Fehlerbehebung bei EGTP-Pfadfehlern

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei Problemen mit dem EGTP-Pfad beschrieben.

Überblick

EGTP-Pfadfehler (Evolved GPRS Tunneling Protocol) beziehen sich auf Probleme mit dem Kommunikationspfad zwischen den GTP-Knoten in einem mobilen Netzwerk. GTP ist ein Protokoll, das für den Transport von Nutzdaten und Signalisierungsnachrichten zwischen verschiedenen Netzwerkelementen verwendet wird.

Mögliche Gründe für EGTP-Pfadfehler

1. Erreichbarkeitsproblem - Probleme mit der Netzwerkverbindung

2. Zählerwertänderungen neu starten

3. Große Anforderung von eingehendem Datenverkehr - Netzwerküberlastung

4. Konfigurationsproblem mit DSCP/QoS usw.

5. Keine Teilnehmer/Sitzungen auf dem EGTPC-Link

Erforderliche Protokolle

1. SSD/Syslogs rund um problematische Zeit deckt den Zeitrahmen mindestens zwei Stunden vor

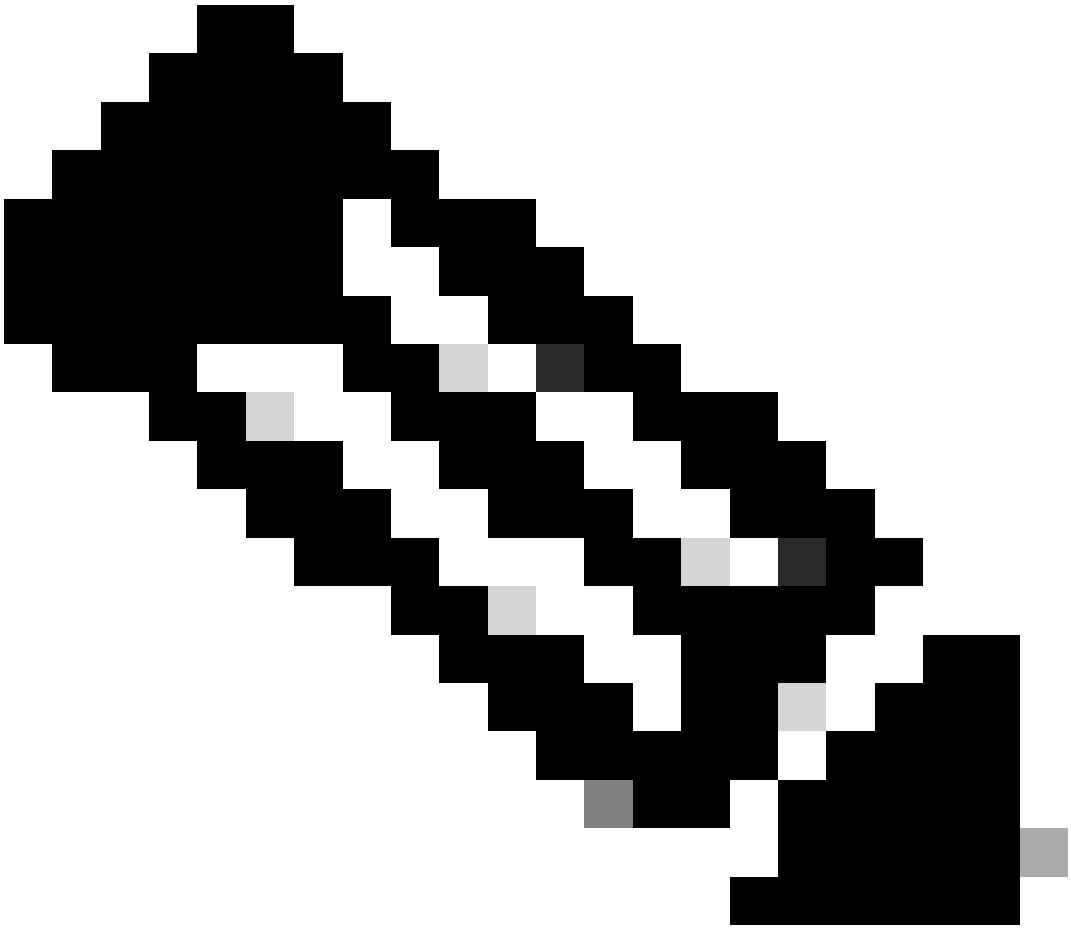
Beginn der Ausgabe bis zur aktuellen Zeit.

2. Erreichbarkeitsbestätigung mit Protokollen, d. h. Ping und Traceroute für den Pfad, für den Pfadfehler festgestellt werden.

3. Konfigurationsprüfung zwischen problematischen und unproblematischen Knoten.

4. Muss bestätigen, wenn eine plötzliche Zunahme des Datenverkehrs oder eine Erhöhung der Ablehnung auf dem gleichen Pfad.

5. Bulkstats während problematischer Zeiten, die den Zeitrahmen mindestens 2-3 Tage vor der Ausgabe abdecken.



Hinweis: Je nach Art des Problems können die zuvor erwähnten Protokolle erforderlich sein. Nicht alle Protokolle werden jedes Mal benötigt.

Befehle für die Fehlerbehebung

<#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 addres
```

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-techn

SNMP-Traps:

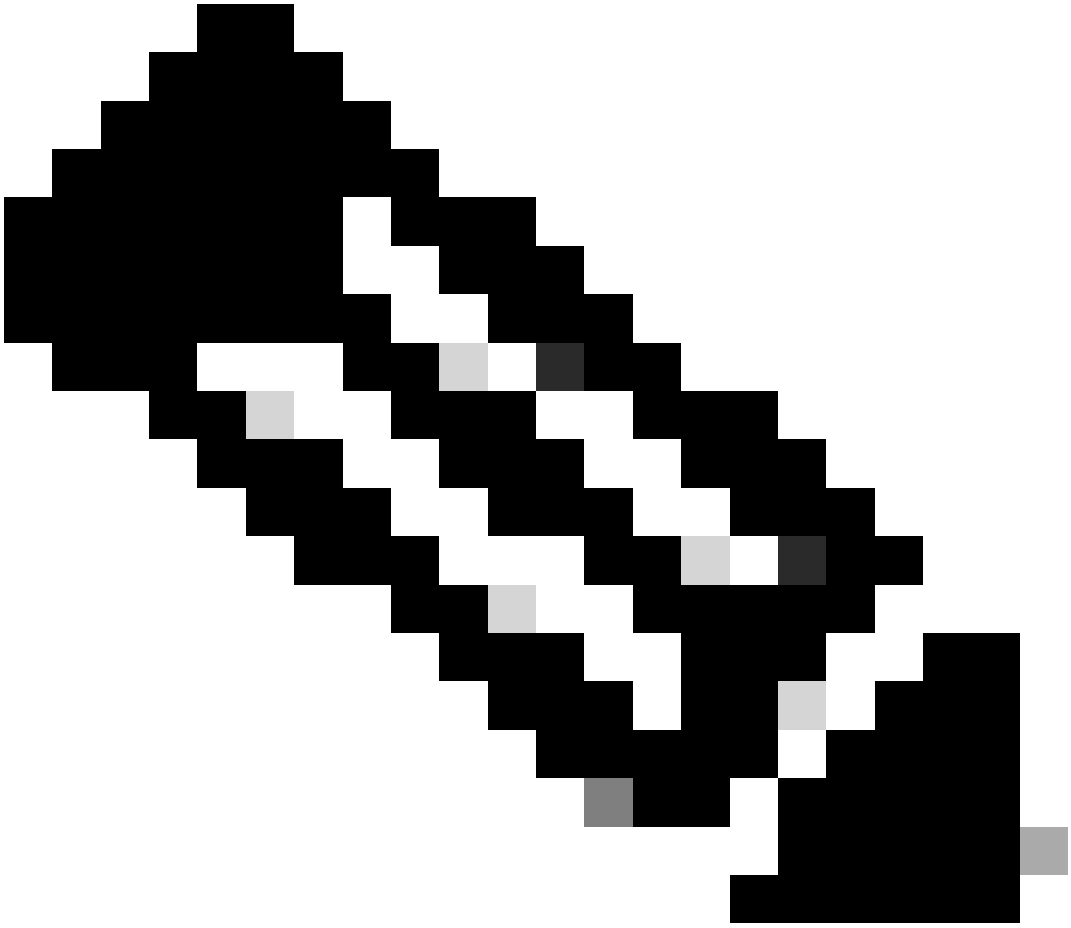
```
Sun Feb 05 03:00:20 2023 Internal trap notification 1112 (EGTPCPathFail) context s11mme, service s11-mm

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

Szenario/Gründe in Kürze

Erreichbarkeitsproblem - Probleme mit der Netzwerkverbindung

Erreichbarkeitsprobleme treten auf, wenn ein Problem im Routing-Pfad auf dem Router-Ende oder der Firewall zwischen SGSN/MME und SPGW/GGSN auftreten kann.

```
ping <destination IP>

traceroute <destination IP> src <source IP>
```



Hinweis: Beide Befehle zur Überprüfung der Erreichbarkeit müssen von dem Inhalt aus überprüft werden, in dem der EGTP-Dienst ausgeführt wird.

Neustarten von Zählerwertänderungen

Über den EGTP-Pfad werden die Neustartzähler an beiden Enden des Pfads zwischen SGSN/MME und GGSN/SPGW beibehalten.

Unter dem Link https://www.cisco.com/c/en/us/support/docs/wireless/asr-5000-series/200026-

ASR-5000-Series-Troubleshooting-GTPC-and.html finden Sie weitere Informationen zu dieser Art von Problem.

Enorme Anforderung von eingehendem Datenverkehr - Netzwerküberlastung

Bei plötzlichen Transaktionen mit hohem Datenverkehr besteht die Chance, dass EGTP-Pakete vom Typ Tx und Rx verworfen werden. Grundlegende Prüfungen zur Bestätigung dieses Szenarios:

1. Sie müssen überprüfen, ob eine hohe CPU-Auslastung für egtpinmgr vorliegt.

```
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. Überprüfen Sie, ob die Echoanfrage/-antwort fehlschlägt (zuvor freigegebener Befehl).

3. Kann überprüfen, ob Pakete von der Demux-Karte verloren gehen.

Der gesamte eingehende EGTP-Datenverkehr muss über denselben egtpmgr erfolgen. Wenn bei einem Knoten Pfadausfälle festgestellt werden, steigt das Volumen des eingehenden Verkehrs wahrscheinlich an. Außerdem können Sie einen Datenverkehrsverlust auf Ebene des egtpmgr-Prozesses feststellen. Selbst der am selben Standort durchgeführte Prozess muss dieselbe egtpmgr-Warteschlange durchlaufen, um sich auszuwirken.

Im Folgenden wird der Schritt zum Überprüfen von Paketverlusten beschrieben, die mit mehreren Iterationen durchgeführt werden müssen.

<#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. Muss die Ausgabe des egtpinmgr CPU Profilers erfassen, wenn Sie eine hohe CPU für egtpinmgr sehen.

Wenn alle oben genannten Bedingungen gültig sind, können Sie nach der genannten möglichen Lösung suchen.

Lösung

1. Vergrößerung des EGTP-Echo-Timeouts: Wenn 5 Sekunden nicht helfen, können Sie 15 oder 25 versuchen. Sie können dies mit Ihrem AS-Team besprechen, um dies abzustimmen.

2. Verringern Sie den Timeout für Peer-Bergung - Je niedriger der Timeout-Wert, desto weniger inaktive Peers. Sie können den Zeitwert daher mit dem folgenden Befehl ändern:

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

3. Überlastungsschutz - Überlastungsschutzoptimierung kann basierend auf dem Datenverkehrstrend durchgeführt werden, da ohne die genaue Eingangsverkehrsrate zu kennen, bevor egpinmgr auf das Problem trifft, es schwierig ist, dies anzupassen. Außerdem kann eine falsche Feinabstimmung zu zusätzlichem Signalisierungsverkehr führen, da es zu unbeaufsichtigten Unterbrechungen kommt.

Um den Überlastungsschutz zu optimieren, können Sie also, wie bereits erwähnt, einige Paketverluste von der Demux-Karte für egtpinmgr- und CPU-Profiler-Ausgaben sammeln.

4. Keine Abonnenten/Sitzungen auf dem EGTPC-Link - Wenn keine Sitzungen über einen bestimmten Tunnel vorhanden sind, wird die GTP-Echo-Funktion gestoppt. Wenn kein angeschlossener Teilnehmer vorhanden ist, darf kein GTPC-Echo gesendet werden.

Wenn die Echo-Funktion beendet wird, werden folgende Fehler angezeigt:

```
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
```

Problemumgehung

Sie können versuchen, die Aufgabe egtpinmgr neu zu starten, um sich zu erholen. Der Neustart des egtpinmgr kann jedoch kurzfristige Auswirkungen haben, die für den Endbenutzer nicht bemerkbar sind, während die NPU-Flows bei der neuen Aufgabe neu installiert werden.

Dieser Vorgang muss weniger als 1 Sekunde in Anspruch nehmen.

1. Deaktivieren Sie die Pfadausfallerkennung:

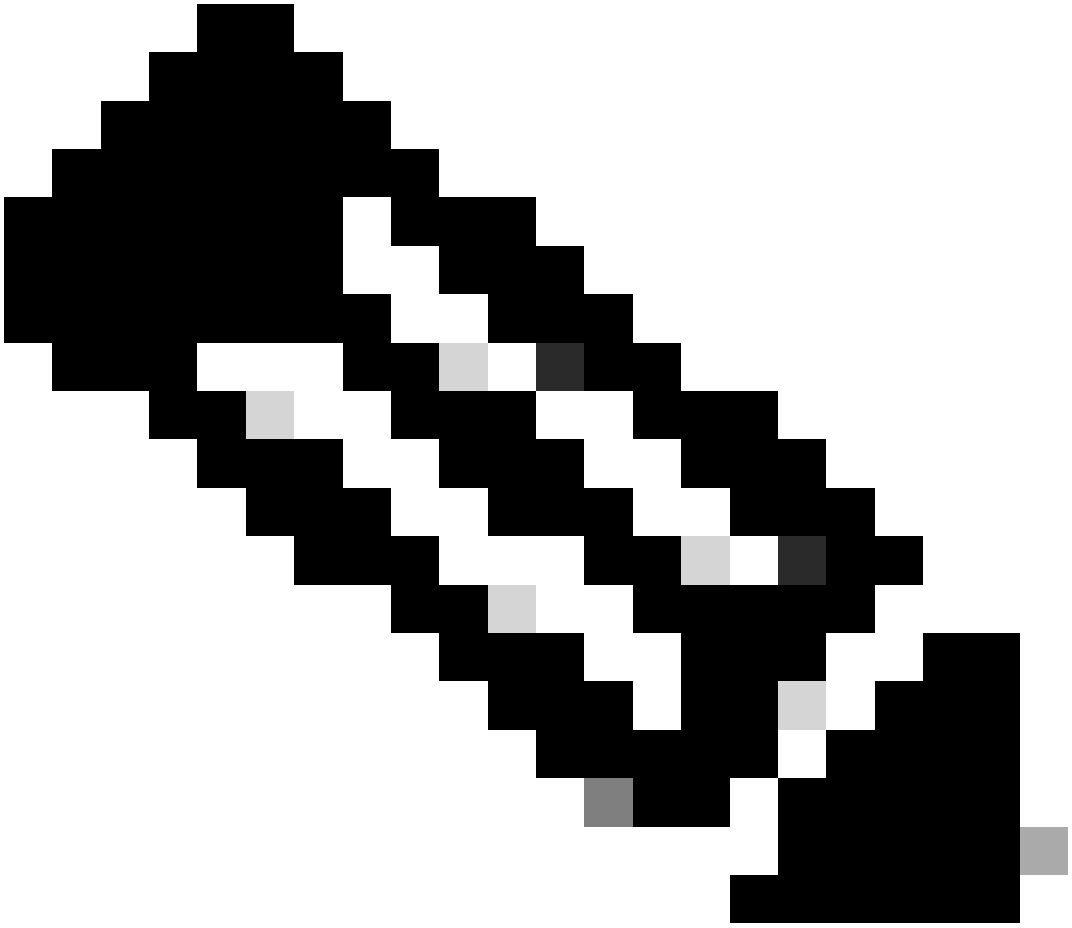
```
    egtp-service S5-PGW

       no gtpc path-failure detection-policy
```

2. Beenden Sie die Aufgabe egtpinmgr:

```
task kill facility egtpinmgr  all
```

3. Aktivieren Sie die Pfadfehlererkennung:

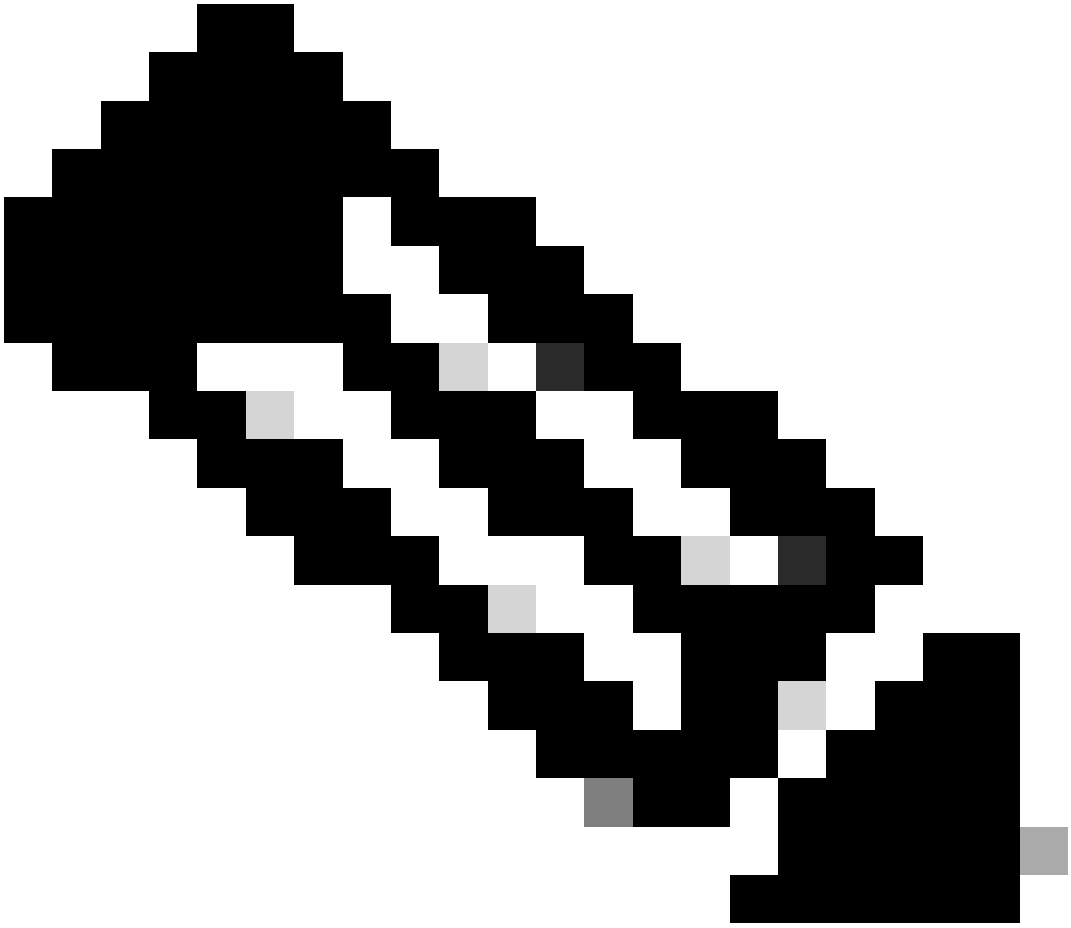
```
    egtp-service S5-PGW

       gtpc path-failure detection-policy
```



Hinweis: Diese Problemumgehung darf nur in MW implementiert werden, da sie Auswirkungen haben kann.

Konfigurationsänderungen

Die Konfiguration hinsichtlich der DSCP-/QOS-/EGTP-IP-Pfad-/Service-Zuordnung kann überprüft werden.



Hinweis: Dies sind die Hauptgründe für EGTP-Pfadfehler. Falls jedoch keines der Szenarien gefunden wird, können Sie einige Ablaufverfolgungen und Debugging-Protokolle sammeln.

Debugging-Protokolle

(Falls erforderlich)

```
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>
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.