由於NAT網守預設配置，對高QFP利用率進行故障排除

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[背景資訊](#)

[症狀](#)

[封包追蹤功能](#)

- [基本資料包跟蹤配置](#)

[什麼是NAT網守](#)

[檢查NAT網守](#)

[解決方法/修復](#)

- [情境 1](#)
- [情境 2](#)

[摘要](#)

[相關資訊](#)

簡介

本文描述如何識別和解決路由平台上由於NATed和非NATed流量混合而引起的高量子流處理器(QFP)使用率。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS® XE資料包轉發架構的基本知識
- 使用資料包跟蹤功能的基本體驗

採用元件

本文件所述內容不限於特定軟體和硬體版本。它適用於具有物理/虛擬化QFP的任何路由Cisco IOS XE平台，如ASR1000、ISR4000、ISR1000、Cat8000或Cat8000v。

本文檔基於處於自主模式的Cisco IOS XE裝置，SDWAN（控制器）或SD路由可以遵循類似的邏輯，但具體內容可能不同。

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

當同一介面上同時存在NATed和非NAT流量時，在Cisco路由器上可以發現Cisco Quantum Flow Processor(QFP)存在高利用率和效能問題。這也會導致其他效能問題，例如介面錯誤或速度緩慢。

附註：QFP位於嵌入式服務處理器(ESP)上，負責所有入站和出站流量資料平面和資料包處理，根據平台的不同，這可以是物理的，也可以是虛擬化的。

症狀

從路由器驗證和確認這些症狀對於識別此行為非常重要：

1. HIgh QFP載入警報。當負載超過80%的閾值時，會出現這些警報。

```
Feb 8 08:02:25.147 mst: %IOSXE_QFP-2-LOAD_EXCEED: Slot: 0, QFP:0, Load 81% exceeds the setting thresho
Feb 8 08:04:15.149 mst: %IOSXE_QFP-2-LOAD_RECOVER: Slot: 0, QFP:0, Load 59% recovered.
```

附註：您還可以運行show platform hardware qfp active datapath utilization summary命令，以顯示QFP上的負載和通訊速率。

```
Router# show platform hardware qfp active datapath utilization summary
  CPP 0: Subdev 0            5 secs        1 min        5 min       60 min
Input:  Priority (pps)            0            0            0            0
                 (bps)           96           32           32           32
    Non-Priority (pps)       327503       526605       552898       594269
                 (bps)   1225600520   2664222472   2867573720   2960588728
           Total (pps)       327503       526605       552898       594269
                 (bps)   1225600616   2664222504   2867573752   2960588760
Output: Priority (pps)            6            7            7            7
                 (bps)         8576         9992         9320         9344
    Non-Priority (pps)       327715       526839       553128       594506
                 (bps)   1257522072   2714335584   2920005904   3016943800
           Total (pps)       327721       526846       553135       594513
                 (bps)   1257530648   2714345576   2920015224   3016953144
Processing: Load (pct)           99           72           34           19
```

2.介面錯誤。如果QFP使用率高，則由於存在背壓，資料包可能會被丟棄。在這種情況下，介面上通常會觀察到超支和輸入丟棄。要顯示此資訊，可以運行show interfaces命令。

```
Router# show interface gigabitEthernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4351-3x1GE, address is e41f.7b59.cba1 (bia e41f.7b59.cba1)
  Description: ### LAN Interface ###
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 2/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is force-up, media type is LX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:06:47, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 9390000 bits/sec, 2551 packets/sec
  30 second output rate 1402000 bits/sec, 1323 packets/sec
     368345166434 packets input, 199203081647360 bytes, 0 no buffer
     Received 159964 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     2884115457 input errors, 0 CRC, 0 frame, 2884115457 overrun, 0 ignored
     0 watchdog, 3691484 multicast, 0 pause input
     220286824008 packets output, 32398293188401 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     3682606 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     21 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

3.在某些情況下，使用者可能會抱怨網路速度緩慢。

封包追蹤功能

- 封包追蹤工具可提供有關Cisco IOS XE平台如何處理資料封包的詳細資訊。
- 它有3個檢查級別，分別是記帳、彙總和資料路徑。
- 您可以獲取以下資訊：
    - 輸入和輸出介面
    - 資料包狀態
    - 時間戳
    - 封包追蹤軌跡

附註：設定資料路徑會消耗更多封包處理資源，這只會反映在符合篩選條件的資料包上。

使用Cisco IOS XE資料路徑資料包跟蹤功能進行故障排除中有關資料包跟蹤的詳細資訊

基本資料包跟蹤配置

以下是具有資料路徑層級檢查的基本封包追蹤組態範例。它以循環方式收集8192個資料包（覆蓋舊資料包），從第3層建立每個資料包的副本，該副本到達並離開介面GigabitEthernet 0/0/1。

```
Router# debug platform packet-trace packet 8192 circular fia-trace data-size 2048
Router# debug platform packet-trace copy packet both L3 size 64
Router# debug platform condition interface gigabitEthernet 0/0/1 both
Router# debug platform condition start
Router# debug platform condition stop
```

您可以使用這些命令檢查資料包跟蹤的結果。

```
Router# show platform packet-trace summary
Router# show platform packet-trace packet all
```

從資料包跟蹤捕獲中，可以看到NAT功能消耗的資源比預期的多。在下一個示例中，您可以看到IPV4_NAT_INPUT_FIA功能的失效時間明顯大於其他功能的失效時間。此行為通常表示QFP處理此功能需要更多時間，因此QFP中的更多資源用於NAT。

```
Packet: 161         CBUG ID: 161
Summary
  Input     : GigabitEthernet0/0/1
  Output    : GigabitEthernet0/0/2.1730
  State     : FWD
  Timestamp
    Start   : 25136781447706429 ns (02/10/2024 00:25:49.584050 UTC)
    Stop    : 25136781447993237 ns (02/10/2024 00:25:49.584337 UTC)




  Feature: IPV4_NAT_INPUT_FIA   <<<<<<<<<<<<
    Entry       : Input - 0x700162ac
    Input       : GigabitEthernet0/0/1
    Output      :



    Lapsed time : 1873376 ns     <<<<<<<<<<<<



  Feature: IPV4_INPUT_IPOPTIONS_PROCESS
    Entry       : Input - 0x70016344
    Input       : GigabitEthernet0/0/1
    Output      : GigabitEthernet0/0/2.1730
    Lapsed time : 64 ns
```

什麼是NAT網守

在Cisco IOS XE路由平台中，功能網路地址轉換(NAT)網守預設啟用。NAT網守最初是為了防止非NAT流使用過多的處理資源來建立NAT轉換。NAT網守根據源地址為從內到外方向和其他方向建立兩個小快取。每個快取條目都包含一個源地址、一個虛擬路由和轉發(VRF)ID、一個計時器值（用於使該條目失效）和一個幀計數器。

NATed介面上的大量非NATed流量會消耗大量資源，並導致QFP利用率高峰。Cisco建議客戶儘可能不要在同一介面上使用NAT和非NAT流。

檢查NAT網守

可以使用show platform hardware qfp active feature nat datapath { gatein 命令檢查NAT網守統計資訊 | gateout }活動。這顯示快取的大小、命中數、未命中數、已老化、已新增和活動條目在快取中的數量。通常，如果存在大量未命中數，並且此數量在短時間內迅速增加，這表示有大量的非歸屬流沒有新增到快取。此行為會導致這些流在NAT工作流中由QFP處理，並且這會提高QFP的利用率。

```
Router# show platform hardware qfp active feature nat datapath gatein activity
Gatekeeper on
def mode Size 8192, Hits 191540578459, Miss 3196566091, Aged 1365537 Added 9 Active 7

Router# show platform hardware qfp active feature nat datapath gateout activity
Gatekeeper on
def mode Size 8192, Hits 448492109001, Miss 53295038401, Aged 149941327 Added 603614728 Active 1899
```

解決方法/修復

在大多數環境中，NAT網守功能運行正常，不會導致問題。但是，如果確實遇到此問題，則有幾種方法可以解決此問題。

情境 1

對於這些型別的問題，Cisco建議將NATed流量和非NATed流量從同一介面分離。它可以在不同的介面或網路裝置中使用。

情境 2

增加NAT網守功能上的快取大小，以減少網守的未命中次數。

下一個示例顯示如何調整Cisco路由器上的網守。請注意，此值必須以2的冪來表示。否則，該值會自動設定為下一個更小的大小。

```
Router(config)# ip nat service gatekeeper
Router(config)# ip nat settings gatekeeper-size 65536
```

附註：調整快取大小可能會花費QFP中的記憶體，從而最佳化其使用。嘗試逐漸調整此值，並以與預設設定最接近的可能值開始。

執行上述解決方案之一後，建議監控這兩個引數，以確認問題已解決：

1. 驗證QFP利用率是否已降低。
2. 驗證未命中數量是否不會繼續增加。

摘要

當NATed介面上存在非NATed流時，NAT網守功能可以提高路由器的效能。當NAT轉換某些NAT流時，同時非NAT流通過同一介面時，通常會發生這種情況。在大多數環境中，NAT Gatekeeper功能不會對路由器造成任何影響。但是，必要時仔細調整該特性以避免副作用，這一點非常重要。

相關資訊

- ASR1K NAT間歇性無法轉換某些資料包
- 使用Cisco IOS XE資料路徑資料包跟蹤功能進行故障排除
- 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）。