Dépannage de la latence réseau et des pertes de paquets sur les commutateurs Catalyst 9000

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Présentation de la latence réseau et des pertes de paquets
  - Latence réseau
  - Abandons de paquets
  - Tests de latence prévus
- Mesurer la latence du réseau
  - Ping
  - Traceroute
- Causes courantes de latence et de perte de paquets
  - Problèmes de couche 1 (couche physique)
  - Pertes en sortie
  - Stabilité STP
  - Flap MAC/boucles de couche 2
  - Contrôle de flux
  - Utilisation du processeur
  - Utilisation de la mémoire
  - Redirections ICMP et messages inaccessibles
  - Tempêtes de trafic
  - Temps de vieillissement CAM et ARP
  - Comment le temps de vieillissement CAM et ARP provoque la latence et les pertes de paquets
  - Surveiller la session
  - Fonctionnement de SPAN
  - Exceptions de niveau ASIC
  - Bogues logiciels
- Étude de cas
  - Détails du problème
  - Topologie
  - Symptômes observés
  - Dépannage effectué
  - Statistiques d'interface pertinentes
  - Cause racine identifiée
  - Résolution

Conclusion

Informations connexes

Introduction

Ce document décrit une méthodologie détaillée de dépannage des problèmes de latence réseau et de perte de paquets sur les commutateurs de la gamme Cisco Catalyst 9000.

Conditions préalables

Exigences

Cisco recommande que vous ayez une compréhension fondamentale des concepts de réseau, y compris TCP/IP, les VLAN et les protocoles STP (Spanning Tree Protocol). Il est essentiel de connaître les commutateurs de la gamme Cisco Catalyst 9000 et l'interface de ligne de commande Cisco IOS® XE. Une bonne connaissance des outils de surveillance du réseau et des privilèges d'accès pour la configuration et les diagnostics est également requise.

Composants utilisés

Les informations contenues dans ce document sont basées sur les commutateurs Cisco Catalyst 9000 avec toutes les versions. Ce document n'est pas limité à des versions logicielles ou matérielles spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document s'adresse aux administrateurs et ingénieurs réseau et leur fournit des conseils pour identifier, isoler et résoudre efficacement ces problèmes dans les environnements réseau d'entreprise. La latence du réseau et la perte de paquets peuvent nuire aux performances et à la fiabilité des environnements d'entreprise. Ces problèmes sont souvent dus à un encombrement du réseau, à une mauvaise configuration ou à des facteurs environnementaux. Les commutateurs de la gamme Cisco Catalyst 9000 sont conçus pour offrir des performances et une résilience élevées. Ce document fournit des étapes de dépannage ciblées pour aider les professionnels du réseau à identifier et à résoudre les problèmes de latence et d'abandon de paquets à l'aide de ces

commutateurs.

Présentation de la latence réseau et des pertes de paquets

Latence réseau

La latence du réseau est la mesure du délai subi par les données lorsqu'elles traversent un réseau de la source à la destination. Le plus souvent, la latence est exprimée sous la forme de temps de parcours aller-retour (RTT, Round Trip Time), c'est-à-dire le temps nécessaire à un paquet pour voyager de la source à la destination et inversement.

La latence est généralement mesurée en millisecondes (ms).

Incidence: Une latence élevée peut dégrader les performances des applications, en particulier pour les protocoles tels que TCP, qui s'appuient sur des accusés de réception opportuns pour envoyer efficacement les données.

Abandons de paquets

Les pertes de paquets se produisent lorsque les périphériques réseau ne peuvent pas transférer les paquets vers leur destination, souvent en raison d'un encombrement, de débordements de mémoire tampon, de configurations incorrectes ou d'un matériel défectueux. Les abandons de paquets sont généralement mesurés en pourcentage de paquets perdus sur un intervalle spécifique.

Impact : les pertes de paquets réduisent le débit, provoquent des retransmissions et peuvent perturber la fiabilité des applications.

Tests de latence prévus

Type de réseau	RTT type
Même VLAN (couche d'accès)	< 1 ms
Traversée du coeur du campus	1 à 5 ms
WAN métropolitain	5 à 30 ms

Internet/WAN	30 à 150 ms

Remarque : La distance géographique entre les sauts de réseau peut augmenter le RTT et contribuer à une latence plus élevée.

Mesurer la latence du réseau

Commencez par bien comprendre votre réseau et sa topologie. Lorsque votre réseau est conçu avec des variables déterministes et une imprévisibilité minimale, le processus d'identification et de résolution des problèmes de latence et de perte de paquets devient beaucoup plus simple.

Deux outils principaux sont généralement utilisés pour mesurer la latence du réseau.

Ping

Il indique si une destination est accessible, ainsi que des statistiques sur la perte de paquets et le délai d’attente. Dès que vous identifiez les sauts problématiques, vous pouvez essayer d'envoyer une requête ping entre eux directement et d'enregistrer les périphériques afin de trouver le problème.

<#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

La commande traceroute affiche tous les sauts du chemin de routage de la source à la destination, ainsi que les résultats RTT pour chaque saut. Par exemple, une commande traceroute peut indiquer où le délai existe ou commence dans le réseau (le saut dans le chemin de routage). Un tel exemple est illustré dans la sortie traceroute suivante.

<#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.
```

Ce résultat indique un délai probable au saut 3, comme le montre une augmentation significative de la durée de transmission entre le saut 2 et le saut 3. La différence de temps relativement faible entre le saut 3 et le saut 4 suggère que le problème est localisé sur le segment entre 20.20.20.20 et 30.30.30.

Causes courantes de latence et de perte de paquets

Problèmes de couche 1 (couche physique)

Les problèmes de couche 1 sont une source courante de latence réseau et de pertes de paquets. Il est important de vérifier ces aspects au niveau de la couche physique :

- Vérifiez que les paramètres duplex et de vitesse sont correctement configurés sur toutes les interfaces.
- Recherchez sur les interfaces des erreurs CRC en entrée, qui peuvent indiquer des problèmes de couche physique.
- Des câbles réseau, des connexions à fibre optique, des modules SFP ou des ports de commutation défectueux peuvent également provoquer des retards et des pertes de paquets.

<#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
  ...
  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
...
```

Pertes en sortie

Les pertes de sortie se produisent lorsqu'une file d'attente de transmission d'une interface de commutateur est pleine et ne peut pas transférer des paquets supplémentaires. Cela peut entraîner une latence accrue lorsque des paquets attendent dans la file d'attente et peut également entraîner des pertes de paquets si la file d'attente déborde, ce qui a un impact sur les performances des applications et la fiabilité du réseau.

<#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
...
```

Le compteur Total des abandons en sortie affiche un grand nombre de paquets abandonnés, indiquant un encombrement ou un dépassement de la file d'attente sur cette interface. Cela peut augmenter la latence et la perte de paquets, ce qui affecte les performances du réseau et des applications.

Stabilité STP

L’instabilité du protocole STP peut contribuer de manière significative à la latence du réseau et aux abandons de paquets. Dans un réseau stable, les modifications de topologie doivent être minimales. Les modifications fréquentes de la topologie peuvent indiquer des problèmes sous-jacents et perturber les opérations de transfert normales.

Considérations clés pour minimiser la latence liée au protocole STP :

Modifications de topologie (TCN) : Des modifications excessives de la topologie STP peuvent entraîner le vidage fréquent de l'adresse MAC de la table de commutation (CAM), entraînant une augmentation du trafic de diffusion et de la latence lorsque les commutateurs inondent des paquets de monodiffusion inconnus jusqu'à ce que la table soit à nouveau remplie.

Configuration du port de périphérie : Vérifiez que tous les ports de périphérie sont configurés avec PortFast. L'activation de PortFast empêche la génération de notifications de modification de topologie STP (TCN) lorsque des clients ou des serveurs se connectent ou se déconnectent, ce qui réduit le vieillissement inutile de la table CAM et améliore la stabilité.

Planification du pont racine : Planifiez et attribuez manuellement les priorités et le pont racine STP afin de maintenir une topologie de réseau prévisible et de minimiser les modifications de topologie inutiles.

Lorsqu’une modification de topologie se produit (par exemple, un état de transition de port), le commutateur envoie une trame BPDU TCN vers le pont racine. Le pont racine propage ensuite les trames TCN BPDU à tous les commutateurs, en les invitant à raccourcir le délai de vieillissement de leur adresse MAC de la valeur par défaut (300 secondes) à la valeur Forward Delay (généralement 15 secondes). Cela entraîne le vidage des entrées récemment inactives, ce qui entraîne un plus grand nombre de monodiffusions inconnues et une inondation accrue sur le réseau.

<#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

Flap MAC/boucles de couche 2

Le battement MAC/les boucles de couche 2 entraînent une latence réseau et des pertes de paquets en mettant à jour continuellement la table d'adresses MAC avec le même MAC source sur différents ports. Ce changement constant interrompt le transfert du trafic, ce qui entraîne des interruptions et des pertes de paquets. Les boucles de couche 2 aggravent le problème en provoquant la circulation sans fin des paquets de diffusion, ce qui entraîne un plus grand battement MAC et une dégradation supplémentaire des performances du réseau. La mise en oeuvre de protocoles de prévention des boucles tels que STP est essentielle pour maintenir un fonctionnement stable du réseau et éviter ces problèmes.

Afin de configurer la notification de déplacement MAC, utilisez la commande mac address-table notification mac-move en mode de configuration globale.

<#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
```

Contrôle de flux

Lorsque le contrôle de flux est activé et qu'une mémoire tampon de réception d'un port de commutateur approche de sa capacité, le commutateur envoie des trames de pause pour arrêter temporairement le trafic entrant. Ce processus peut augmenter la latence lorsque la transmission de données est interrompue par intermittence. Inversement, si le contrôle de flux n'est pas activé ou si les périphériques en amont n'acceptent pas les trames de pause, le trafic entrant peut dépasser la capacité de la mémoire tampon, ce qui entraîne des dépassements de mémoire tampon et des pertes de paquets.

Le contrôle de flux doit être configuré avec soin, en tenant compte des capacités de tous les périphériques dans le chemin de trafic. Une mauvaise utilisation ou une mauvaise configuration peut entraîner une augmentation de la latence et des pertes de paquets, ce qui a un impact négatif sur les performances des applications.


```
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
```

Utilisation du processeur

Une utilisation CPU élevée peut entraîner une augmentation de la latence du réseau et des pertes de paquets. Lorsque le processeur est fortement chargé, le commutateur ne peut pas traiter efficacement le trafic du plan de contrôle, les mises à jour de routage ou les fonctions de gestion. Cela peut retarder le transfert de paquets, provoquer des délais d'attente pour des protocoles comme ARP ou Spanning Tree et entraîner l'abandon de paquets, en particulier pour le trafic qui nécessite une intervention du processeur.

```
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
```

Utilisation de la mémoire

Une utilisation élevée de la mémoire peut entraîner une latence et des pertes de paquets en surchargeant les processus du processeur et du plan de contrôle. Cette surcharge retarde la gestion des mises à jour de routage, des stratégies QoS et de la gestion des tampons, ce qui entraîne un encombrement du pipeline de traitement des paquets. Par conséquent, les paquets peuvent être abandonnés ou retardés. Ainsi, une utilisation élevée de la mémoire affecte les performances du réseau en réduisant l'efficacité du commutateur dans la gestion du trafic.

<#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
```

Redirections ICMP et messages inaccessibles

Lorsqu'un paquet arrive sur une interface de couche 3 et est acheminé à partir de la même interface, le commutateur génère un message de redirection ICMP afin d'informer la source d'un saut suivant plus efficace sur le même sous-réseau. Le paquet d'origine traverse donc le réseau local virtuel deux fois, ce qui augmente l'utilisation de la bande passante. En outre, le paquet de redirection ICMP lui-même consomme de la bande passante et nécessite un traitement CPU, ce qui peut entraîner des interruptions CPU et une latence accrue. Si un grand nombre de ces redirections se produisent, en particulier lors d'un trafic important, la charge du processeur peut augmenter considérablement, ce qui peut entraîner des pertes de paquets.

La génération et le traitement fréquents de messages ICMP inaccessibles peuvent également augmenter l'utilisation du processeur, affectant ainsi les performances du réseau. Des volumes élevés de trafic ICMP inaccessible consomment les ressources du processeur, ce qui peut entraîner une latence et des pertes de paquets.

Afin d'atténuer ces effets, Cisco recommande de désactiver les messages ICMP inaccessibles et les redirections ICMP sur les interfaces virtuelles de commutateur (SVI) et les interfaces de couche 3 en utilisant les commandes no ip unreachables et no ip redirects. Cette meilleure pratique réduit la charge du processeur et améliore la stabilité du réseau.

<#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

```
...
```

Tempêtes de trafic

Une tempête de trafic se produit lorsque des paquets de diffusion, de multidiffusion ou de monodiffusion excessifs inondent un réseau local, saturant les ressources du commutateur et dégradant les performances du réseau.

Le contrôle des tempêtes sur les commutateurs surveille le trafic de diffusion, multidiffusion et monodiffusion sur les interfaces physiques et le compare aux seuils configurés. Lorsque le trafic dépasse ces limites, le commutateur bloque temporairement le trafic excessif afin d'empêcher la dégradation du réseau. Cela protège les ressources du commutateur et maintient la stabilité et les performances globales du réseau.

<#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
```

Temps de vieillissement CAM et ARP

Le temps d'obsolescence de la table d'adresses MAC par rapport au temps d'obsolescence du protocole ARP (Address Resolution Protocol) peut également entraîner une latence du réseau et des pertes de paquets. Cela se produit parce que la table CAM, qui stocke les mappages adresse MAC-port, expire généralement plus rapidement les entrées (par défaut, environ cinq minutes) que la table ARP, qui stocke les mappages adresse IP-adresse MAC (par défaut, environ quatre heures). Lorsqu'une adresse MAC vieillit hors de la table CAM mais qu'elle existe toujours dans la table ARP, le commutateur ne connaît plus le port spécifique pour transférer le trafic de monodiffusion pour cette adresse MAC. Par conséquent, le commutateur inonde le trafic de monodiffusion vers tous les ports du VLAN, provoquant un encombrement du réseau et une perte potentielle de paquets.

Comment le temps de vieillissement CAM et ARP provoque la latence et les pertes de paquets

- Lorsque l'entrée de la table CAM expire avant l'entrée ARP, le commutateur inonde les paquets de monodiffusion car il ne dispose pas du mappage MAC-port.
- Cette inondation augmente la charge du processeur et consomme inutilement de la bande passante, ce qui entraîne une latence du réseau et des pertes de paquets.
- La non-correspondance peut également entraîner un transfert inefficace et un traitement accru du plan de contrôle.

<#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

Surveiller la session

Lorsque des sessions de surveillance active (SPAN) sont configurées sur un commutateur avec plusieurs ports source et de destination, elles peuvent contribuer à la latence du réseau et aux pertes de paquets.

<#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)
```

Fonctionnement de SPAN

La fonctionnalité SPAN (Switched Port Analyzer) est une fonctionnalité assistée par matériel qui met en miroir le trafic des ports source vers les ports de destination sans impliquer de recherche de CPU. L'ASIC de réplication sur le module de supervision gère la mise en miroir des paquets, tandis que le moteur de transfert redirige les paquets mis en miroir vers les ports de destination. Les paquets mis en miroir sont commutés au même moment que le trafic normal.

Impact de plusieurs ports source et de destination :

Dans l’exemple précédent, le commutateur doit répliquer le trafic de toutes les interfaces source vers les interfaces de destination. Par exemple, le trafic de l'interface Po170 est mis en miroir et transféré deux fois vers deux destinations différentes. Cette réplication augmente la charge sur le moteur de transfert et peut entraîner un encombrement du fond de panier du commutateur.

- Si un canal de port transporte trois Gbit/s de trafic, la réplication de ce trafic vers plusieurs destinations peut entraîner plus de 15 Gbit/s de trafic en miroir.
- La charge sur l'ASIC de réplication augmente proportionnellement au débit du trafic sur les interfaces source.
- À des débits de trafic plus faibles, l'impact de la latence peut être minime, mais à mesure que le trafic augmente, la latence et la congestion peuvent devenir importantes.

Exceptions de niveau ASIC

Utilisez ces commandes afin de vérifier l'interface avec les mappages ASIC, qui montre l'instance ASIC où réside l'interface.

<#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)

Une fois l'instance ASIC identifiée, exécutez la commande suivante afin d'afficher les exceptions de suppression ASIC de transfert pour cet ASIC.

<#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
...
```

Bogues logiciels

Les bogues logiciels peuvent parfois provoquer directement ou indirectement des comportements inattendus. Ces bogues peuvent entraîner des problèmes tels que la latence du réseau, les pertes de paquets ou d'autres dégradations des performances. Afin de résoudre ces problèmes, une première étape commune consiste à recharger le commutateur, ce qui peut effacer les pannes transitoires et rétablir le fonctionnement normal. En outre, il est essentiel de maintenir vos périphériques à jour en appliquant régulièrement les dernières mises à jour du micrologiciel et des logiciels. Ces mises à jour incluent souvent des correctifs pour les bogues connus et des améliorations qui améliorent la stabilité et les performances des périphériques, ce qui aide à prévenir les problèmes liés aux défauts logiciels.

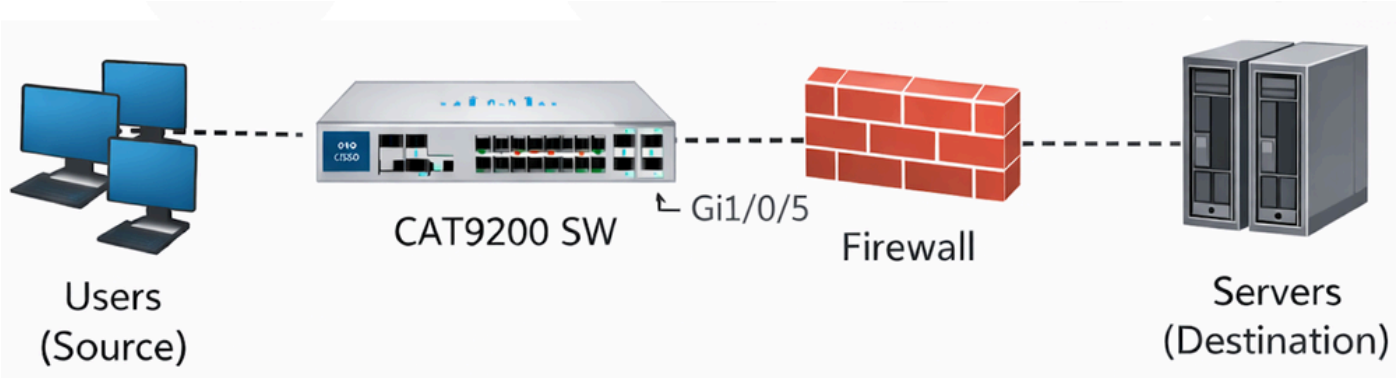
Outil de recherche de bogues Cisco

Étude de cas

Détails du problème

Les utilisateurs subissent des pertes de connectivité réseau intermittentes lors de tentatives de transfert de volumes importants de données sur des vLAN, par exemple lors de transferts de fichiers à haute capacité. Ces interruptions se traduisent par des pannes sporadiques dans la transmission des données malgré plusieurs tentatives réussies, ce qui a un impact significatif sur la fiabilité du réseau et les performances des applications. Le problème est temporairement résolu en rechargeant le commutateur.

Topologie



Symptômes observés

- Les transferts de fichiers entre la source et la destination échouent par intermittence après plusieurs tentatives réussies.
- Le commutateur perd la connectivité avec le pare-feu pendant les périodes de panne.
- L'authentification 802.1X reste opérationnelle tout au long des incidents.
- Le commutateur reste réactif via la console pendant les incidents.
- Le port connecté du pare-feu affiche uniquement le trafic de diffusion pendant les périodes de panne.
- Les tests de diagnostic (DiagGoldPktTest) échouent régulièrement sur l'interface Gi1/0/5, indiquant un problème de chemin de données.

Dépannage effectué

- Les compteurs d'interface et les statistiques de tampon au niveau de la plate-forme sont examinés.
- L'interface de commutateur Gi1/0/5 affiche un volume très élevé de trames de pause 802.3x reçues du pare-feu.
- Les pertes de sortie et les statistiques de trames de pause sont surveillées de près.
- Les statistiques de file d'attente du moteur de transfert du logiciel de plate-forme sont examinées pour identifier le comportement du tampon.
- Les paramètres de contrôle de flux sur l’interface du commutateur sont vérifiés.

Statistiques d'interface pertinentes

<#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 is 0

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

Cause racine identifiée

La cause principale a été identifiée comme le blocage de la mémoire tampon en raison d'un nombre excessif de trames de pause 802.3x envoyées par le pare-feu à l'interface du commutateur. Les trames de pause Ethernet indiquent au commutateur d'arrêter la transmission afin de permettre au périphérique récepteur de se rétablir de l'encombrement. Cependant, lorsque des trames de pause sont envoyées de façon répétée ou pendant des durées prolongées :

- La file d'attente de sortie de la mémoire tampon du commutateur pour l'interface devient complètement saturée.
- Le commutateur continue d'accepter les paquets entrants destinés à l'interface en pause, qui s'accumulent dans la file d'attente de sortie.
- La saturation de la file d'attente entraîne des pertes de sortie et un blocage du trafic.

- Dans ce cas, les tampons sont devenus verrouillés et le transfert n'a pas repris même après la diminution de la fréquence de trames de pause.
- Un rechargement du commutateur a été nécessaire pour effacer l'état de la mémoire tampon verrouillée.

Ce comportement est documenté dans le bogue Cisco CSCwm14612 qui décrit comment des trames de pause écrasantes provoquent une mise en mémoire tampon incorrecte de l'interface, ce qui entraîne des pertes de sortie.

Résolution

Le contrôle de flux en entrée a été désactivé sur l'interface du commutateur affecté à l'aide de la commande :

<#root>

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

flowcontrol receive off

Conclusion

Les pannes de connectivité réseau intermittentes et les pertes de paquets entre le commutateur Cisco C9200L et le pare-feu sont dues à un blocage de la file d'attente logicielle déclenché par un volume excessif de trames de pause 802.3x. La désactivation du contrôle de flux d'entrée sur l'interface du commutateur a résolu le problème en empêchant la file d'attente de devenir saturée et verrouillée.

Informations connexes

- Dépannage des pertes de sortie sur les commutateurs Catalyst 9000
- Dépannage de STP sur les commutateurs Catalyst
- Dépannage des flaps/boucles MAC sur les commutateurs Cisco Catalyst
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.