

# EGTP路徑故障排除

## 目錄

---

[簡介](#)

[概觀](#)

[EGTP路徑失敗的可能原因](#)

[需要日誌](#)

[疑難排解指令](#)

[案例/原因簡介](#)

[連通性問題-網路連線問題](#)

[重新啟動計數器值更改](#)

[大量傳入流量請求-網路擁塞](#)

[解決方案](#)

[因應措施](#)

[配置更改](#)

[偵錯記錄](#)

---

## 簡介

本文檔介紹如何對EGTP路徑故障問題進行故障排除。

## 概觀

演化的GPRS隧道協定(EGTP)路徑故障是指行動網路中GTP節點之間的通訊路徑問題。GTP是用於在不同網元之間傳輸使用者資料和信令消息的協定。

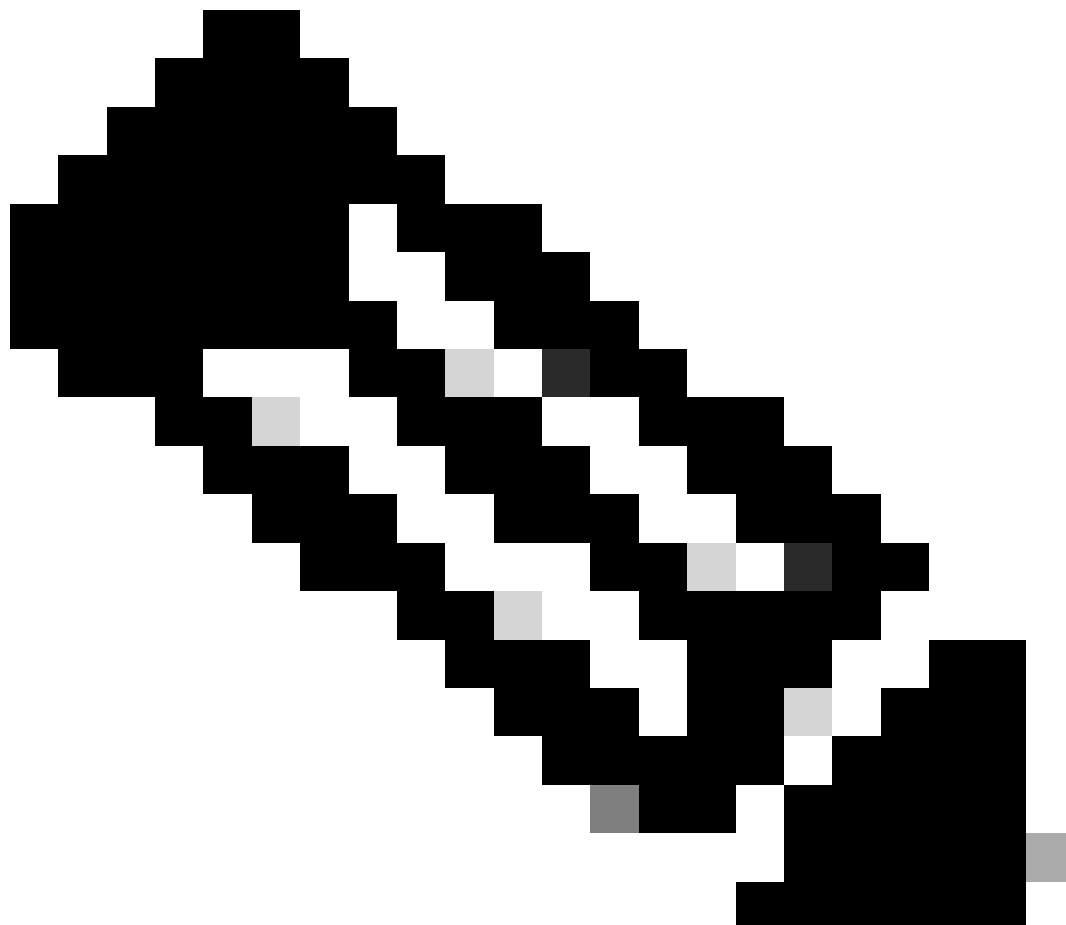
### EGTP路徑失敗的可能原因

1. 連通性問題-網路連線問題
2. 重新啟動計數器值更改
3. 巨大的傳入流量請求-網路擁塞
4. 關於DSCP/QOS等的配置問題
5. EGTP鏈路上沒有訂戶/會話

### 需要日誌

1. SSD/系統日誌涵蓋問題時間範圍，從問題開始前至少兩小時一直持續到目前時間。
2. 使用日誌確認可接通性，即發現路徑故障的路徑的ping和traceroute。

3. 有問題和無問題節點之間的配置檢查。
  4. 需要確認同一路徑上的流量是否突然增加或拒絕增加。
  5. 在問題發生的時間段內（至少在問題發生前2-3天）提供批次統計資料。
- 



注意：根據問題型別，可能需要前面提到的日誌。並非每次都需要所有日誌。

---

## 疑難排解指令

```
<#root>
```

```
show egtpc peers interface
```

```
show egtpc peers path-failure-history
```

```
show egtpc statistics path-failure-reasons
```

```
show egtp-service all
```

```
show egtpc sessions
```

```
show egtpc statistics
```

```
egtpc test echo gtp-version 2 src-address <source node IP address> peer-address <remote node IP address>
```

For more details related to above command refer doc as mentioned below

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/gateway-gprs-support-node-ggsn/119246-tech.html>

SNMP陷阱：

```
Sun Feb 05 03:00:20 2023 Internal trap notification 1112 (EGTPCPathFail) context s11mme, service s11-mm
```

```
Tue Jul 09 18:41:36 2019 Internal trap notification 1112 (EGTPCPathFail) context pgw, service s5-s8-sgw
```

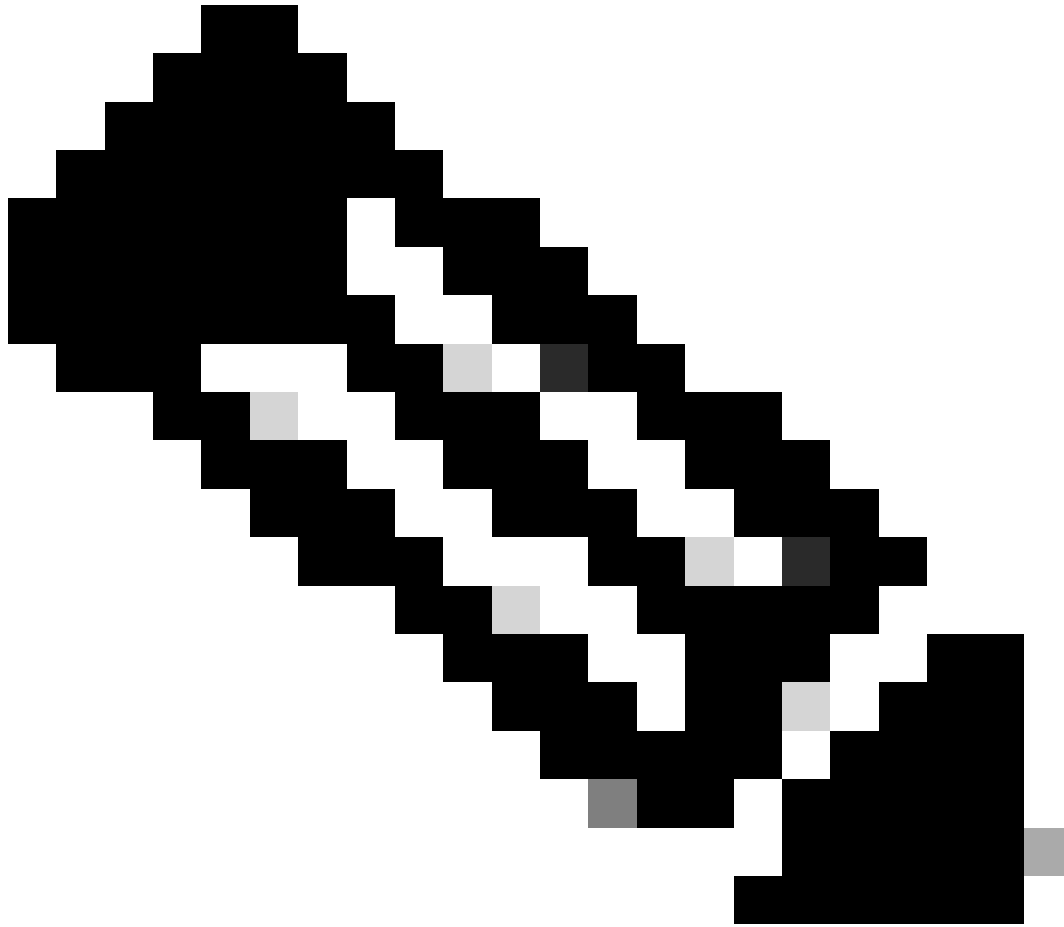
## 案例/原因簡介

### 連通性問題-網路連線問題

當路由路徑中的問題可能在SGSN/MME和SPGW/GGSN之間的路由器端或防火牆時，就會發生可達性問題。

```
ping <destination IP>
```

```
tracert <destination IP> src <source IP>
```



注意：必須從運行EGTP服務的內容中檢查兩個用於檢查可接通性的命令。

## 重新啟動計數器值更改

EGTP路徑在SGSN/MME和GGSN/SPGW之間的路徑的兩端維護重新啟動計數器。



要詳細瞭解此類問題，請參閱<https://www.cisco.com/c/en/us/support/docs/wireless/asr-5000-series/200026-ASR-5000-Series-Troubleshooting-GTPC-and.html>連結。

## 大量傳入流量請求-網路擁塞

每當突然出現高流量事務時，就有可能發生EGTP Tx和Rx資料包丟棄。確認此情況的基本檢查：

1. 您必須檢查egtpinmgr的CPU使用率是否過高。

```
Mar 25 14:30:48 10.224.240.132 evlogd: [local-60sec48.142] [resmgr 14907 debug] [6/0/10088 <rmmgr:60> _  
Mar 25 14:31:05 10.224.240.132 evlogd: [local-60sec5.707] [resmgr 14907 debug] [6/0/10088 <rmmgr:60> _r
```

2. 檢查回聲請求/響應是否失敗 ( 之前共用了命令 )。

3. 可以檢查demux卡是否丟棄任何資料包。

所有EGTP入站流量都必須透過同一個egtpmgr。如果一個節點出現路徑故障，入站流量可能會增加。並且，您可能會在egtpmgr進程級別遇到資料流丟棄。即使是協同定位的進程也必須透過相同的egtpmgr隊列進行並受到影響。

下面是檢查資料包丟失的步驟，該資料包丟失必須透過多次迭代才能完成

<#root>

```
debug shell card <> cpu 0
```

```
cat /proc/net/boxer
```

```
***** card1-cpu0 /proc/net/boxer *****
```

```
Wednesday March 25 17:34:54 AST 2020
```

what	total_used	next	refills	hungry	exhausted	system_rate_kbps	system_cr
bdp_rld	4167990936249KB	094	51064441	292	1	3557021/65000000	7825602KB/7934

what	bhn	local	remote	ver	rx	rx_drop	tx
total cpu 34	*	*	*	*	3274522	59	60
total cpu 35	*	*	*	*	6330639	46	121

```
total cpu 46      * * * * * 5076520      27      15524

total cpu 47      * * * * * 4163101019      83922  133540922
```

4. 如果發現egtpinmgr的CPU使用率較高，則必須捕獲egtpinmgr CPU分析器輸出。

如果上述所有條件都有效，則您可以檢查是否出現了上述可能的解決方案。

## 解決方案

1. 增加EGTP回應逾時-如果5秒沒有幫助，您可以嘗試15或25。您可以與您的AS團隊討論此問題以調整此功能。

2. 減少對等拯救逾時-逾時值越小，非作用中對等體的數目就越少，因此您可以使用此命令變更時間值：

```
gtpc peer-salvation min-peers 2000 timeout 24
```

3. 過載保護-可以根據流量趨勢進行過載保護最佳化，因為在egpinmgr遇到問題之前不知道確切的傳入流量速率，很難對其進行調整。此外，由於無訊息捨棄，錯誤調整也會導致額外的訊號流量。

因此，對於超載保護最佳化，您可以從egtpinmgr和CPU分析器輸出的解複用卡中收集一些資料包丟棄，如前所述。

4. EGTPC鏈路上沒有訂戶/會話-當特定隧道上沒有會話時，GTP回聲功能將停止。如果沒有連線的使用者，則不得傳送GTPC響應。

以下是停止回應功能時看到的錯誤：

```
2019-Jul-26+08:41:51.261 [egtpmgr 143047 debug] [1/0/4626 <egtpinmgr:2> egtpmgr_pm.c:798] [context: EPC
2019-Jul-26+08:41:51.261 [egtpmgr 143048 debug] [1/0/4626 <egtpinmgr:2> egtpmgr_pm.c:818] [context: EPC
```

## 因應措施

您可以嘗試重新啟動egtpinmgr工作以進行復原。但是，重新啟動egtpinmgr可能會帶來短期影響，終端使用者不會察覺，而新任務中會重新安裝NPU流。

此操作必須少於1秒才能完成。

1. 停用路徑失敗偵測：

```
egtp-service S5-PGW
```

```
no gtpc path-failure detection-policy
```

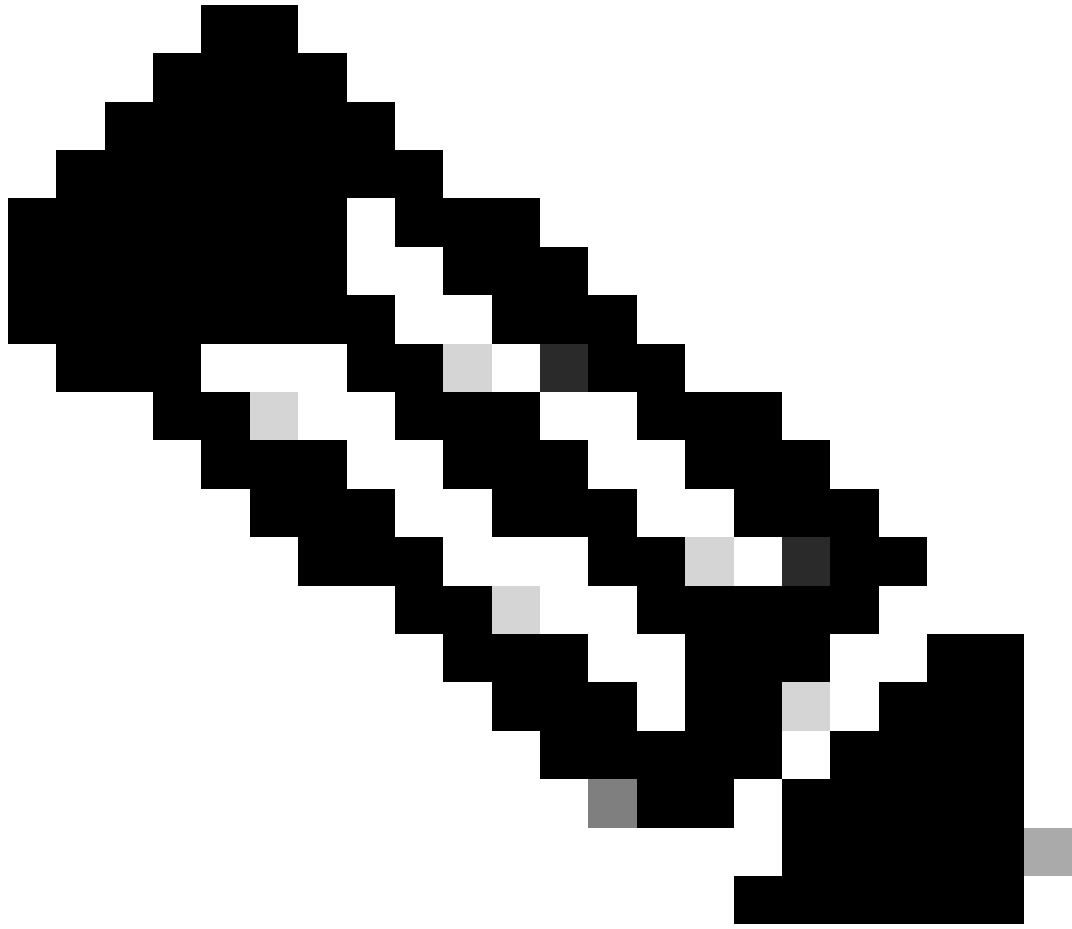
## 2. 終止egtpinmgr任務：

```
task kill facility egtpinmgr all
```

## 3. 啟用路徑故障檢測：

```
egtp-service S5-PGW
```

```
gtpc path-failure detection-policy
```



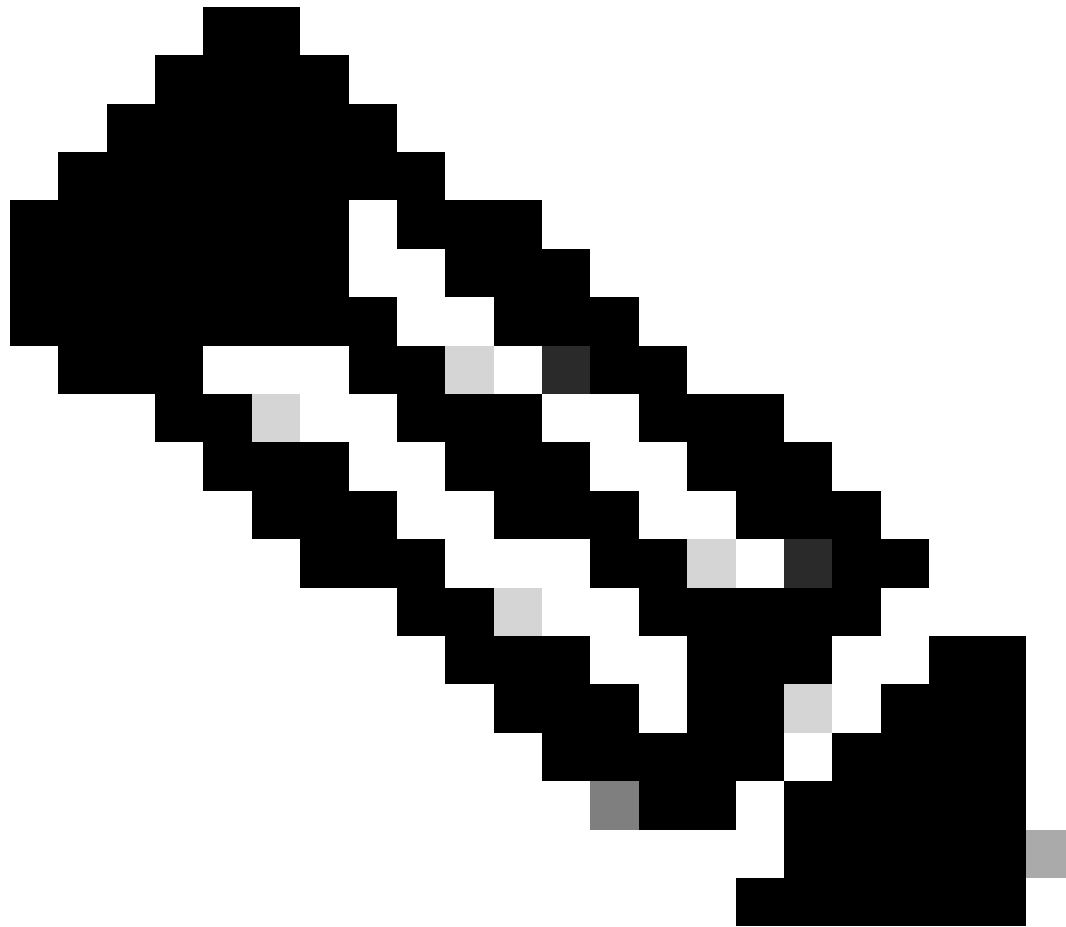
註：此解決方法只能在MW中實施，因為它會造成一些影響。

---

## 配置更改

可以檢查DSCP/QOS/EGTP IP路徑/服務對映方面的配置。





注意：這些是導致EGTP路徑失敗的主要原因，但在找不到任何場景的情況下，您可以進一步收集一些跟蹤和調試日誌。

---

## 偵錯記錄

( 如果需要 )

```
logging filter active facility egtpc level<critical/error/debug>  
logging filter active facility egtpmgr level<critical/error/debug>  
logging filter active facility egtpinmgr level<critical/error/debug>
```

## 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）。