

# Dépannage des défaillances du chemin EGTP

## Table des matières

---

[Introduction](#)

[Aperçu](#)

[Raisons possibles des défaillances du chemin EGTP](#)

[Journaux requis](#)

[Dépannage des commandes](#)

[Scénario/Raisons en bref](#)

[Problème d'accessibilité - Problèmes de connectivité réseau](#)

[Redémarrer les modifications des valeurs du compteur](#)

[Demande de trafic entrant énorme - Encombrement du réseau](#)

[Solution](#)

[Solution de contournement](#)

[Problèmes liés à la modification de la configuration](#)

[Journaux de débogage](#)

---

## Introduction

Ce document décrit comment dépanner les problèmes de défaillance du chemin EGTP.

## Aperçu

Les défaillances de chemin EGTP (Evolved GPRS Tunneling Protocol) font référence à des problèmes de chemin de communication entre les noeuds GTP dans un réseau mobile. GTP est un protocole utilisé dans le transport de données utilisateur et de messages de signalisation entre différents éléments du réseau.

## Raisons possibles des défaillances du chemin EGTP

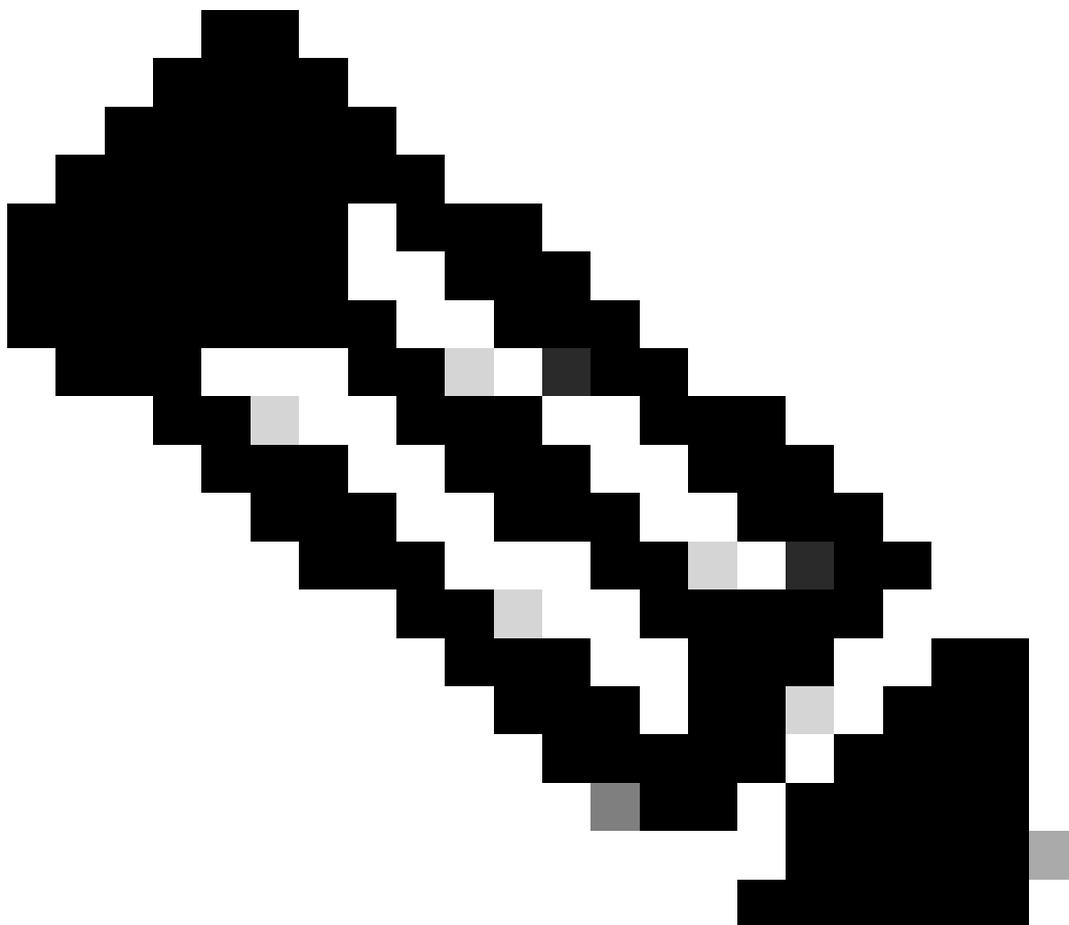
1. Problème d'accessibilité - Problèmes de connectivité réseau
2. Modifications des valeurs du compteur de redémarrage
3. Demande de trafic entrant énorme - Congestion du réseau
4. Problème de configuration en termes de DSCP/QOS, etc
5. Aucun abonné/aucune session sur la liaison EGTPC

## Journaux requis

1. SSD/syslog autour de l'heure problématique couvrant la période au moins deux heures avant le

début du problème jusqu'à l'heure actuelle.

2. Confirmation d'accessibilité avec les journaux, c'est-à-dire ping et traceroute pour le chemin pour lequel des défaillances de chemin sont observées.
  3. Vérification de la configuration entre les noeuds problématiques et non problématiques.
  4. Nécessité de confirmer si une augmentation soudaine du trafic ou une augmentation du rejet sur le même chemin.
  5. Bulkstats pendant les périodes problématiques couvrant la période au moins 2-3 jours avant le problème.
- 



Remarque : selon le type de problème, les journaux mentionnés précédemment peuvent être requis. Tous les journaux ne sont pas requis à chaque fois.

---

## Dépannage des commandes

<#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-techr>

Déroutements SNMP :

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

## Scénario/Raisons en bref

### Problème d'accessibilité - Problèmes de connectivité réseau

Les problèmes d'accessibilité surviennent lorsqu'un problème dans le chemin de la route peut se situer à l'extrémité du routeur ou du pare-feu entre SGSN/MME et SPGW/GGSN.

ping <destination IP>

traceroute <destination IP> src <source IP>



Remarque : les deux commandes permettant de vérifier l'accessibilité doivent être vérifiées à partir du contenu où le service EGTP s'exécute.

---

## Redémarrer les modifications des valeurs du compteur

Le chemin EGTP maintient les compteurs de redémarrage aux deux extrémités du chemin entre SGSN/MME et GGSN/SPGW.



Consultez le lien <https://www.cisco.com/c/en/us/support/docs/wireless/asr-5000-series/200026->

[ASR-5000-Series-Troubleshooting-GTPC-and.html](#) afin de comprendre ce type de problème en détail.

## Demande de trafic entrant énorme - Encombrement du réseau

Chaque fois qu'il y a des transactions soudaines à fort trafic, il y a un risque de perte de paquets EGTP Tx et Rx. Vérifications de base pour confirmer ce scénario :

1. Vous devez vérifier s'il y a une utilisation CPU élevée pour egtpinmgr.

```
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. Vérifiez si la requête/réponse d'écho échoue (commande partagée précédemment).

3. Peut vérifier s'il y a des pertes de paquets de la carte de démultiplexage.

Tout le trafic entrant EGTP doit passer par le même egtpmgr. Si des défaillances de chemin sont observées avec un noeud, le volume du trafic entrant augmente probablement. De plus, vous pouvez constater une baisse du trafic au niveau du processus egtpmgr. Même le processus colocalisé doit passer par la même file d'attente egtpmgr et être impacté.

Voici l'étape permettant de vérifier la perte de paquets qui doit être effectuée avec plusieurs itérations

<#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/793
```

```
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. Vous devez capturer la sortie du profileur de CPU d'egtpinmgr si vous voyez un CPU élevé pour egtpinmgr.

Si toutes les conditions ci-dessus sont valides, alors vous pouvez vérifier la solution possible mentionnée.

## Solution

1. Augmentation du délai d'attente d'écho EGTP - Si 5 secondes ne vous aident pas, vous pouvez essayer 15 ou 25. Vous pouvez en discuter avec votre équipe AS pour régler ce problème.

2. Diminuer le délai d'attente de salut par les pairs : plus la valeur du délai d'attente est faible, plus le nombre d'homologues inactifs est faible. Vous pouvez donc modifier la valeur du délai à l'aide de cette commande :

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

3. protection contre les surcharges - l'optimisation de la protection contre les surcharges peut être effectuée en fonction de la tendance du trafic, car sans connaître le débit exact du trafic entrant avant qu'egpinmgr ne rencontre le problème, il est difficile de régler cela. En outre, un mauvais réglage peut entraîner un trafic de signalisation supplémentaire dû à des abandons silencieux.

Ainsi, pour l'optimisation de la protection contre les surcharges, vous pouvez collecter quelques paquets abandonnés de la carte de démultiplexage pour les sorties de egtpinmgr et du profileur de CPU comme mentionné précédemment.

4. Absence d'abonnés/de sessions sur la liaison EGTPC : en l'absence de sessions sur un tunnel spécifique, la fonctionnalité d'écho GTP est arrêtée. Si aucun abonné n'est connecté, l'écho GTPC ne doit pas être envoyé.

Voici les erreurs que vous voyez lorsque la fonctionnalité d'écho est arrêtée :

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

## Solution de contournement

Vous pouvez essayer de redémarrer la tâche egtpinmgr afin de récupérer. Mais, le redémarrage de l'egtpinmgr peut avoir un impact à court terme, insensible pour l'utilisateur final, tandis que les flux NPU sont réinstallés dans la nouvelle tâche.

Cette opération doit prendre moins d'une seconde.

1. Désactivez la détection des défaillances de chemin :

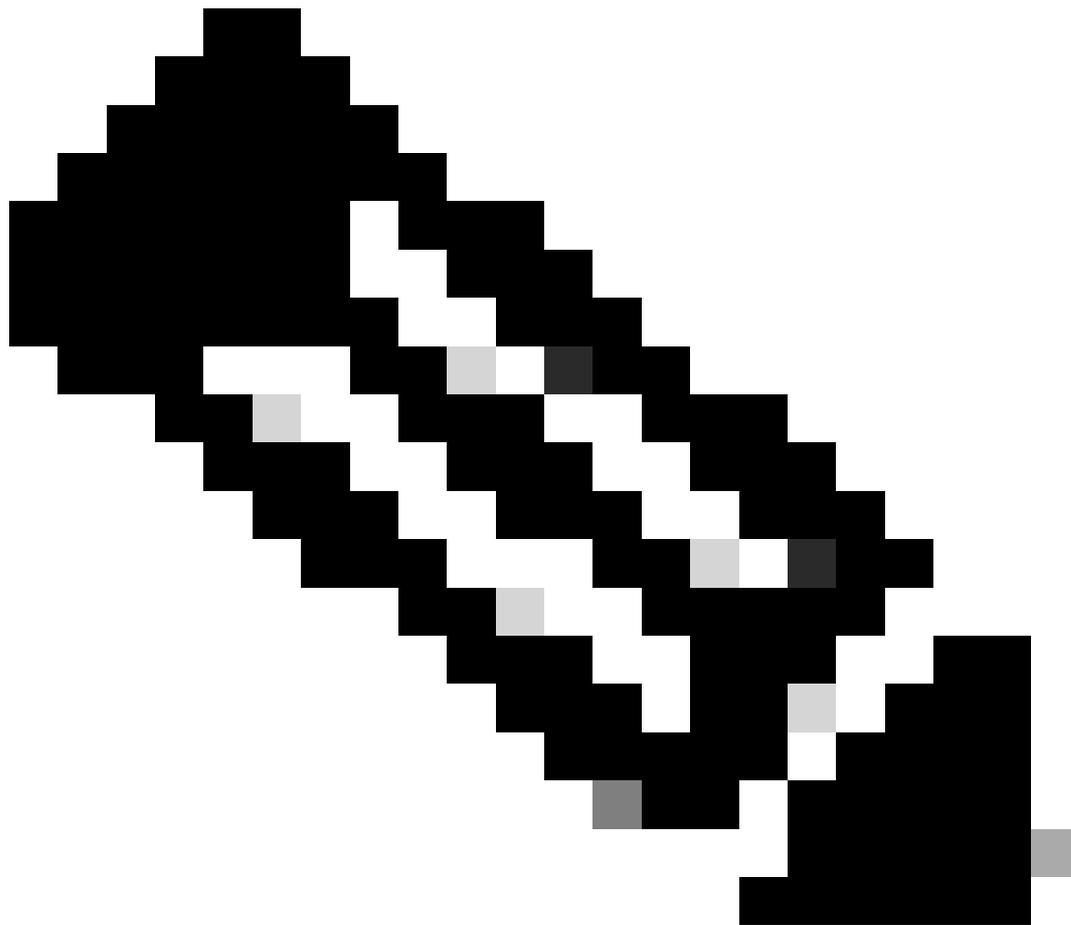
```
egtp-service S5-PGW  
no gtpc path-failure detection-policy
```

2. Tâche Kill egtpinmgr :

```
task kill facility egtpinmgr all
```

3. Activez la détection des pannes de chemin :

```
egtp-service S5-PGW  
gtpc path-failure detection-policy
```



Remarque : cette solution de contournement doit être implémentée uniquement dans MW, car elle peut avoir un impact.

---

## Problèmes liés à la modification de la configuration

La configuration en termes de mappage chemin IP/service DSCP/QOS/EGTP peut être vérifiée.



Remarque : ce sont les principales raisons qui contribuent aux échecs du chemin EGTP, mais si aucun des scénarios n'est trouvé, vous pouvez collecter des traces et des journaux de débogage plus loin.

---

## Journaux de débogage

(Si nécessaire)

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.