Solución de problemas de errores de ruta EGTP

Contenido

Introducción

Este documento describe cómo resolver problemas de falla en la trayectoria de EGTP.

Overview

Las fallas de trayectoria del Protocolo de tunelización GPRS (EGTP) evolucionado se refieren a problemas con la trayectoria de comunicación entre los nodos GTP en una red móvil. GTP es un protocolo utilizado en el transporte de datos de usuario y mensajes de señalización entre diferentes elementos de red.

Posibles razones de las fallas de trayecto de EGTP

1. Problema de disponibilidad: problemas de conectividad de red

2. Reiniciar cambios de valores de contador

3. Enorme solicitud de tráfico entrante - Congestión de la red

4. Problema de configuración en términos de DSCP/QOS, etc.

5. No hay suscriptores/sesiones en el enlace EGTPC

Registros necesarios

1. SSD/syslogs en torno al tiempo problemático que cubre el marco de tiempo al menos dos horas

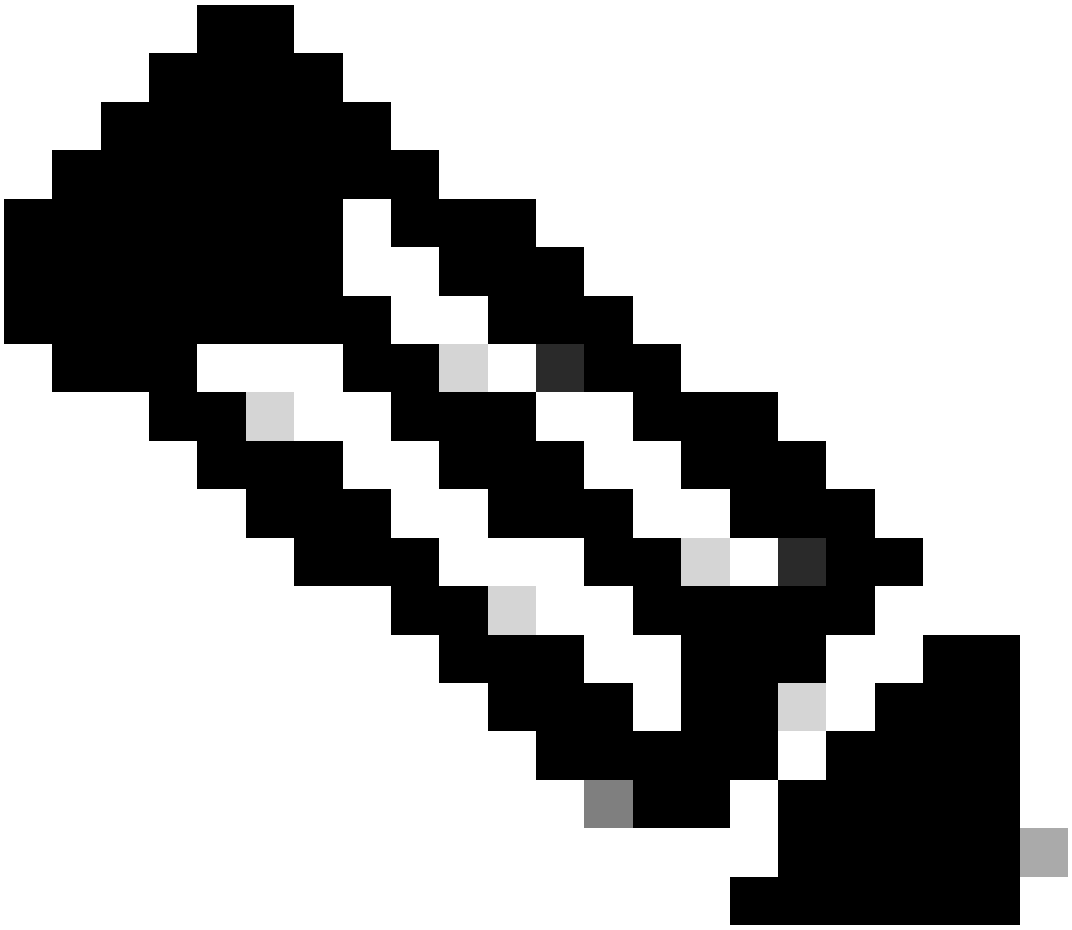
antes de que el problema comenzó hasta el tiempo actual.

2. Confirmación de disponibilidad con registros, es decir, ping y traceroute para la trayectoria para la cual se observan fallas de trayectoria.

3. Verificación de la configuración entre nodos problemáticos y no problemáticos.

4. Necesidad de confirmar si hay algún aumento repentino en el tráfico o cualquier aumento en el rechazo en el mismo trayecto.

5. Estadísticas masivas durante tiempos problemáticos que cubran el período de tiempo al menos 2-3 días antes de la emisión.



Nota: Dependiendo del tipo de problema, los registros mencionados anteriormente pueden ser necesarios. No todos los registros son obligatorios cada vez.

Comandos para resolución de problemas

<#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

Trampas del protocolo 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
```

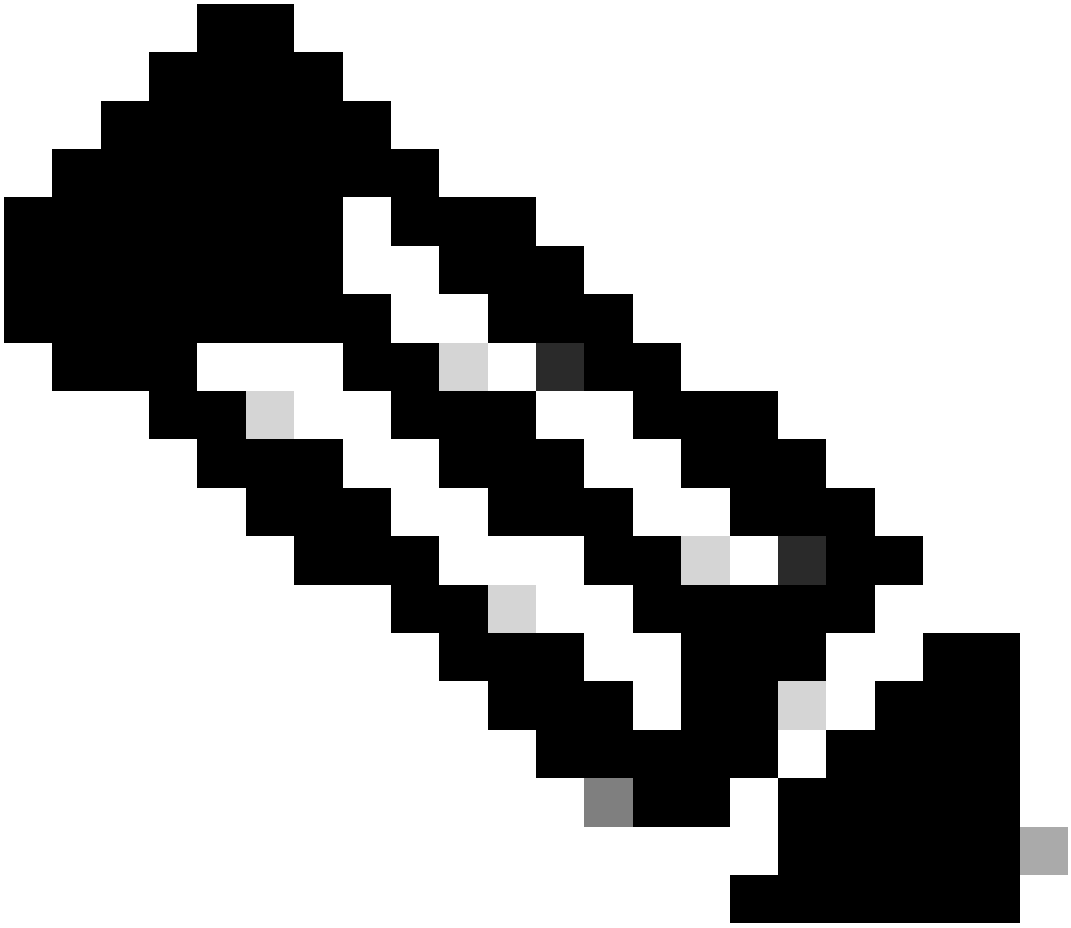
Escenario/Razones en resumen

Problema de disponibilidad: problemas de conectividad de red

Los problemas de disponibilidad ocurren cuando un problema en la trayectoria de ruta puede estar en el extremo del router o en el firewall entre SGSN/MME y SPGW/GGSN.

```
ping <destination IP>

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



> Nota: ambos comandos para verificar la disponibilidad deben ser verificados desde el contenido donde se ejecuta el servicio EGTP.

Reiniciar cambios de valores de contadores

La trayectoria EGTP mantiene los contadores de reinicio en ambos extremos de la trayectoria entre SGSN/MME y GGSN/SPGW.

Consulte el enlace https://www.cisco.com/c/en/us/support/docs/wireless/asr-5000-series/200026-

ASR-5000-Series-Troubleshooting-GTPC-and.html para entender este tipo de problema en detalle.

Gran petición de tráfico entrante: congestión de red

Siempre que hay transacciones de alto tráfico repentinas, existe la posibilidad de que se descarten paquetes Rx y Tx de EGTP. Comprobaciones básicas para confirmar esta situación:

1. Debe verificar si hay un uso elevado de la CPU para 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. Compruebe si falla la solicitud/respuesta de eco (comando compartido anteriormente).

3. Puede verificar si hay alguna pérdida de paquetes de la tarjeta de demux.

Todo el tráfico entrante de EGTP debe pasar por el mismo egtpmgr. Si se observan fallas de trayectoria en un nodo, es probable que el volumen de tráfico entrante aumente. Además, puede experimentar una caída del tráfico en el nivel de proceso de egtpmgr. Incluso el proceso co-ubicado debe continuar a través de la misma cola de egtpmgr y se verá afectado.

Este es el paso para verificar la pérdida de paquetes que se debe realizar con varias iteraciones

<#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. Debe capturar la salida del analizador de CPU egtpinmgr si observa una CPU alta para egtpinmgr.

Si todas las condiciones anteriores son válidas, puede buscar la solución posible mencionada.

Solución

1. Aumento en el tiempo de espera de eco EGTP - Si 5 segundos no ayuda, puede probar 15 o 25. Puede comentar esto con su equipo de AS para ajustar esto.

2. Disminuir el tiempo de espera de salvación de pares: Cuanto más bajo sea el valor del tiempo de espera, menor será el número de pares inactivos, por lo que puede cambiar el valor del tiempo con este comando:

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

3. protección contra sobrecargas: la optimización de la protección contra sobrecargas se puede hacer en función de la tendencia del tráfico, ya que sin conocer la velocidad exacta del tráfico entrante antes de que egpinmgr detecte el problema, es difícil ajustar esto. Además, un ajuste incorrecto puede causar tráfico de señalización adicional debido a caídas silenciosas.

Por lo tanto, para la optimización de la protección contra sobrecarga, puede recopilar algunas caídas de paquetes de la tarjeta de demux para obtener salidas de getpinmgr y del analizador de CPU, como se mencionó anteriormente.

4. No hay suscriptores/sesiones en el link EGTPC - cuando no hay sesiones en un túnel específico, se detiene la funcionalidad de eco GTP. Si hay cero/ningún suscriptor conectado, no se debe enviar eco GTPC.

Estos son los errores que se ven cuando se detiene la funcionalidad de eco:

```
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
```

Solución Aternativa

Puede intentar reiniciar la tarea egtpinmgr para recuperarse. Sin embargo, reiniciar el egtpinmgr puede tener un impacto a corto plazo, que no se percibe en el usuario final, mientras que los flujos de NPU se reinstalan en la nueva tarea.

Esta operación debe tardar menos de 1 segundo en completarse.

1. Inhabilite la detección de falla de trayectoria:

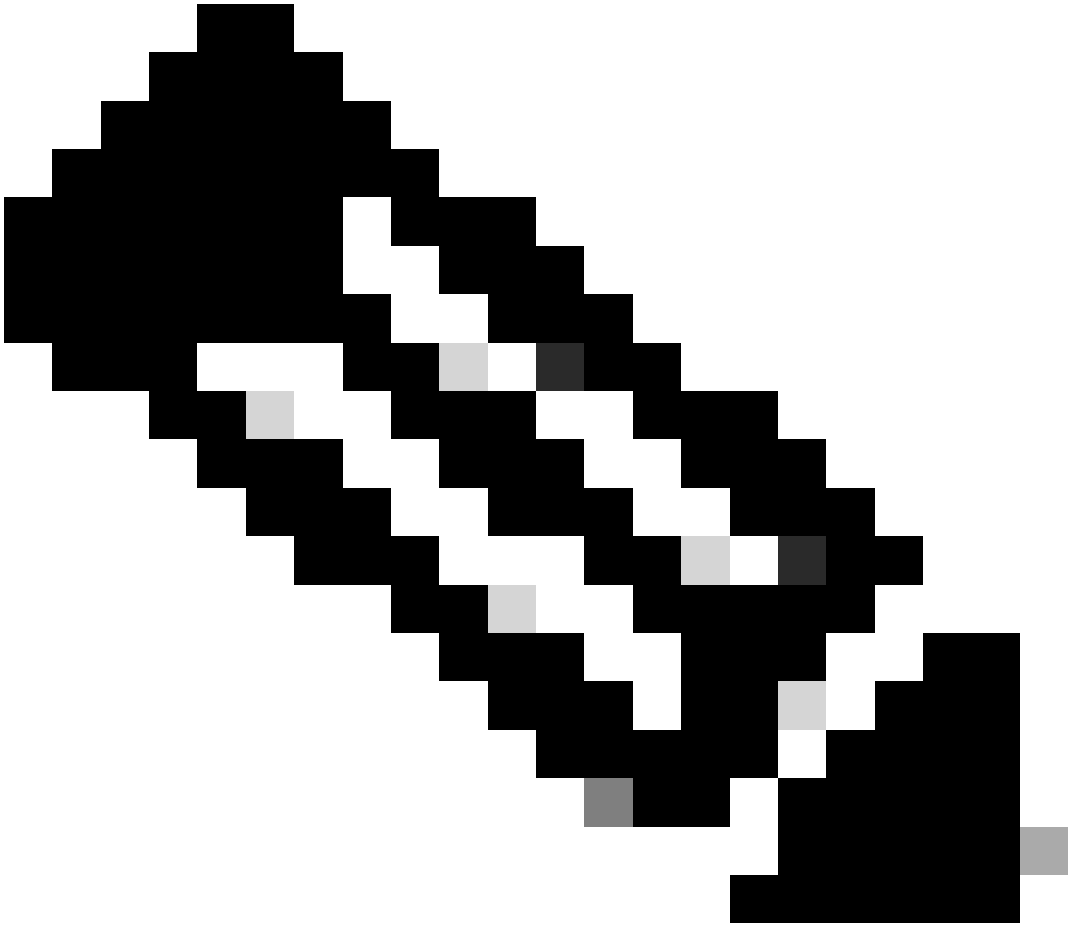
```
egtp-service S5-PGW
   no gtpc path-failure detection-policy
```

2. Matar tarea egtpinmgr:

```
task kill facility egtpinmgr  all
```

3. Active la detección de fallos de ruta:

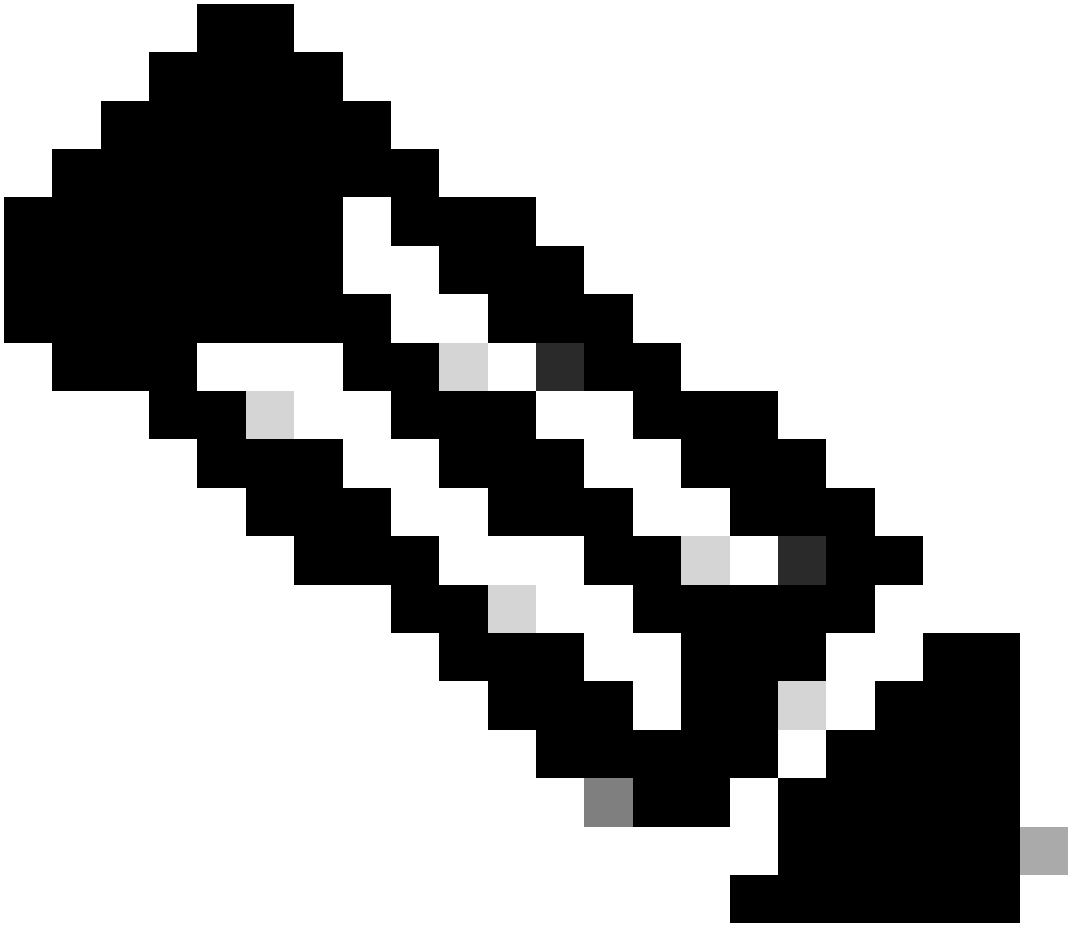
```
egtp-service S5-PGW
   gtpc path-failure detection-policy
```



Nota: esta solución alternativa debe implementarse solo en MW, ya que puede causar cierto impacto.

Cambios de configuración

Se puede verificar la configuración en términos de asignación de servicio/ruta IP DSCP/QOS/EGTP.



Nota: Estas son las razones principales que contribuyen a los errores de trayectoria de EGTP, pero en caso de que no se encuentre ninguno de los escenarios, puede recopilar algunos seguimientos y registros de depuración más adelante.

Registros de depuración

(Si es necesario)

```
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>
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).