van essentieel belang. Ook moet u vertrouwd zijn met netwerkbewakingstools en toegangsrechten voor configuratie en diagnostiek.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Catalyst 9000-Switches met alle versies. Dit document is niet beperkt tot specifieke software- of hardwareversies.

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

Dit document is bedoeld voor netwerkbeheerders en technici en biedt richtlijnen voor het efficiënt identificeren, isoleren en oplossen van deze problemen binnen bedrijfsnetwerkomgevingen. Netwerklatentie en pakketverlies kunnen de prestaties en betrouwbaarheid in bedrijfsomgevingen nadelig beïnvloeden. Deze problemen zijn vaak het gevolg van netwerkcongestie, verkeerde configuratie of omgevingsfactoren. De switches uit de Cisco Catalyst 9000-reeks zijn ontworpen

voor hoge prestaties en veerkracht. Dit document bevat gerichte stappen voor probleemoplossing om netwerkprofessionals te helpen bij het identificeren en oplossen van problemen met latentie en pakketverlies met behulp van deze switches.

Netwerklatentie en pakketdrops begrijpen

Netwerklatentie

Netwerklatentie is de meting van vertraging die wordt ervaren wanneer gegevens een netwerk van bron naar bestemming doorkruisen. Meestal wordt latentie uitgedrukt als RTT (Round Trip Time) - de tijd die een pakket nodig heeft om van de bron naar de bestemming en terug te reizen.

Latentie wordt meestal gemeten in milliseconden (ms).

Impact: hoge latentie kan de prestaties van toepassingen verminderen, vooral voor protocollen zoals TCP, die afhankelijk zijn van tijdige bevestigingen om gegevens efficiënt te verzenden.

Packet Drops

Packet drops treden op wanneer netwerkapparaten niet in staat zijn om pakketten door te sturen naar hun beoogde bestemming, vaak als gevolg van congestie, bufferoverlopen, verkeerde configuraties of defecte hardware. Packet drops worden meestal gemeten als een percentage van verloren pakketten over een specifiek interval.

Impact: pakketdalingen verminderen de doorvoer, veroorzaken hertransmissies en kunnen de betrouwbaarheid van toepassingen verstoren.

Benchmarks voor verwachte latentie

Netwerktype	Typische RTT
Zelfde VLAN (toegangslaag)	< 1 ms
Campus Core Traversal	1 – 5 ms
Metro WAN	5 – 30 ms

Internet/WAN	30 – 150 ms

Opmerking: de geografische afstand tussen de netwerkhops kan de RTT verhogen en bijdragen aan een hogere latentie.

Netwerklatentie meten

Begin met het grondig begrijpen van uw netwerk en de topologie ervan. Wanneer uw netwerk is ontworpen met deterministische variabelen en minimale onvoorspelbaarheid, wordt het proces van het identificeren en oplossen van latentie- en pakketvalproblemen aanzienlijk eenvoudiger.

Twee belangrijke hulpmiddelen worden meestal gebruikt om netwerklatentie te meten.

pingelen

Het retourneert als uitvoer of een bestemming bereikbaar is, samen met statistieken over pakketverlies en RTT. Zodra u de problematische hop identificeert, kunt u proberen rechtstreeks tussen hen te pingen en de apparaten in te checken om het probleem te vinden.

<#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

traceroute

Traceroute toont alle hops in het routeringspad van bron naar bestemming, samen met RTT-resultaten voor elke hop. Een traceroute kan bijvoorbeeld laten zien waar in het netwerk (welke hop in het routeringspad) de vertraging bestaat of begint. Een dergelijk voorbeeld wordt getoond in de volgende traceroute-uitvoer.

<#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.
```

Deze output wijst op een waarschijnlijke vertraging bij hop 3, zoals blijkt uit een aanzienlijke toename van de RTT tussen hop 2 en hop 3. Het relatief kleine tijdsverschil tussen hop 3 en hop 4 wijst erop dat de uitgifte gelokaliseerd is in het segment tussen 20.20.20.20 en 30.30.30.30.

Oorzaken van latentie en Packet Drops

Problemen met laag 1 (fysieke laag)

Layer 1-problemen zijn een veelvoorkomende bron van netwerklatentie en pakketdalingen. Het is belangrijk om deze aspecten te verifiëren op de fysieke laag:

- Controleer of duplex- en snelheidsinstellingen correct zijn geconfigureerd op alle interfaces.
- Controleer interfaces op CRC, invoerfouten, die kunnen wijzen op problemen met de fysieke laag.
- Defecte netwerkkabels, glasvezelverbindingen, SFP-modules of switch-poorten kunnen ook leiden tot pakketvertragingen en -dalingen.


```
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
...
```

Uitgangsdruppels

Uitgangsdalingen treden op wanneer een zendwachtrij van een switch-interface vol is en geen extra pakketten kan doorsturen. Dit kan leiden tot verhoogde latentie als pakketten in de wachtrij wachten en kan ook leiden tot pakketdalingen als de wachtrij overloopt, wat van invloed is op de prestaties van toepassingen en de betrouwbaarheid van het netwerk.

<#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
...
```

De Total output drops teller toont een groot aantal gevallen pakketten, wat wijst op congestie of wachtrij overflow op deze interface. Dit kan leiden tot verhoogde latentie en pakketverlies, wat de prestaties van het netwerk en de toepassingen beïnvloedt.

STP-stabiliteit

STP-instabiliteit kan aanzienlijk bijdragen aan netwerklatentie en pakketdalingen. In een stabiel netwerk moeten topologische veranderingen minimaal zijn. Frequente veranderingen in de

topologie kunnen wijzen op onderliggende problemen en kunnen normale doorstuurbewerkingen verstoren.

Belangrijkste overwegingen voor het minimaliseren van STP-gerelateerde latentie:

Overmatige veranderingen in de STP-topologie kunnen ertoe leiden dat het MAC-adres van de switch (CAM)-tabel vaak wordt doorgespoeld, wat leidt tot meer uitzendverkeer en latentie, omdat switches onbekende unicastpakketten overspoelen totdat de tabel opnieuw wordt gevuld.

Edge Port Configuration: zorg ervoor dat alle Edge-poorten zijn geconfigureerd met PortFast. Door PortFast in te schakelen, worden STP Topology Change Notifications (TCN's) niet gegenereerd wanneer clients of servers verbinding maken of de verbinding verbreken, waardoor onnodige veroudering van de CAM-tabel wordt verminderd en de stabiliteit wordt verbeterd.

Root-brug Planning: handmatig plannen en toewijzen van STV-root-brug en -prioriteiten om een voorspelbare netwerktopologie te behouden en overbodige topologische wijzigingen te minimaliseren.

Wanneer een topologiewijziging optreedt (zoals een poortovergangsstatus), stuurt de switch een TCN-BPDU naar de root-brug. De root-brug verspreidt vervolgens TCN-BPDU's naar alle switches en vraagt hen om hun verouderingstijd van het MAC-adres te verkorten van de standaardwaarde (300 seconden) tot de waarde Forward Delay (meestal 15 seconden). Dit zorgt ervoor dat onlangs inactieve inzendingen worden doorgespoeld, wat resulteert in meer onbekende unicasts en verhoogde overstromingen in het hele netwerk.

<#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-lussen

MAC flapping / Layer 2 loops veroorzaken netwerklatentie en pakketdalingen door de MAC-adrestabel voortdurend bij te werken met dezelfde bron-MAC op verschillende poorten. Deze constante verandering verstoort het doorsturen van verkeer, wat leidt tot onderbrekingen en pakketverlies. Layer 2-lussen verergeren het probleem door broadcast-pakketten te veroorzaken om eindeloos te circuleren, waardoor meer MAC-flapping en verdere verslechtering van de netwerkprestaties worden veroorzaakt. Het implementeren van looppreventieprotocollen zoals STP is essentieel om een stabiele netwerkwerking te behouden en deze problemen te voorkomen.

Om MAC-verzetmelding te configureren, gebruikt u de opdracht mac-adrestabelmelding mac-move in globale configuratiemodus.

<#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
```

Flow Control

Wanneer de stroomregeling is ingeschakeld en een ontvangstbuffer van een switch nadert, stuurt de switch pauzeframes om het binnenkomende verkeer tijdelijk te stoppen. Dit proces kan de latentie verhogen omdat de gegevensoverdracht met tussenpozen wordt onderbroken. Omgekeerd, als flow control niet is ingeschakeld of upstream-apparaten pauzeframes niet respecteren, kan inkomend verkeer de buffercapaciteit overschrijden, wat resulteert in bufferoverschrijdingen en pakketdalingen.

Flow control moet zorgvuldig worden geconfigureerd, rekening houdend met de mogelijkheden van alle apparaten in het verkeerspad. Onjuist gebruik of verkeerde configuratie kan leiden tot verhoogde latentie en pakketdalingen, wat een negatieve invloed heeft op de prestaties van toepassingen.

<#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-gebruik

Een hoog CPU-gebruik kan leiden tot verhoogde netwerklatentie en pakketdalingen. Wanneer de processor zwaar is belast, kan de switch het vliegverkeer, de routeringsupdates of de beheerfuncties niet efficiënt verwerken. Dit kan het doorsturen van pakketten vertragen, time-outs veroorzaken voor protocollen zoals ARP of Spanning Tree en resulteren in gedropte pakketten, vooral voor verkeer waarvoor CPU-interventie vereist is.

<#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
```

Geheugengebruik

Een hoog geheugengebruik kan latentie en pakketverlies veroorzaken door de CPU te overbelasten en de processen van het controlevliegtuig te beheersen. Deze overbelasting vertraagt de afhandeling van routeringsupdates, QoS-beleid en bufferbeheer, wat leidt tot congestie in de pakketverwerkingspijplijn. Pakketten kunnen worden weggelaten of vertraagd. Een hoog geheugengebruik heeft dus invloed op de netwerkprestaties door de efficiëntie van de switch bij het beheer van het verkeer te verminderen.

<#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-omleidingen en onbereikbare berichten

Wanneer een pakket op een Layer 3-interface aankomt en uit dezelfde interface wordt gerouteerd, genereert de switch een ICMP-omleidingsbericht om de bron te informeren over een efficiëntere volgende hop op hetzelfde subnet. Dit zorgt ervoor dat het originele pakket tweemaal door het vLAN loopt, waardoor het gebruik van de bandbreedte toeneemt. Bovendien verbruikt het ICMP-omleidingspakket zelf bandbreedte en vereist het CPU-verwerking, wat kan leiden tot CPU-onderbrekingen en verhoogde latentie. Als veel van dergelijke omleidingen plaatsvinden, vooral tijdens zwaar verkeer, kan de CPU-belasting aanzienlijk stijgen, wat mogelijk leidt tot pakketdalingen.

Frequente generatie en verwerking van onbereikbare ICMP-berichten kan ook het CPU-gebruik verhogen, waardoor de netwerkprestaties worden beïnvloed. Hoge volumes van ICMP-onbereikbaar verkeer verbruiken CPU-bronnen, wat kan leiden tot latentie en pakketdalingen.

Om deze effecten te beperken, raadt Cisco aan om ICMP-onbereikbare berichten en ICMP-omleidingen op Switch Virtual Interfaces (SVI's) en Layer 3-interfaces uit te schakelen met behulp van de opdrachten no ip unreach ables en no ip redirects. Deze best practice verlaagt de CPU-belasting en verbetert de netwerkstabiliteit.

<#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


...
```

verkeersstormen

Een verkeersstorm treedt op wanneer overmatige broadcast-, multicast- of unicastpakketten een LAN overspoelen, de bronnen van de switch overweldigen en de netwerkprestaties verminderen.

Stormbesturing op switches bewaakt uitzend-, multicast- en unicastverkeer op fysische interfaces en vergelijkt dit met geconfigureerde drempelwaarden. Wanneer het verkeer deze limieten overschrijdt, blokkeert de switch tijdelijk het overmatige verkeer om netwerkdegradatie te voorkomen. Dit beschermt de bronnen van de switch en zorgt ervoor dat het netwerk stabiel blijft en blijft presteren.

<#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 vs ARP Verouderingstijd

De verouderingstijd van de CAM (MAC Address Table) ten opzichte van het Address Resolution Protocol (ARP) kan ook leiden tot netwerklatentie en pakketdalingen. Dit gebeurt omdat de CAM-tabel, die MAC-adres naar poorttoewijzingen opslaat, meestal sneller veroudert (standaard ongeveer vijf minuten) dan de ARP-tabel, die IP naar MAC-adrestoewijzingen opslaat (standaard ongeveer vier uur). Wanneer een MAC-adres ouder wordt uit de CAM-tabel, maar nog steeds bestaat in de ARP-tabel, weet de switch niet langer de specifieke poort om unicast-verkeer voor dat MAC-adres door te sturen. Als gevolg hiervan stroomt de switch het unicastverkeer naar alle poorten in het VLAN, waardoor netwerkcongestie en mogelijk pakketverlies ontstaan.

Hoe CAM vs ARP Aging Time Latency en Packet Drops veroorzaakt

- Wanneer het CAM-tabelitem veroudert voordat het ARP-item wordt ingevoerd, worden unicastpakketten door de switch overspoeld omdat de MAC-naar-poorttoewijzing ontbreekt.
- Deze overstroming verhoogt de CPU-belasting en verbruikt onnodig bandbreedte, wat leidt tot netwerklatentie en pakketdalingen.
- De mismatch kan ook leiden tot inefficiënte forwarding en verhoogde controle vliegtuig verwerking.

<#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
```

Monitorsessie

Wanneer actieve monitorsessies (SPAN) worden geconfigureerd op een switch met meerdere bron- en bestemmingspoorten, kunnen deze bijdragen aan netwerklatentie en pakketdalingen.

<#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)

Hoe SPAN werkt

SPAN (Switched Port Analyzer) is een hardwareondersteunde functie die verkeer van bronpoorten naar bestemmingspoorten spiegelt zonder CPU-opzoekingen te betrekken. De ASIC-replicatie op de supervisor-module behandelt pakketmirroring, terwijl de forwarding-engine de gespiegelde pakketten omleidt naar de bestemmingspoorten. Gespiegelde pakketten worden geschakeld met dezelfde timing als het reguliere verkeer.

Impact van meerdere bron- en bestemmingspoorten:

In het eerdere voorbeeld moet de switch verkeer repliceren van alle broninterfaces naar de doelinterfaces. Het verkeer van interface Po170 wordt bijvoorbeeld gespiegeld en twee keer doorgestuurd naar twee verschillende bestemmingen. Deze replicatie verhoogt de belasting op de forwarding-engine en kan congestie in de backplane van de switch veroorzaken.

- Als een Port-channel drie GBPS aan verkeer heeft, kan het repliceren van dit verkeer naar meerdere bestemmingen resulteren in meer dan 15 GBPS aan gespiegeld verkeer.
- De belasting op de ASIC-replicatie neemt evenredig toe met de verkeerssnelheid op broninterfaces.
- Bij lagere verkeerssnelheden kan de latentie-impact minimaal zijn, maar naarmate het verkeer toeneemt, kunnen latentie en congestie aanzienlijk worden.

Uitzonderingen op ASIC-niveau

Gebruik deze opdracht om de interface te controleren op ASIC-toewijzingen, die de ASIC-instantie toont waar de interface zich bevindt.

<#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)

Als de ASIC-instantie is geïdentificeerd, voert u de volgende opdracht uit om de uitzonderingen voor het doorsturen van de ASIC-drop voor die ASIC te bekijken.

<#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
...
```

Softwarebugs

Softwarebugs kunnen soms direct of indirect onbedoeld en onverwacht gedrag veroorzaken. Deze bugs kunnen leiden tot problemen zoals netwerklatentie, pakketdalingen of andere verslechtering van de prestaties. Om deze problemen aan te pakken, is een gemeenschappelijke eerste stap het herladen van de switch, die voorbijgaande fouten kan wissen en de normale werking kan herstellen. Daarnaast is het van cruciaal belang om uw apparaten up-to-date te houden door regelmatig de nieuwste firmware- en software-updates toe te passen. Deze updates bevatten vaak oplossingen voor bekende bugs en verbeteringen die de stabiliteit en prestaties van het apparaat verbeteren, waardoor problemen met betrekking tot softwarefouten worden voorkomen.

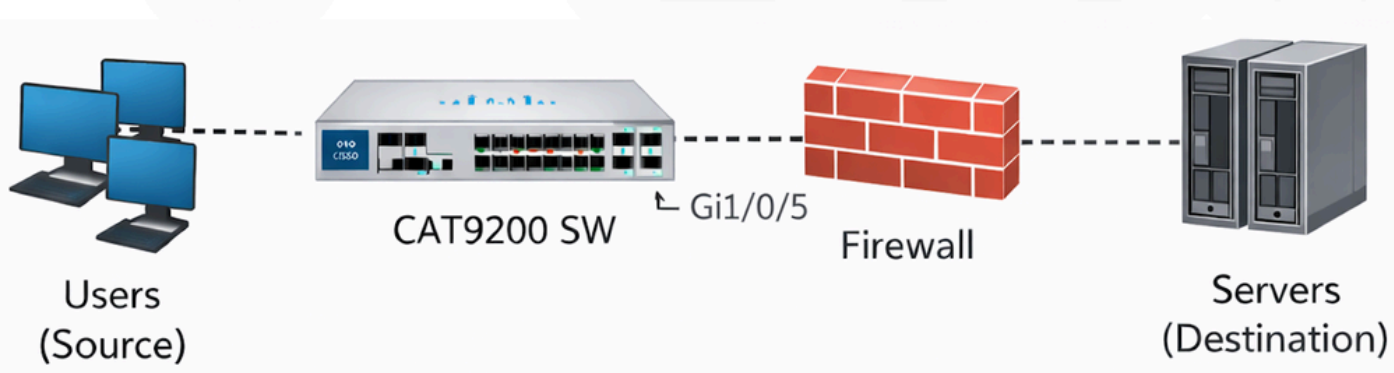
Cisco Bug Search Tool

casestudy

Probleemdetails

Gebruikers ondervinden intermitterend verlies van netwerkconnectiviteit tijdens pogingen om grote hoeveelheden gegevens over te dragen via vLAN's, zoals tijdens bestandsoverdracht met hoge capaciteit. Deze onderbrekingen manifesteren zich als sporadische fouten in gegevensoverdracht ondanks meerdere succesvolle pogingen, wat de betrouwbaarheid van het netwerk en de prestaties van de toepassing aanzienlijk beïnvloedt. Het probleem wordt tijdelijk opgelost door de switch opnieuw te laden.

Topologie



Symptomen waargenomen

- Bestandsoverdrachten tussen de bron en de bestemming mislukken na verschillende succesvolle pogingen.
- De switch verliest de connectiviteit met de firewall tijdens storingsperioden.
- 802.1X-verificatie blijft tijdens de incidenten operationeel.
- De switch blijft tijdens de incidenten via de console reageren.
- De verbonden poort van de firewall toont alleen uitzendverkeer tijdens storingsperioden.
- Diagnostische tests (DiagGoldSpotTest) mislukken consequent op interface Gi1/0/5, wat wijst op een gegevenspad probleem.

Problemen oplossen uitgevoerd

- Interfacetellers en bufferstatistieken op platformniveau worden beoordeeld.
- De switch-interface Gi1/0/5 toont een zeer groot aantal 802.3x pauzeframes die van de firewall zijn ontvangen.
- Uitgangsdalingen en pauzeframestatistieken worden nauwlettend gevolgd.
- Platform software forwarding engine queue statistieken worden onderzocht om buffergedrag te identificeren.
- De instellingen voor de stroombesturing in de switch-interface worden gecontroleerd.

Relevante interfacestatistieken

<#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

Oorzaak geïdentificeerd

De hoofdoorzaak werd vastgesteld als buffervergrendeling vanwege te hoge 802.3x-pauzeframes die door de firewall naar de switch-interface werden verzonden. Ethernet-pauzeframes instrueren de switch om te stoppen met verzenden zodat het ontvangende apparaat zich kan herstellen van congestie. Wanneer pauzeframes echter herhaaldelijk of voor langere tijd worden verzonden:

- De uitvoerwachtrij van de interfacebuffer voor de switch raakt volledig verzadigd.
- De switch blijft binnenkomende pakketten accepteren die bestemd zijn voor de gepauzeerde interface, die zich ophopen in de uitvoerwachtrij.
- De verzadiging van de wachtrij leidt tot outputdalingen en het blokkeren van het verkeer.
- In dit geval werden de buffers vergrendeld en werd het doorsturen niet hervat, zelfs niet nadat de pauzeframesnelheid was afgenomen.
- Een herladen van de switch was vereist om de vergrendelde bufferstatus te wissen.

Dit gedrag is gedocumenteerd in Cisco-bug CSCwm14612 die beschrijft hoe overweldigende pauzeframes ervoor zorgen dat de interface buffers verkeerd vasthoudt, wat resulteert in uitvoerdalingen.

resolutie

Invoerstroombesturing is uitgeschakeld in de betreffende switch-interface met de opdracht:

<#root>

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

flowcontrol receive off

Conclusie

De intermitterende netwerkconnectiviteitsfouten en pakketdalingen tussen de Cisco C9200L-switch en Firewall werden veroorzaakt door een blokkering van de softwarewachtrij die werd veroorzaakt door een te groot aantal 802.3x pauzeframes. Het uitschakelen van de

invoerstroombesturing op de switch-interface loste het probleem op door te voorkomen dat de wachtrij verzadigd en vergrendeld raakte.

Gerelateerde informatie

- Afwijzingen in de uitvoer op Catalyst 9000-switches oplossen
- Problemen met STP op katalysatorSwitches oplossen
- Problemen oplossen met MAC Flaps/Loop op Cisco Catalyst-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.