

Catalyst 9000交換器上的網路延遲和封包捨棄疑難排解

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[瞭解網路延遲和資料包丟棄](#)

[網路延遲](#)

[封包捨棄](#)

[預期延遲基準](#)

[測量網路延遲](#)

[Ping](#)

[Traceroute](#)

[延遲和丟包的常見原因](#)

[第1層（物理層）問題](#)

[輸出丟棄](#)

[STP穩定性](#)

[MAC擺動/第2層環路](#)

[流量控制](#)

[CPU利用率](#)

[記憶體利用率](#)

[ICMP重定向和無法到達消息](#)

[交通風暴](#)

[CAM與ARP老化時間](#)

[CAM與ARP老化時間如何導致延遲和丟包](#)

[監控作業階段](#)

[SPAN的運作方式](#)

[ASIC級異常](#)

[軟體錯誤](#)

[案例研究](#)

[問題詳細資訊](#)

[拓撲](#)

[觀察到的症狀](#)

[已執行故障排除](#)

[相關介面統計資訊](#)

[確定的根本原因](#)

[解析](#)

簡介

本檔案介紹疑難排解Cisco Catalyst 9000系列交換器上的網路延遲和封包遺失問題的詳細方法。

必要條件

需求

思科建議您深入瞭解網路概念，包括TCP/IP、VLAN和跨距樹狀目錄通訊協定(STP)。必須瞭解Cisco Catalyst 9000系列交換機和Cisco IOS® XE CLI。還需要熟悉網路監控工具以及配置和診斷的訪問許可權。

採用元件

本檔案中的資訊是根據所有版本的Cisco Catalyst 9000交換器。本檔案所述內容不限於任何特定軟體或硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔專為網路管理員和工程師而設計，旨在指導他們如何在企業網路環境中有效地識別、隔離和解決這些問題。網路延遲和丟包會對企業環境的效能和可靠性產生負面影響。這些問題通常由網路擁塞、配置錯誤或環境因素導致。Cisco Catalyst 9000系列交換機經過精心設計，可提供高效能和可復原性。本文提供有針對性的故障排除步驟，幫助網路專業人員識別並解決使用這些交換機的延遲和丟包問題。

瞭解網路延遲和資料包丟棄

網路延遲

網路延遲是指資料從源到目的地穿越網路時所經歷的延遲的度量。最常見的是，延遲表示為來回時間(RTT) — 資料包從源傳輸到目的地並返回所需的時間。

延遲通常以毫秒(ms)來衡量。

影響:高延遲會降低應用效能，尤其是對於依賴及時確認來高效傳送資料的TCP等協定。

封包捨棄

網路裝置無法將資料包轉發到其預定目標時，通常由於擁塞、緩衝區溢位、配置錯誤或硬體故障，就會發生資料包丟棄。丟包率通常以特定時間間隔內丟失資料包的百分比來衡量。

影響：丟包會降低吞吐量，導致重新傳輸，並可能中斷應用程式的可靠性。

預期延遲基準

網路型別	典型RTT
相同VLAN (接入層)	< 1毫秒
園區核心遍歷	1 - 5毫秒
城域WAN	5 - 30毫秒
網際網路/廣域網	30 - 150毫秒



附註：網路躍點之間的地理距離會增加RTT並導致更高的延遲。

測量網路延遲

首先全面瞭解您的網路及其拓撲。如果您的網路設計具有確定變數和最小的不可預測性，則識別和解決延遲和丟包問題的過程變得更加簡單。

測量網路延遲通常使用兩種主要工具。

Ping

它返回輸出形式為目標是否可以訪問，並返回有關資料包丟失和RTT的統計資訊。一旦識別出有問題的躍點，您可以嘗試在這些躍點之間直接ping並簽入裝置以找出問題。

```
<#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/
```

/22 ms

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

Traceroute

Traceroute顯示從來源到目的地的路由路徑中的所有躍點，以及每個躍點的RTT結果。例如，traceroute可以顯示延遲在網路中的什麼位置（路由路徑中的哪個躍點）存在或開始。下一個traceroute輸出中顯示了此類示例。

<#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.

此輸出表示第3跳可能有延遲，證據是第2跳和第3跳之間的RTT顯著增加。第3跳和第4跳之間的相對較小的時間差表明，此問題已侷限於20.20.20.20和30.30.30之間的網段。

延遲和丟包的常見原因

第1層（物理層）問題

第1層問題是網路延遲和丟包的常見來源。在物理層驗證這些方面非常重要：

- 檢驗是否在所有介面上正確配置了雙工和速度設定。
- 檢查介面的CRC和輸入錯誤，這些錯誤可能指示物理層問題。
- 網路纜線、光纖連線、SFP模組或交換器連線埠發生故障也可能會導致封包延遲和捨棄。

<#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 runs, 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
...						

輸出丟棄

當交換器介面的傳輸佇列已滿且無法轉送其他封包時，就會發生輸出捨棄。當資料包在佇列中等待時，這會導致延遲增加；如果佇列溢位，則還會導致丟包，從而影響應用程式效能和網路可靠性。

```
<#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
...
```

Total output drops計數器顯示大量丟棄的資料包，指示此介面上出現擁塞或隊列溢位。這可能導致延遲和資料包丟失增加，從而影響網路和應用效能。

STP穩定性

STP不穩定性可顯著導致網路延遲和資料包丟棄。在穩定的網路中，拓撲變化必須最小。頻繁的拓撲更改可能表示根本問題，並可能中斷正常的轉發操作。

最大程度減少與STP相關的延遲的關鍵注意事項：

拓撲更改(TCN):過多的STP拓撲更改可能導致頻繁刷新交換機(CAM)表的MAC地址，導致廣播流量增加和延遲增加，因為交換機會在重新填充表之前泛洪未知的單點傳播資料包。

邊緣埠配置：確保所有邊緣埠都配置了PortFast。啟用PortFast可防止在客戶端或伺服器連線或斷開連線時生成STP拓撲更改通知(TCN)，從而減少不必要的CAM表老化並提高穩定性。

根網橋規劃：手動規劃和分配STP根網橋和優先順序，以維護可預知的網路拓撲並最大程度地減少不必要的拓撲更改。

發生拓撲更改（例如埠轉換狀態）時，交換機向根網橋傳送TCN BPDU。然後，根網橋會將TCN BPDU傳播到所有交換機，提示它們將其MAC地址老化時間從預設值（300秒）縮短到「轉發延遲」值（通常為15秒）。這會導致刷新最近空閒的條目，從而導致更多的未知單播和增加整個網路的泛洪。

<#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擺動/第2層環路

MAC擺動/第2層環路通過在不同的埠上使用相同的源MAC持續更新MAC地址表，導致網路延遲和資料包丟棄。這種持續的變化中斷流量轉發，導致中斷和資料包丟失。第2層循環使問題惡化，因為它導致廣播資料包無休止地循環，從而觸發更多的MAC抖動，並進一步降低網路效能。實施STP等環路預防協定對於保持網路穩定運行和避免這些問題至關重要。

要配置MAC移動通知，請在全域性配置模式下使用命令 `mac address-table notification mac-move`。

```
<#root>
```

```
Mac Flapping logs:
```

```
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po1
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po1
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po1 and port Po2
%MAC_MOVE-SW1-4-NOTIF: Host b0f1.ec27.69ea in vlan 154 is flapping between port Po9 and port Po10
```

流量控制

當流量控制啟用且交換器連線埠的接收緩衝區接近容量時，交換器會傳送暫停訊框，以暫時停止傳入流量。由於資料傳輸間歇性暫停，此過程可能會增加延遲。反之，如果沒有啟用流量控制或上游裝置不支援暫停幀，則傳入流量可能會超過緩衝區容量，從而導致緩衝區溢位和資料包丟棄。

必須仔細配置流量控制，要考慮流量路徑中所有裝置的功能。不正確使用或配置錯誤會導致延遲和丟包增加，從而對應用程式效能造成負面影響。

```
<#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利用率

CPU使用率高會導致網路延遲和丟包增加。當CPU負載較重時，交換機無法有效處理控制平面流量、路由更新或管理功能。這可能會延遲封包轉送，造成ARP或跨距樹狀目錄等通訊協定逾時，並導致封包捨棄，尤其是對於需要CPU介入的流量。

```
<#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

記憶體利用率

高記憶體使用率會使CPU和控制平面進程過載，從而導致延遲和資料包丟棄。這種過載會延遲路由更新、QoS策略和緩衝區管理的處理，導致資料包處理管道擁塞。因此，資料包可能會被丟棄或延遲。因此，高記憶體利用率會降低交換機管理流量的效率，從而影響網路效能。

<#root>

```
Switch#show platform resources
```

Resource	Usage	Max	Warning	Critical
Control Processor DRAM	25.00%	100%	90%	95%
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重定向和無法到達消息

當封包到達第3層介面並從同一介面路由出去時，交換器會產生ICMP重新導向訊息，告知來源在同一子網中更有效率的下一個躍點。這會導致原始資料包在vLAN中經過兩次，從而增加頻寬使用量。此外，ICMP重定向資料包本身會消耗頻寬，並需要CPU處理，這可能導致出現CPU中斷和延遲增加。如果發生許多此類重定向（尤其是在流量繁重時），CPU負載可能會顯著增加，從而可能導致資料包丟棄。

頻繁生成並處理ICMP不可達消息也會增加CPU利用率，從而影響網路效能。大量ICMP不可達流量會消耗CPU資源，這可能導致延遲和資料包丟棄。

為了緩解這些影響，Cisco建議在交換器虛擬介面(SVI)和第3層介面上使用no ip unreachable和no ip redirects 指令停用ICMP無法到達訊息和ICMP重新導向。此最佳實踐可減少CPU負載並增強網路穩定性。

<#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

```
=====
```

QId	PlcIdx	Queue Name	Enabled	(default) Rate	(set) Rate	Queue Drop(Bytes)	Queue 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

```
-----
```

...

交通風暴

當過多的廣播、多點傳送或單播資料包泛洪LAN，使交換機資源無法承受並且降低了網路效能時，就會發生流量風暴。

交換機上的風暴控制監控物理介面上的廣播、組播和單播流量，並將其與配置的閾值進行比較。當流量超過這些限制時，交換器會暫時封鎖多餘的流量，以避免網路退化。這樣可以保護交換機資源並維護整個網路的穩定性和效能。

<#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

QId	PlcIdx	Queue Name	Enabled	(default) Rate	(set) Rate	Queue Drop(Bytes)	Queue 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與ARP老化時間

CAM (MAC地址表) 老化時間與地址解析協定(ARP)老化時間之間也可能造成網路延遲和資料包丟棄。發生這種情況的原因是，儲存MAC地址到埠對映的CAM表通常會比ARP表 (儲存IP到MAC地址對映，預設值為4小時) 更快地過期條目 (預設值為5分鐘)。當MAC地址在CAM表中過期但仍存在於ARP表中時，交換機不再知道要轉發該MAC地址的單點傳播流量的特定埠。因此，交換機將單播流量泛洪到VLAN中的所有埠，導致網路擁塞和潛在的資料包丟失。

CAM與ARP老化時間如何導致延遲和丟包

- 當CAM表條目在ARP條目之前過期時，交換機將泛洪單播資料包，因為它缺少MAC到埠的對映。
- 這種泛洪會增加CPU負載和不必要地消耗頻寬，導致網路延遲和資料包丟棄。
- 這種不匹配還可能導致低效的轉發以及控制平面處理量的增加。

```
<#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
```

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
```

監控作業階段

在具有多個來源和目的地連線埠的交換器上設定作用中監控器(SPAN)作業階段時，可能會導致網路延遲和封包捨棄。

```
<#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)
```

SPAN的運作方式

SPAN (交換連線埠分析器) 是一種硬體輔助功能，可將來自來源連線埠的流量映象到目的地連線埠，不會涉及CPU查詢。Supervisor模組上的複製ASIC處理資料包映象，而轉發引擎將映象資料包重定向到目標埠。映象資料包的交換時間與常規流量相同。

多個來源和目的地連線埠的影響：

在先前的範例中，交換器必須將流量從所有來源介面複製到目的地介面。例如，介面Po170的流量被映象並轉發到兩個不同的目的地。此複製會增加轉發引擎的負載，並可能導致交換機背板擁塞。

- 如果埠通道傳輸了3 GBPS的流量，則將此流量複製到多個目標會導致超過15 GBPS的映象流量。
- 複製ASIC上的負載會隨著源介面上的流量速率成比例增加。
- 在較低的流量速率下，延遲影響可以降至最低，但隨著流量的增加，延遲和擁塞可能會變得顯著。

ASIC級異常

使用這些命令檢查介面到ASIC的對映，其中顯示了介面所在的ASIC例項。

```
<#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)
```

識別ASIC例項後，運行下一個命令以檢視該ASIC的轉發ASIC丟棄異常。

<#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

```
.....
```

軟體錯誤

軟體錯誤有時可能直接或間接造成意外及意外行為。這些錯誤可能會導致網路延遲、封包捨棄或其他效能下降等問題。為了解決這些問題，常見的第一步是重新載入交換機，這樣可以清除瞬態故障並恢復正常操作。此外，定期應用最新的韌體和軟體更新，使您的裝置保持最新狀態也至關重要。這些更新通常包括對已知錯誤的修復以及增強裝置穩定性和效能的改進，有助於防止與軟體缺陷相關的問題。

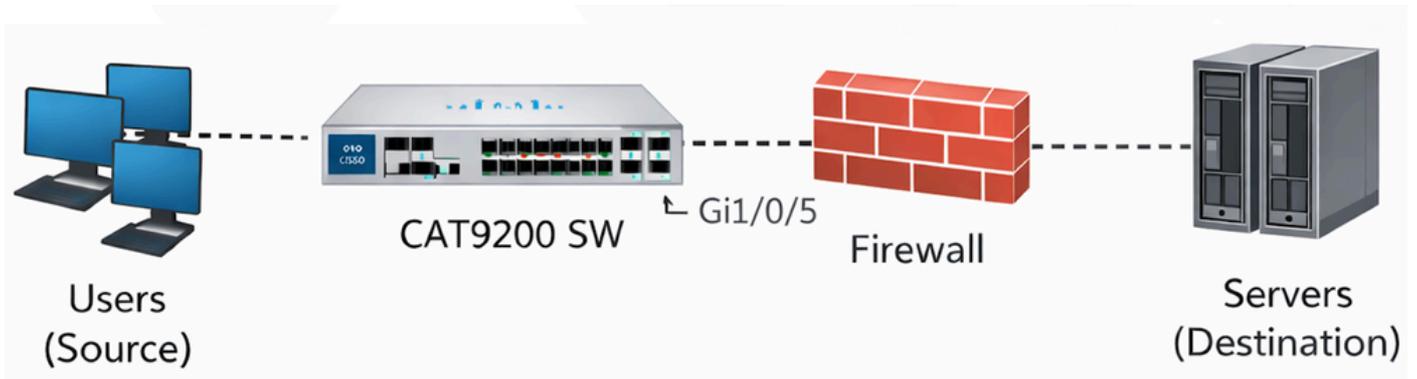
[思科錯誤搜尋工具](#)

案例研究

問題詳細資訊

使用者在嘗試通過vLAN傳輸大量資料時（例如高容量檔案傳輸時），會間歇性丟失網路連線。儘管多次嘗試成功，這些中斷仍表現為資料傳輸中的零星故障，嚴重影響網路可靠性和應用效能。通過重新載入交換機可暫時解決此問題。

拓撲



觀察到的症狀

- 在多次成功嘗試後，源與目標之間的檔案傳輸間歇性失敗。
- 發生故障時，交換機將失去與防火牆的連線。
- 802.1X身份驗證在整個事件中保持可操作性。
- 發生事件時，交換機通過控制檯保持響應。
- 防火牆的已連線埠僅在故障期間顯示廣播流量。
- 介面Gi1/0/5上的診斷測試(DiagGoldPktTest)始終失敗，表明存在資料路徑問題。

已執行故障排除

- 將檢查介面計數器和平台級緩衝區統計資訊。
- 交換器介面Gi1/0/5顯示從防火牆接收的802.3x暫停訊框數量非常大。
- 輸出丟棄和暫停幀統計資訊會受到嚴密監控。
- 檢查平台軟體轉發引擎隊列統計資訊以識別緩衝區行為。
- 已檢查交換機介面上的流量控制設定。

相關介面統計資訊

<#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.
```

<===== 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
```

確定的根本原因

根本原因確定為由於防火牆向交換機介面傳送了過多的802.3x暫停幀而導致緩衝區鎖定。乙太網暫停幀指示交換機停止傳送，以允許接收裝置從擁塞中恢復。但是，當重複傳送暫停訊框或為了延長持續時間時：

- 介面的交換機緩衝區的輸出隊列變為完全飽和。
- 交換器繼續接受目的地為暫停介面的傳入封包，這些封包會在輸出佇列中累積。
- 隊列飽和會導致輸出丟棄和流量黑洞。
- 在這種情況下，緩衝區被鎖定，即使暫停幀速率降低，轉發也不會恢復。
- 需要重新載入交換機才能清除鎖定的緩衝區狀態。

此行為記錄在Cisco錯誤[CSCwm14612](#)中，該錯誤描述過多的暫停訊框如何導致介面錯誤地保留緩衝區，進而導致輸出捨棄。

解析

已使用以下命令在受影響的交換機介面上禁用輸入流控制：

```
<#root>
```

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

結論

思科C9200L交換機和防火牆之間間歇性網路連線故障和資料包丟棄是由過量802.3x暫停幀觸發軟體隊列鎖定引起的。禁用交換機介面上的輸入流控制可防止隊列變得飽和並鎖定，從而解決了此問題。

相關資訊

- [Catalyst 9000交換器上的輸出捨棄疑難排解](#)
- [疑難排解 Catalyst 交換器上的 STP 問題](#)
- [疑難排解Cisco Catalyst交換器上的MAC擺動/回圈](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。