Risoluzione dei problemi di latenza della rete e perdita di pacchetti sugli switch Catalyst 9000

Introduzione

Questo documento descrive una metodologia dettagliata per la risoluzione dei problemi di latenza di rete e perdita di pacchetti sugli switch Cisco Catalyst serie 9000.

Prerequisiti

Requisiti

Cisco consiglia di avere una conoscenza di base dei concetti di rete, tra cui TCP/IP, VLAN e STP (Spanning Tree Protocol). La conoscenza degli switch Cisco Catalyst serie 9000 e della CLI di Cisco IOS® XE è essenziale. È inoltre richiesta la familiarità con gli strumenti di monitoraggio della rete e con i privilegi di accesso per la configurazione e la diagnostica.

Componenti usati

Per la stesura del documento, sono stati usati switch Cisco Catalyst 9000 di tutte le versioni. Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento è destinato agli amministratori e ai tecnici di rete e fornisce indicazioni per identificare, isolare e risolvere in modo efficiente questi problemi all'interno degli ambienti di rete aziendali. La latenza di rete e il packet drop possono influire negativamente sulle prestazioni e sull'affidabilità negli ambienti aziendali. Questi problemi spesso derivano da congestione della rete, configurazioni errate o fattori ambientali. Gli switch Cisco Catalyst serie 9000 sono progettati

per garantire prestazioni elevate e resilienza. In questo documento viene descritto come risolvere i problemi relativi alla latenza e alle perdite di pacchetti usando questi switch.

Informazioni sulla latenza di rete e le perdite di pacchetti

Latenza di rete

La latenza di rete è la misurazione del ritardo riscontrato quando i dati attraversano una rete dall'origine alla destinazione. In genere, la latenza viene espressa come Round Trip Time (RTT), il tempo necessario al pacchetto per viaggiare dalla sorgente alla destinazione e tornare indietro.

La latenza viene in genere misurata in millisecondi (ms).

Conseguenze: L'alta latenza può ridurre le prestazioni delle applicazioni, in particolare per protocolli come il TCP, che si basano su riconoscimenti tempestivi per inviare i dati in modo efficiente.

Perdite di pacchetti

Le perdite di pacchetti si verificano quando i dispositivi di rete non sono in grado di inoltrare i pacchetti alla destinazione prevista, spesso a causa di congestione, sovraccarico del buffer, configurazioni errate o hardware difettoso. Le perdite di pacchetti vengono in genere misurate come percentuale di pacchetti persi in un intervallo specifico.

Impatto: le perdite di pacchetti riducono il throughput, causano ritrasmissioni e possono compromettere l'affidabilità dell'applicazione.

Benchmark della latenza prevista

Tipo di rete	RTT standard
Stessa VLAN (livello di accesso)	< 1 ms
Campus Core Traversal	1 - 5 ms
Metro WAN	5 - 30 ms

Internet/WAN	30-150 ms

Nota: La distanza geografica tra gli hop della rete può aumentare il segnale RTT e contribuire a una latenza più elevata.

Misura latenza di rete

Comprendere innanzitutto a fondo la rete e la relativa topologia. Quando la rete è progettata con variabili deterministiche e imprevedibilità minima, il processo di identificazione e risoluzione dei problemi di latenza e di perdita dei pacchetti diventa notevolmente più semplice.

Per misurare la latenza della rete vengono in genere utilizzati due strumenti principali.

Ping

Restituisce come output se una destinazione è raggiungibile insieme alle statistiche sulla perdita di pacchetti e sull'RTT. Non appena si identificano gli hop con problemi, è possibile provare a eseguire il ping tra di essi direttamente e controllare i dispositivi per trovare il problema.

<#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

Il comando traceroute mostra tutti gli hop nel percorso di routing tra l'origine e la destinazione e i risultati RTT per ciascun hop. Ad esempio, un traceroute può mostrare dove nella rete (quale hop nel percorso di routing) inizia il ritardo. Questo esempio viene mostrato nell'output del comando traceroute successivo.

<#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.
```

Questo output indica un probabile ritardo all'hop 3, come evidenziato da un aumento significativo dell'RTT tra l'hop 2 e l'hop 3. La differenza di tempo relativamente piccola tra l'hop 3 e l'hop 4 suggerisce che il problema è localizzato sul segmento tra le ore 20.20.20.20 e le ore 30.30.30.30.

Cause comuni della latenza e delle perdite di pacchetti

Problemi relativi al layer 1 (livello fisico)

I problemi di layer 1 sono una causa comune di latenza di rete e perdita di pacchetti. È importante verificare questi aspetti a livello fisico:

- Verificare che le impostazioni duplex e la velocità siano configurate correttamente su tutte le interfacce.
- Controllare le interfacce per CRC, errori di input, che possono indicare problemi di livello fisico.
- Cavi di rete, connessioni in fibra, moduli SFP o porte dello switch difettosi possono causare ritardi e perdite dei pacchetti.

<#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
...
```

Cadute di output

Le perdite di output si verificano quando una coda di trasmissione di un'interfaccia dello switch è piena e non può inoltrare pacchetti aggiuntivi. Ciò può portare a una maggiore latenza durante l'attesa dei pacchetti in coda e può inoltre causare la perdita dei pacchetti in caso di overflow della coda, con conseguente impatto sulle prestazioni dell'applicazione e sull'affidabilità della rete.

<#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
...
```

Il contatore Totale eliminazioni di output consente di visualizzare un numero elevato di pacchetti ignorati, indicando congestione o overflow della coda su questa interfaccia. Ciò può comportare un aumento della latenza e la perdita di pacchetti, con effetti negativi sulle prestazioni della rete e delle applicazioni.

Stabilità STP

L'instabilità del protocollo STP può contribuire in modo significativo alla latenza della rete e alla

perdita di pacchetti. In una rete stabile, le modifiche alla topologia devono essere minime. Frequenti modifiche alla topologia possono indicare problemi di base e interrompere le normali operazioni di inoltro.

Considerazioni principali per ridurre al minimo la latenza relativa a STP:

Modifiche topologiche (TCN): Modifiche eccessive della topologia STP possono causare uno scaricamento frequente dell'indirizzo MAC della tabella dello switch (CAM), con conseguente aumento del traffico e della latenza di trasmissione, in quanto gli switch inviano pacchetti unicast sconosciuti fino a quando la tabella non viene ripopolata.

Configurazione porta Edge: Verificare che tutte le porte perimetrali siano configurate con PortFast. L'attivazione di PortFast impedisce la generazione di notifiche di modifica della topologia (TCN) STP quando i client o i server si connettono o si disconnettono, riducendo l'invecchiamento non necessario della tabella CAM e migliorando la stabilità.

Pianificazione bridge radice: Pianificare e assegnare manualmente il bridge radice STP e le relative priorità per mantenere una topologia di rete prevedibile e ridurre al minimo le modifiche non necessarie alla topologia.

Quando si verifica una modifica della topologia (ad esempio, uno stato di transizione della porta), lo switch invia un BPDU TCN al bridge radice. Il bridge radice propaga quindi i BPDU TCN a tutti gli switch, chiedendo loro di ridurre il tempo di aging dell'indirizzo MAC dal valore predefinito (300 secondi) al valore di ritardo successivo (generalmente 15 secondi). Questo causa lo svuotamento delle voci inattive di recente, con conseguenti unicast sconosciuti e un aumento delle inondazioni in tutta la rete.

<#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
```

Flapping MAC/loop di livello 2

Lo sfarfallio degli indirizzi MAC e i loop di layer 2 causano la latenza di rete e la perdita di pacchetti aggiornando continuamente la tabella degli indirizzi MAC con lo stesso MAC di origine su porte diverse. Questo cambiamento costante interrompe l'inoltro del traffico, provocando interruzioni e perdita di pacchetti. I loop di layer 2 peggiorano il problema causando la circolazione continua dei pacchetti broadcast, aumentando il flapping degli MAC e riducendo ulteriormente le prestazioni della rete. L'implementazione di protocolli di prevenzione del loop come STP è essenziale per mantenere un funzionamento stabile della rete ed evitare questi problemi.

Per configurare la notifica di spostamento dell'indirizzo MAC, usare il comando mac address-table notification mac-move in modalità di configurazione 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
```

Controllo flusso

Quando il controllo del flusso è abilitato e un buffer di ricezione di una porta dello switch si avvicina alla capacità, lo switch invia dei frame di pausa per interrompere temporaneamente il traffico in entrata. Questo processo può aumentare la latenza in quanto la trasmissione dei dati viene sospesa in modo intermittente. Al contrario, se il controllo del flusso non è abilitato o i dispositivi upstream non supportano i frame di pausa, il traffico in arrivo può superare la capacità del buffer, causando sovraccarichi del buffer e perdite di pacchetti.

Il controllo del flusso deve essere configurato attentamente, considerando le funzionalità di tutti i dispositivi nel percorso del traffico. Un utilizzo non corretto o una configurazione errata possono causare un aumento della latenza e la perdita di pacchetti, con un impatto negativo sulle prestazioni delle applicazioni.

<#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

Utilizzo CPU

Un utilizzo elevato della CPU può comportare un aumento della latenza di rete e la perdita di pacchetti. Quando la CPU è sovraccarica, lo switch non è in grado di elaborare il traffico del piano di controllo, gli aggiornamenti del routing o le funzioni di gestione in modo efficiente. Ciò può ritardare l'inoltro dei pacchetti, causare timeout per protocolli come ARP o Spanning Tree e causare la perdita di pacchetti, in particolare per il traffico che richiede l'intervento della CPU.

<#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
```

Utilizzo della memoria

Un utilizzo elevato della memoria può causare latenza e perdite di pacchetti sovraccaricando i processi della CPU e del control plane. Questo sovraccarico ritarda la gestione degli aggiornamenti di routing, dei criteri QoS e della gestione dei buffer, causando una congestione nella pipeline di elaborazione dei pacchetti. Di conseguenza, i pacchetti possono essere scartati o ritardati. Di conseguenza, un utilizzo elevato della memoria influisce sulle prestazioni di rete riducendo l'efficienza dello switch nella gestione del traffico.

<#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
```

Reindirizzamenti ICMP e messaggi non raggiungibili

Quando un pacchetto arriva su un'interfaccia di layer 3 e viene indirizzato fuori dalla stessa interfaccia, lo switch genera un messaggio di reindirizzamento ICMP per informare l'origine di un hop successivo più efficiente sulla stessa subnet. In questo modo, il pacchetto originale attraversa la vLAN due volte, aumentando l'utilizzo della larghezza di banda. Inoltre, il pacchetto di reindirizzamento ICMP stesso consuma larghezza di banda e richiede l'elaborazione della CPU, che può causare interrupt della CPU e una maggiore latenza. Se si verificano molti reindirizzamenti di questo tipo, in particolare durante un traffico elevato, il carico della CPU può aumentare in modo significativo, causando potenzialmente la perdita di pacchetti.

La generazione e l'elaborazione frequente di messaggi ICMP "destinazione irraggiungibile" possono inoltre aumentare l'utilizzo della CPU, influendo sulle prestazioni della rete. Volumi elevati di traffico ICMP non raggiungibile utilizzano le risorse della CPU, il che può causare latenza e perdita di pacchetti.

Per mitigare questi effetti, Cisco consiglia di disabilitare i messaggi ICMP "destinazione irraggiungibile" e i reindirizzamenti ICMP sulle interfacce virtuali di switch (SVI) e sulle interfacce di layer 3 usando i comandi no ip unreachables e no ip redirects. Questa procedura ottimale riduce il carico della CPU e migliora la stabilità della rete.

<#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


...
```

Tempeste di traffico

Una tempesta di traffico si verifica quando un numero eccessivo di pacchetti broadcast, multicast o unicast invade una LAN, sovraccaricando le risorse dello switch e riducendo le prestazioni della rete.

Il controllo della temporizzazione sugli switch monitora il traffico broadcast, multicast e unicast su interfacce fisiche e lo confronta con le soglie configurate. Quando il traffico supera questi limiti, lo switch blocca temporaneamente il traffico in eccesso per evitare il degrado della rete. Ciò protegge le risorse dello switch e mantiene la stabilità e le prestazioni complessive della rete.

<#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
```

Tempo di aging CAM e ARP

Anche il tempo di aging CAM (MAC Address Table) rispetto al tempo di aging ARP (Address Resolution Protocol) può causare la latenza della rete e la perdita di pacchetti. Questo accade perché la tabella CAM, che memorizza le mappature tra indirizzo MAC e porta, in genere distribuisce le voci più velocemente (per impostazione predefinita, circa cinque minuti) rispetto alla tabella ARP, che memorizza le mappature tra indirizzo IP e MAC (per impostazione predefinita, circa quattro ore). Quando un indirizzo MAC non è più valido nella tabella CAM, ma esiste ancora nella tabella ARP, lo switch non conosce più la porta specifica per inoltrare il traffico unicast per l'indirizzo MAC. Di conseguenza, lo switch scarica il traffico unicast su tutte le porte della VLAN, causando la congestione della rete e la potenziale perdita di pacchetti.

Latenza e perdita di pacchetti causate dal tempo di aging CAM/ARP

- Quando la voce della tabella CAM scade prima della voce ARP, lo switch invia i pacchetti unicast perché non dispone della mappatura da MAC a porta.
- Questo effetto aumenta il carico della CPU e consuma inutilmente la larghezza di banda, con conseguenti perdite di pacchetti e latenza della rete.
- La mancata corrispondenza può inoltre causare un inoltro inefficiente e un aumento dell'elaborazione del control plane.

<#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
```

Sessione di monitoraggio

Quando le sessioni di monitoraggio attivo (SPAN) sono configurate su uno switch con più porte di

origine e di destinazione, possono contribuire alla latenza della rete e alle perdite di pacchetti.

<#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)
```

Funzionamento di SPAN

SPAN (Switched Port Analyzer) è una funzione assistita da hardware che esegue il mirroring del traffico dalle porte di origine alle porte di destinazione senza coinvolgere le ricerche della CPU. L'ASIC di replica sul modulo supervisor gestisce il mirroring dei pacchetti, mentre il motore di inoltro reindirizza i pacchetti con mirroring alle porte di destinazione. I pacchetti con mirroring vengono scambiati con lo stesso orario del traffico normale.

Impatto di più porte di origine e di destinazione:

Nell'esempio precedente, lo switch deve replicare il traffico da tutte le interfacce di origine alle interfacce di destinazione. Ad esempio, il traffico dell'interfaccia Po170 viene riflesso e inoltrato due volte a due destinazioni diverse. Questa replica aumenta il carico sul motore di inoltro e può causare congestione nel backplane dello switch.

- Se un canale porta trasporta tre GBPS di traffico, la replica di questo traffico su più destinazioni può generare più di 15 GBPS di traffico con mirroring.
- Il carico sull'ASIC di replica aumenta proporzionalmente alla velocità del traffico sulle interfacce di origine.
- A velocità di traffico inferiori, l'impatto della latenza può essere minimo, ma con l'aumento del traffico, la latenza e la congestione possono diventare significative.

Eccezioni a livello ASIC

Utilizzare questi comandi per verificare i mapping tra l'interfaccia e l'ASIC, che mostrano l'istanza ASIC in cui risiede l'interfaccia.

<#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)
```

Dopo aver identificato l'istanza ASIC, eseguire il comando successivo per visualizzare le eccezioni di eliminazione ASIC di inoltro per tale 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
...
```

Bug del software

A volte i bug del software possono causare, direttamente o indirettamente, comportamenti indesiderati e imprevisti. Questi bug possono causare problemi di latenza di rete, perdita di pacchetti o altre riduzioni delle prestazioni. Per risolvere questi problemi, un primo passo comune è ricaricare lo switch, in modo da eliminare gli errori temporanei e ripristinare il normale funzionamento. Inoltre, è fondamentale mantenere aggiornati i dispositivi applicando regolarmente gli ultimi aggiornamenti firmware e software. Questi aggiornamenti spesso includono correzioni per bug noti e miglioramenti che migliorano la stabilità e le prestazioni dei dispositivi, contribuendo

a prevenire problemi relativi a difetti software.

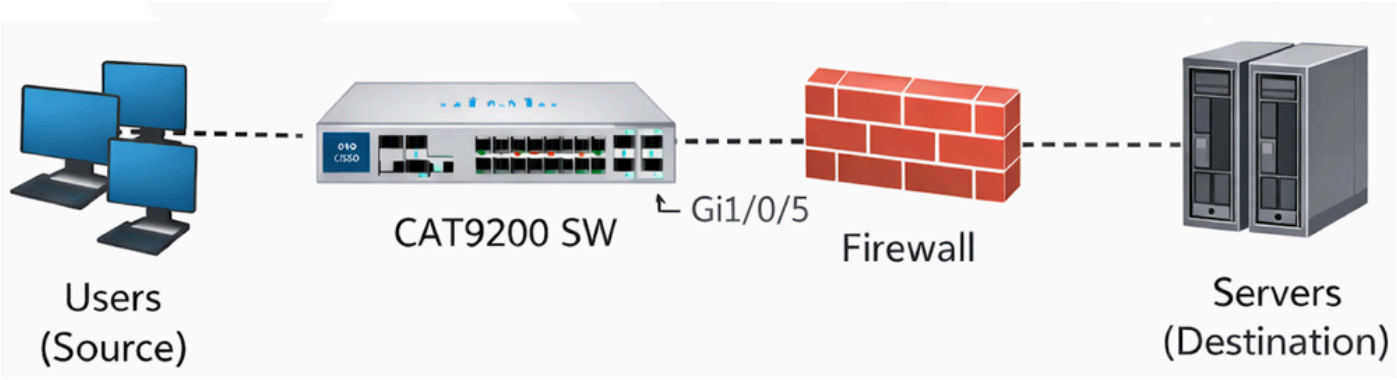
Cisco Bug Search Tool

Case study

Dettagli problema

Gli utenti stanno riscontrando perdite intermittenti della connettività di rete durante i tentativi di trasferimento di grandi volumi di dati attraverso le VLAN, ad esempio durante trasferimenti di file ad alta capacità. Queste interruzioni si manifestano come errori sporadici nella trasmissione dei dati, nonostante vari tentativi riusciti, con un impatto significativo sull'affidabilità della rete e sulle prestazioni delle applicazioni. Per risolvere temporaneamente il problema, ricaricare lo switch.

Topologia



Sintomi osservati

- I trasferimenti di file tra l'origine e la destinazione hanno esito negativo in modo intermittente dopo diversi tentativi riusciti.
- Lo switch perde la connettività al firewall durante i periodi di errore.
- L'autenticazione 802.1X rimane operativa durante tutti gli incidenti.
- Lo switch continua a rispondere tramite la console durante gli incidenti.
- La porta connessa del firewall visualizza solo il traffico di trasmissione durante i periodi di errore.
- I test diagnostici (DiagGoldPktTest) hanno esito negativo sull'interfaccia Gi1/0/5, indicando un problema nel percorso dei dati.

Risoluzione dei problemi

- I contatori di interfaccia e le statistiche dei buffer a livello di piattaforma vengono esaminati.

- L'interfaccia dello switch Gi1/0/5 mostra un volume molto elevato di frame di pausa 802.3x ricevuti dal firewall.
- Le perdite di output e le statistiche del frame di pausa sono strettamente monitorate.
- Le statistiche della coda del motore di inoltro del software della piattaforma vengono esaminate per identificare il comportamento del buffer.
- Le impostazioni di controllo del flusso sull'interfaccia dello switch sono controllate.

Statistiche interfaccia interessata

<#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.

<===== DiagGoldPktTest Failed For Port 5

Port 25 26 27 28□----------□U U U U

Switch#show flowcontrol interface GigabitEthernet 1/0/

Port	Send FlowControl admin	oper	Receive FlowControl admin	Oper	RxPause	TxPause
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
```

Identificazione della root cause

La causa principale è stata identificata come blocco del buffer a causa di un numero eccessivo di frame di pausa 802.3x inviati dal firewall all'interfaccia dello switch. I frame di pausa Ethernet indicano allo switch di interrompere la trasmissione per consentire al dispositivo ricevente di ripristinare la normale operatività dopo la congestione. Tuttavia, quando i frame di pausa vengono inviati ripetutamente o per durate estese:

- La coda di output del buffer dello switch per l'interfaccia diventa completamente satura.
- Lo switch continua ad accettare i pacchetti in arrivo destinati all'interfaccia in pausa, che vengono accumulati nella coda di output.
- La saturazione della coda causa perdite di output e blocchi del traffico.
- In questo caso, i buffer sono stati bloccati e l'inoltro non è stato ripreso anche dopo la riduzione della frequenza dei frame di pausa.
- È stato necessario ricaricare lo switch per cancellare lo stato del buffer bloccato.

Questo comportamento è documentato nel bug Cisco CSCwm14612 in cui viene descritto come la presenza di frame di pausa eccessivi causi un errore nell'interfaccia durante la memorizzazione dei buffer, con conseguenti perdite di output.

Risoluzione

Il controllo del flusso di input è stato disabilitato sull'interfaccia dello switch interessata tramite il comando:

<#root>

```
Switch#configure terminal
```

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

flowcontrol receive off
```

Conclusioni

Gli errori intermittenti di connettività di rete e le perdite di pacchetti tra lo switch Cisco C9200L e il firewall sono stati causati da un blocco della coda software attivato da un volume eccessivo di frame di pausa 802.3x. La disattivazione del controllo del flusso di input sull'interfaccia dello switch ha risolto il problema impedendo che la coda diventi satura e bloccata.

Informazioni correlate

- Risoluzione dei problemi relativi ai pacchetti eliminati nella coda di output sui dispositivi Catalyst 9000 Switch
- Risoluzione dei problemi STP sugli switch Catalyst
- Risoluzione dei problemi di loop/flap MAC sugli switch Cisco Catalyst
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).