

# ASR1000通道管制器記錄與監控

## 目錄

[簡介](#)

[每個介面分支管制器](#)

[設定和驗證](#)

[記錄預設Punt-Policer](#)

[結論](#)

## 簡介

本檔案介紹思科聚合服務路由器(ASR)1000和整合服務路由器(ISR)G3裝置的點策略器功能及其中的一些新變化。預設情況下，Punt-policer處於啟用狀態，它管制所有控制平面的流量。如果您想瞭解有關punt-policer和punt相關丟棄的詳細資訊，請參閱[Cisco ASR 1000系列服務路由器上的資料包丟棄](#)。最近，在點策略器日誌記錄和操作方面進行了一些更改，旨在為普通CLI使用者提供一個清晰的日誌記錄機制，以識別裝置上丟包的原因。

## 每個介面分支管制器

這是在Polaris版本16.4中引入的。

這樣，網路管理員可以基於每個介面配置點策略器限制。當您希望確定產生大量突發流量的介面時，它特別有用，因此它減少了故障排除時間並為資料包捕獲提供了替代方案。在此功能之前，如果您需要知道突發流量的源介面，則必須執行消耗大量時間和資源的資料包捕獲。

## 設定和驗證

```
Router(config)#platform punt-intf rate < packet per second>
```

```
Router(config)#interface gigabitEthernet 0/0/0
```

```
Router(config-if)#punt-control enable
```

此配置為每個介面啟用點策略監控。例如，如果在全域性和特定介面上將點壓控制速率配置為1000，裝置將跟蹤此特定介面的點壓丟棄30秒。在30秒的時間間隔之後，路由器會顯示一個這樣的日誌，以提醒管理員發生了點數違規事件。

```
*Jun 21 23:01:01.476: %IOSXE-5-PLATFORM: F1: cpp_cp: QFP:0.1 Thread:076 TS:00000044123616602847  
%PUNT_INJECT-5-DROP_PUNT_INTF: punt interface policer drop packet from GigabitEthernet0/0/0
```

由於30秒是一個較大的時間間隔，因此引入了一個命令，通過該命令可以檢視介面的最新丟棄。

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-intf-drop
```

## latest

Punt Intf Drop Statistics (lastest 1000 dropped packets):

Interface	Packets
GigabitEthernet0/0/0	1000

您可以清除捨棄統計資料以監控即時捨棄情況。

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-intf-drop latest clear
```

Punt Intf Drop Statistics (lastest 1000 dropped packets):

Interface	Packets
-----------	---------

Router#

## 記錄預設Punt-Policer

對於每個介面，需要顯式配置punt-policer。但是，在全域性的ASR裝置上，按原因的點策略器始終處於活動狀態。最近，在16.6.1版映像中，針對每個原因的點監察器實施了日誌記錄。從現在開始，每當發生按原因的點數違規時，都會生成日誌。

從第一個日誌的時間開始，路由器將監控punt原因30秒。如果30秒後有另一個丟棄活動，則會生成另一個日誌。

日誌消息將如下所示，因此您會看到punt cause 60。

```
F1: cpp_cp: QFP:0.1 Thread:035 TS:00000000089593031387 %PUNT_INJECT-5-DROP_PUNT_CAUSE: punt cause policer drop packet cause 60
```

您可以使用此命令檢查點原因相關詳細資訊。

```
BGL14.Q.20-ASR1006-1#show platform hardware qfp active infrastructure punt config cause 60  
QFP Punt Table Configuration
```

```
Punt table base addr : 0x48F46010  
punt cause index      60  
punt cause name       IP subnet or broadcast packet  
maximum instances    1  
punt table address    : 0x48F46100  
instance[0] ptr       : 0x48F46910  
  QFP interface handle : 3  
  Interface name       : internal1/0/rp:1  
  instance address     : 0x48F46910  
  fast failover address : 0x48F2B884  
  Low priority policer : 70  
  High priority policer : 71
```

除了此日誌之外，您還可以始終使用舊命令來監控點滴操作。

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-drop  
Router#show platform hardware qfp active infrastructure punt statistics type per-cause  
Router#show platform hardware qfp active infrastructure punt statistics type global-drop
```

## 結論

隨著逐點原因日誌記錄和逐介面點監控的引入，有更好的工具可以隔離點相關問題。當您看到QFP狀態中的punt drop時，應該使用說明工具進一步隔離問題。