排除企業網路中的路由器問題

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[背景資訊](#)

[延遲定義](#)

[延遲使用情況](#)

[解決延遲問題](#)

[常見原因故障排除](#)

- [平台相關](#)
  - [高CPU](#)
- [流量相關](#)
  - [MTU和分段](#)
- [與設計相關](#)
  - [次優路由](#)
  - [服務品質(QoS)](#)

[其他效能問題](#)

- [Drops](#)
- [TCP重傳](#)
- [超訂用和瓶頸](#)

[相關資訊](#)

簡介

本文說明如何使用Cisco路由器識別、排除和解決企業網路中的延遲問題。

必要條件

需求

本檔案沒有特定先決條件或要求。

採用元件

本文檔不限於特定的軟體版本和硬體型別，但命令適用於Cisco IOS® XE路由器，例如ASR 1000、ISR 4000和Catalyst 8000系列。

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

本文檔介紹了瞭解、隔離和排除一般延遲問題的基本指南，並提供了用於檢測根本原因和最佳實踐的有用命令/調試。切記，不能考慮所有可能的變數和情景，且更深入的分析取決於具體情況。

延遲定義

一般而言，並引述儲存和轉送裝置的嚴格定義（在RFC 1242上），延遲是指從輸入訊框的最後一位到達輸入連線埠時開始並在輸出連線埠上看到輸出訊框的第一位時結束的時間間隔。

網路延遲可能只是指通過網路傳輸資料的延遲。對於實際問題，此定義只是一個起點；您需要定義每個特定案例所討論的延遲問題，雖然看起來顯而易見的是，解決問題所需的第一步，也是真正重要的第一步，是定義問題。

延遲使用情況

許多應用程式要求即時通訊和業務運營的低延遲；隨著每天硬體和軟體改進，更多應用程式可用於任務關鍵型計算、線上會議應用程式、流傳輸等；同樣，網路流量繼續增長，對最佳化網路設計和提高裝置效能的需求也隨之增加。

除了提供更好的使用者體驗和滿足對延遲敏感型應用程式的最低要求外，有效識別並減少網路上的延遲問題可以節省網路中非常寶貴的時間和資源。

解決延遲問題

這類問題的難點在於必須考慮的變數數量以及不能出現單點故障。因此，延遲的定義成為解決延遲問題的重要關鍵，下面是您必須考慮的一些方面才能有一個有用的問題描述。

1.期望和檢測

區分所需延遲、預期或基線工作延遲和當前延遲非常重要。根據網路設計、提供商或裝置，有時無法達到所需的延遲，在正常情況下測量實際延遲是一個很好的過程，但您需要對測量方法保持一致，以避免產生誤導性數字；IP SLA和網路分析工具可在這方面提供幫助。

通過ICMP或ping來確定應用程式甚至IP SLA延遲的最常用和最基本的工具之一：

<#root>

```
Router#
```

ping

```
 198.51.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
```

round-trip min/avg/max

=

2/109/541 ms

除了檢查可達性之外，ping還會顯示從來源到目的地的來回時間(RTT)；最小值(2)、平均值(109)和最大值(541)（毫秒）。這表示路由器收到來自裝置目的地的回覆時，從路由器傳送請求到為止的持續時間。但是，它並不顯示有多少跳數或更深入的資訊，但它是檢測問題的一種簡單快速的方法。

2.隔離

與ping一樣，traceroute也可用作隔離的起始點，它可發現躍點及每躍點的RTT:

<#root>

Router#

traceroute

 198.51.100.1
Type escape sequence to abort.
Tracing the route to 198.51.100.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.3.1 5 msec 6 msec 1 msec
  2 10.0.1.1 1 msec 1 msec 1 msec
  3 10.60.60.1 1 msec 1 msec 1 msec
  4 10.90.0.2

362 msec 362 msec 362 msec

<<<< you can see the RTT of the three probes only on both hops

  5 10.90.1.2

363 msec 363 msec 183 msec

  6 10.90.7.7 3 msec 2 msec 2 msec

Traceroute的運作方式為發出包含存留時間(TTL)為1的封包。第一躍點傳回一則ICMP錯誤訊息，說明封包因為TTL過期且已測量RTT而無法轉送，接著第二封包以TTL 2重新傳送，且第二躍點傳回TTL已過期。此程式會一直持續，直到到達目的地為止。

在此範例中，現在您可以縮小到兩個特定主機，並從那裡開始隔離。

儘管這些命令非常有用，可以輕鬆識別問題，但它們不會考慮其他變數，例如協定、資料包標籤和大小（雖然您可以將其設定為第二步）、不同的IP源、多個因素中的目的地。

說延遲可能是一個非常寬泛的概念，您通常只看到應用程式、瀏覽、呼叫或特定任務上的症狀。首先要限制的事情之一是瞭解影響並更詳細地定義問題，回答接下來的問題和元素可以幫助進行這種劃分：

- 延遲是否只影響特定型別的流量或應用？示例：僅UDP、TCP、ICMP...
- 如果是，此流量是否有唯一識別符號？示例：特定QoS標籤、僅確定的資料包大小、IP選項……
- 有多少使用者或站點受到影響？示例：只有一個特定子網、一個或兩個終端主機、連線到一個或多個裝置的整個站點……
- 是否標識了特定的時間戳？示例：這是否僅在高峰時間、任何時間模式或完全隨機期間發生……
- 設計方面。示例：通過特定裝置的流量，可能是許多裝置，但只連線到一個提供商，流量進行負載均衡，但影響一個路徑……

還有許多其它注意事項，但是如果能跨越不同的答案（甚至可以對其進行回答的測試），則可以有效地隔離並限制故障排除的進行範圍。例如，只有一個應用程式（相同型別的流量）影響所有通過不同提供商的分支機構，這些提供商在高峰時段終止於同一資料中心。在這種情況下，您不會開始檢查所有分支機構中的所有接入交換機，而是會集中精力收集有關資料中心的更多資訊，然後在該側進一步檢查。

在網路上可以使用的監控工具和一些自動化功能也很大程度上依賴於這種隔離，這真的取決於您擁有的資源和獨特的情況。

常見原因故障排除

一旦限制故障排除的範圍，就可以開始檢查特定原因，例如，在提供的traceroute示例中，可以隔離到兩個不同的躍點，然後縮小到可能的原因。

平台相關

高CPU

一個常見的原因可能是裝置的CPU高，導致處理所有資料包時延遲。對於路由器，檢查路由器的最有用和最基本的命令是

路由器的整體效能：

<#root>

Router#

show platform resources

```
**State Acronym: H - Healthy, W - Warning, C - Critical
Resource               Usage                Max            Warning         Critical        State
------------------------------------------------------------------------------------------------
RPO (ok, active)                                                                              H

Control Processor      1.15%                100%           80%             90%             H

DRAM                   3631MB(23%)          15476MB        88%             93%             H
```

```
  bootflash              11729MB(46%)          25237MB          88%              93%              H
  harddisk               1121MB(0%)            225279MB         88%              93%              H
ESP0(ok, active)                                                                                  H
 QFP                                                                                              H
  TCAM                   8cells(0%)            131072cells      65%              85%              H
  DRAM                   359563KB(1%)          2097152OKB       85%              95%              H
  IRAM                   16597KB(12%)          131072KB         85%              95%              H

CPU Utilization        0.00%                 100%             90%              95%              H


Crypto Utilization     0.00%                 100%             90%              95%              H

  Pkt Buf Mem (0)        1152KB(0%)            164864KB         85%              95%              H
  Pkt Buf CBlk (0)       14544KB(1%)           986112KB         85%              95%              H
```

對於同時檢視記憶體和CPU利用率很有用，它在控制平面和資料平面(QFP)上與每個平面的閾值相同。記憶體本身不會產生延遲問題，但是，如果沒有更多用於控制平面的DRAM記憶體，Cisco Express Forwarding(CEF)就會被禁用並導致高CPU使用率（可能導致延遲），這就是保持數字處於正常狀態的重要原因。記憶體故障診斷的基本指南超出範圍，但請參考「相關資訊」部分中的有用連結。

如果檢測到控制處理器、QFP CPU或加密使用率的CPU使用率高，則可以使用以下命令：

對於控制平面：

show process cpu sorted

<#root>

```
Router#
show processes cpu sorted
CPU utilization for five seconds:
99%/0%
; one minute: 13%; five minutes: 3%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  65        1621         638       2540 89.48%  1.82%  0.41%  0 crypto sw pk pro
   9         273          61       4475  1.56%  0.25%  0.05%   0 Check heaps
  51         212          64       3312  0.72%  0.21%  0.05%   0 Exec
 133         128          16       8000  0.60%  0.08%  0.01%   0 DBAL EVENTS
 473          25          12       2083  0.48%  0.04%  0.00%   0 WSMAN Process
  84        1173         353       3322  0.36%  0.07%  0.02%   0 IOSD ipc task
  87          23          12       1916  0.24%  0.02%  0.00%   0 PuntInject Keepa
  78         533         341       1563  0.12%  0.29%  0.07%   0 SAMsgThread
 225          25        1275         19  0.12%  0.00%  0.00%   0 SSS Feature Time
 386           4           4       1000  0.12%  0.00%  0.00%   0 Crypto WUI
 127         204       18810         10  0.12%  0.02%  0.00%   0 L2 LISP Punt Pro
```

如果控制平面CPU過高（由於進程的原因，此示例為99%），則需要隔離進程，並根據該進程繼續隔離（可為我們傳送的資料包，如ARP或控制網路資料包，可以是任何路由協定、組播、NAT、DNS、加密流量或任何服務）。

視您的流量而定，這可能會造成進一步處理的問題，如果流量並非目的地為路由器，您可以專注於資料平面：

對於資料平面：

show platform hardware qfp active datapath utilization [summary]

<#root>

```
Router#
show platform hardware qfp active datapath utilization

  CPP 0: Subdev 0

5 secs

        1 min        5 min       60 min
Input:  Priority (pps)            0            0            0            0
                 (bps)            0            0            0            0
    Non-Priority (pps)          231          192           68            6
                 (bps)       114616        95392        33920         3008
           Total (pps)          231          192           68            6
                 (bps)       114616        95392        33920         3008
Output: Priority (pps)            0            0            0            0
                 (bps)            0            0            0            0
    Non-Priority (pps)            3            2            2            0
                 (bps)        14896         9048         8968         2368


Total (pps)

         3323         2352          892            0


(bps)

        14896         9048         8968         2368

Processing: Load (pct)


3

            3            3            3

Crypto/IO


Crypto: Load (pct)            0

            0            0            0
        RX: Load (pct)            0            0            0            0
        TX: Load (pct)            1            1            0            0
            Idle (pct)           99           99           99           99
```

如果資料平面高（通過處理負載數達到100%來標識），則需要檢視通過路由器的流量大小（每秒資料包總數和每秒位元數）和平台的吞吐量效能（您可以在特定資料表上有個想法）。

若要判斷此流量是否為預期流量，可以使用封包擷取(EPC)或任何監控功能（例如Netflow）進行進一步分析，某些檢查如下：

- 流量是否有效且預期會通過此路由器？
- 識別異常流量或更高的速率。
- 如果每秒資料包數較高，請查詢資料包的大小。判斷這是否預期會看到，或是您是否有分段問題。

如果所有流量都是預期流量，則可能會達到平台限制，然後，通過show running-config（主要是在介面上）查詢作為第二部分在路由器上運行的功能進行分析，找出任何不必要的功能並禁用它們，或者平衡流量以釋放CPU週期。

但是，如果沒有平台限制的指示，另一個用於驗證路由器是否在資料包上增加延遲的有用工具是FIA跟蹤，您可以看到每個資料包的確切處理時間，以及佔用大部分處理的功能。完成高CPU故障排除超出本文檔的範圍，但請參閱相關資訊部分的連結。

流量相關

MTU和分段

最大傳輸單元(MTU)是要傳輸的最大封包長度，這取決於實體連結可以傳輸的八位元數量。當上層通訊協定將資料提交給基礎IP，且產生的IP封包長度大於路徑MTU時，封包會被分割成片段。網路上這種較小的容量會使某些案例的處理更多，處理方式也不盡相同，這就是您必須儘可能避免使用它的原因。

對於某些功能（如NAT或基於區域的防火牆），需要虛擬重組以「擁有整個資料包」、應用所需的內容、轉發其碎片並丟棄已重組的副本。此過程會增加CPU週期，而且容易出錯。

某些應用不依賴分段，檢查MTU的最基本測試之一是包含無分段選項的ping，並且測試不同的封包大小：ping ip-address df-bit size number。 如果ping失敗，請在發生捨棄時透過路徑修正MTU，這會導致其他問題。

在含有分段封包的網路上，諸如原則型路由和等價多重路徑等功能可能會產生延遲問題和更多錯誤（大多是在高資料速率上），從而引發高彙集時間、重複ID和損毀的封包。如果識別到其中某些問題，請儘量解決此分段。用於檢查是否有片段以及任何潛在問題的一個命令是show ip traffic:

<#root>

```
Router#
show ip traffic


IP statistics:
  Rcvd:  9875429 total, 14340254 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
```

```
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other, 0 ignored

Frags:


150 reassembled

, 0

timeouts

,

0 could not reassemble

         0

fragmented

, 600

fragments

, 0

could not fragment

         0 invalid hole
  Bcast: 31173 received, 6 sent
  Mcast: 0 received, 0 sent
  Sent:  15742903 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop, 0 unsupported-addr
         0 options denied, 0 source IP address zero
<output omitted>
```

從以上輸出中，Frags部分上的粗體字請參閱：

- 已重組：已重組的資料包數。
- 逾時：每次封包片段的重組時間到期時。
- 無法重組：無法重組的資料包數。
- 已分段：超過MTU和要分段的主題的資料包數。
- 片段：將封包分段到其中的區塊數。
- 無法分段：超過MTU但無法分段的資料包數。

如果使用分段且超時或無法重組計數器增加，則驗證由平台導致問題的一種方法是通過QFP丟棄，使用後面在丟棄部分介紹的相同命令：show platform hardware qfp active statistics drop。查詢錯誤，例如：TcpBadfrag、IpFragErr、FragTailDrop、ReassDrop、ReassFragTooBig、ReassTooManyFrags、ReassTimeout或相關錯誤。每個案例都有不同的原因，例如沒有獲得所有片段、重複、CPU擁塞等。同樣，用於進一步分析和潛在修復的有用工具可以是FIA跟蹤和配置檢查。

TCP提供最大區段大小(MSS)機制來解決此問題，但如果發現不正確、非MSS交涉或錯誤的路徑

MTU，則可能導致延遲。

由於UDP沒有此分段機制，您可以依靠手動實作PMTD或任何應用層解決方案，因此您可以啟用它們(如果適用)來傳送小於576位元組的封包，這是根據RFC1122傳送編號的較小有效MTU，有助於避免分段。

與設計相關

除了故障排除建議外，本節還簡要介紹兩個可能增加延遲問題的關鍵元件，它們需要進行本文檔範圍之外的廣泛討論和分析。

次優路由

網路中的次優路由是指資料包不會透過網路中最有效或最短的路徑傳輸的情況。相反，這些資料包採用的路由效率較低，可能會導致延遲增加、擁塞或影響網路效能。IGP會始終選擇最佳路徑，這表示成本較低，但並不一定是最便宜的路徑或最低延遲路徑（最佳路徑可以是具有較高頻寬的路徑）。

路由協定問題可能會發生次優路由；配置或任何情況，如競爭條件、動態更改（拓撲更改或鏈路故障）、基於公司策略或成本的預期流量工程、冗餘或故障轉移（在特定條件下轉到備份路徑）等。

諸如traceroute或監控裝置之類的工具可幫助識別特定流的這種情況（如果確實如此），並且取決於許多其他因素、滿足應用程式要求並降低延遲可能要求重新設計路由或流量工程。

服務品質(QoS)

通過配置服務品質(QoS)，您可以為特定型別的流量提供優先處理，而犧牲其他流量型別。如果沒有QoS， 裝置 為每個資料包提供盡力服務，無論資料包的內容或大小如何。其 裝置 傳送資料包，但不保證可靠性、延遲界限或吞吐量。

如果QoS就位，那麼確定路由器是標籤、重新標籤還是僅對資料包分類、檢查配置以及show policy-map [name_of_policy_map就變得非常重要 | 會話 | interface interface_id] 有助於瞭解受高速率、丟包或錯誤分類的資料包影響的類。

實施QoS是一項繁重的工作，需要進行認真分析，並且不屬於本文檔的範圍，但強烈建議考慮此項，以便排定對時間敏感的應用程式的優先順序，並解決或防止許多延遲和應用程式問題。

其他效能問題

其他情況可能增加您需要檢查的慢度、會話重新連線或一般效能不佳，其中有些情況是：

Drops

與裝置處理直接相關的一個問題是丟包，您需要從介面角度檢查輸入和輸出端：

```
Router#sh interfaces GigabitEthernet0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is vNIC, address is 0ce0.995d.0000 (bia 0ce0.995d.0000)
  Internet address is 10.10.1.2/24
  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 set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is Virtual
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:19, output 00:08:33, output hang never
  Last clearing of "show interface" counters never


 Input queue: 0/375/6788/0 (size/max/drops/flushes); Total output drops: 18263

  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 114000 bits/sec, 230 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     193099 packets input, 11978115 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles


1572 input errors

,

12 CRC

, 0 frame,

1560 overrun

, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     142 packets output, 11822 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     23 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

在輸入端，您有：

- 輸入佇列捨棄：每個介面都擁有輸入佇列（這是可修改軟體緩衝區），傳入封包會被放置以等待路由處理器(RP)處理。 如果放置在輸入隊列上的傳入資料包的速率超過RP可以處理丟棄增量資料包的速率。但是，請注意，僅放置控制資料包和「For us」流量，因此，如果在通過流量時看到延遲，即使有零星丟棄，這肯定不是原因。

- 溢位：當接收器硬體由於輸入速率超出接收器處理資料的能力而無法將接收的資料包交給硬體緩衝區時，會發生這種情況。此數字可能表示路由器的速率和效能有問題，只捕獲此介面的流量並查詢流量峰值。常見的解決方法是啟用流量控制，但這可能會增加延遲資料包。這也可能是存在瓶頸和超訂用的證據。

- CRC：由於物理問題而發生，請檢查電纜、埠和SFP是否正確連線以及是否正常工作。

在輸出端，您有：

- 輸出隊列丟棄：每個介面都有一個輸出隊列，在該隊列中放置要在該介面上傳送的傳出資料包。有時RP在輸出隊列中放置的傳出資料包的速率超過了介面可以傳送資料包的速率。如果未設定QoS，則可能導致效能問題和延遲問題；否則，由於應用了某些策略，您可以使此數量增加，並建議檢查或實施QoS配置以保護並確保預期或關鍵流量。

最後，QFP上的丟包與可能導致延遲的高處理直接相關，請通過show platform hardware qfp active statistics drop進行檢查：

<#root>

```
Router#

show platform hardware qfp active statistics drop

Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats                          Packets                 Octets
-------------------------------------------------------------------------
Disabled                                         2                    646
Ipv4NoAdj                                   108171                6706602
Ipv6NoRoute                                     10                    560
```

原因取決於代碼，如果此時丟棄了受延遲影響的流量，則FIA跟蹤可幫助證實或丟棄。

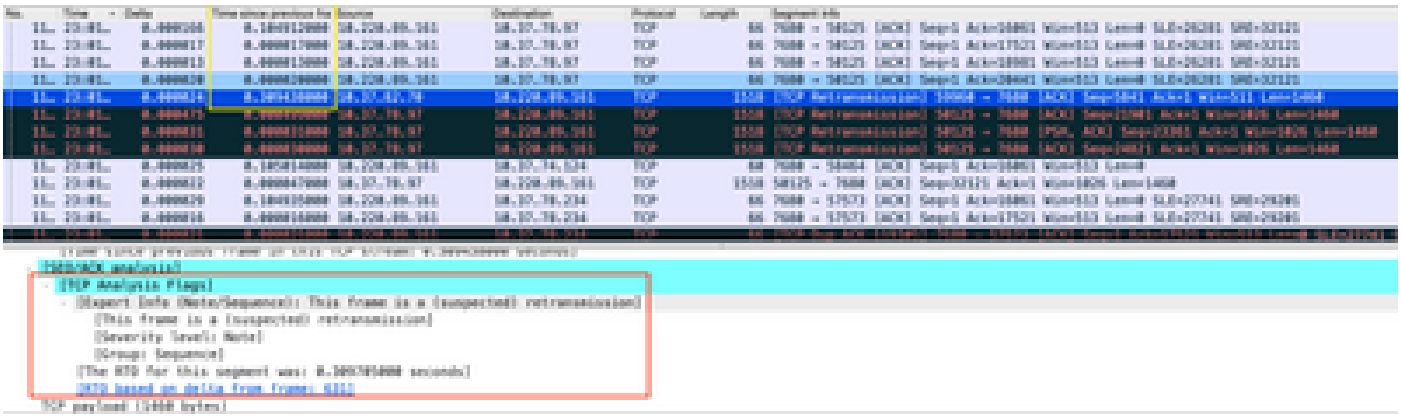
TCP重傳

TCP重新傳輸是症狀，或者可能是由於底層問題（如資料包丟失）所致。這一問題會導致應用速度慢和效能差。

傳輸控制通訊協定(TCP)使用重新傳輸計時器，以確保在遠端資料接收器沒有回饋的情況下進行資料傳輸。此計時器的持續時間稱為RTO（重傳超時）。當重傳計時器到期時，傳送方重新傳輸尚未被TCP接收方確認的最早資料段，並且RTO增加。

有些重傳不能完全消除，如果重傳量很小，則不能反映問題。但是，您可以推斷，看到更多重傳，TCP會話上的延遲更大，需要加以解決。

在Wireshark中分析的資料包捕獲可以作為下一個示例來證實問題：



TCP會話捕獲

如果存在重新傳輸，請在路由器入口和出口方向使用相同的捕獲方法檢查傳送和接收的所有資料包。當然，在每個躍點上執行此操作可能代表巨大的努力，因此TCP需要進行詳細的捕獲分析，檢視TTL 、同一TCP流上之前幀的時間，以瞭解您有此延遲或缺乏響應來指導故障排除。

超訂用和瓶頸

當所需的資源（頻寬）大於實際可用資源時，會發生超訂用。用於識別路由器上是否存在此問題的命令已在上一節中介紹。

因此，當頻寬或硬體容量不足導致流量速度減慢時，可能會出現瓶頸。重要的是要查明這種情況是發生在短期還是長期的情況下才適用解決辦法。

沒有解決此問題的特定建議，但根據當前需求和未來增長分析，有些選項是平衡到不同平台的流量、對網路進行分段或升級到更強大的裝置。

相關資訊

- IP SLA ICMP回應操作
- 記憶體故障排除
- 使用Cisco IOS-XE資料路徑資料包跟蹤功能進行故障排除
- 排除ASR 1000系列服務路由器上的資料包丟棄故障。
- Qos相關資訊
- 路由器上的QoS配置
- 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）。