Troubleshooting de Falhas de Caminho EGTP

Contents

Introdução

Este documento descreve como resolver problemas de falha de caminho EGTP.

Overview

As falhas de caminho do EGTP (Evolved GPRS Tunneling Protocol) referem-se a problemas com o caminho de comunicação entre os nós GTP em uma rede móvel. O GTP é um protocolo usado no transporte de dados de usuários e mensagens de sinalização entre diferentes elementos da rede.

Possíveis motivos para falhas de caminho EGTP

1. Problema de acessibilidade - Problemas de conectividade de rede

2. Reiniciar alterações de valores do contador

3. Enorme solicitação de tráfego de entrada - Congestionamento da rede

4. Problema de configuração em termos de DSCP/QOS e assim por diante

5. Inexistência de assinantes/sessões na ligação EGTPC

Registros necessários

1. SSD/syslogs em torno de hora problemática cobrindo o período de tempo pelo menos duas

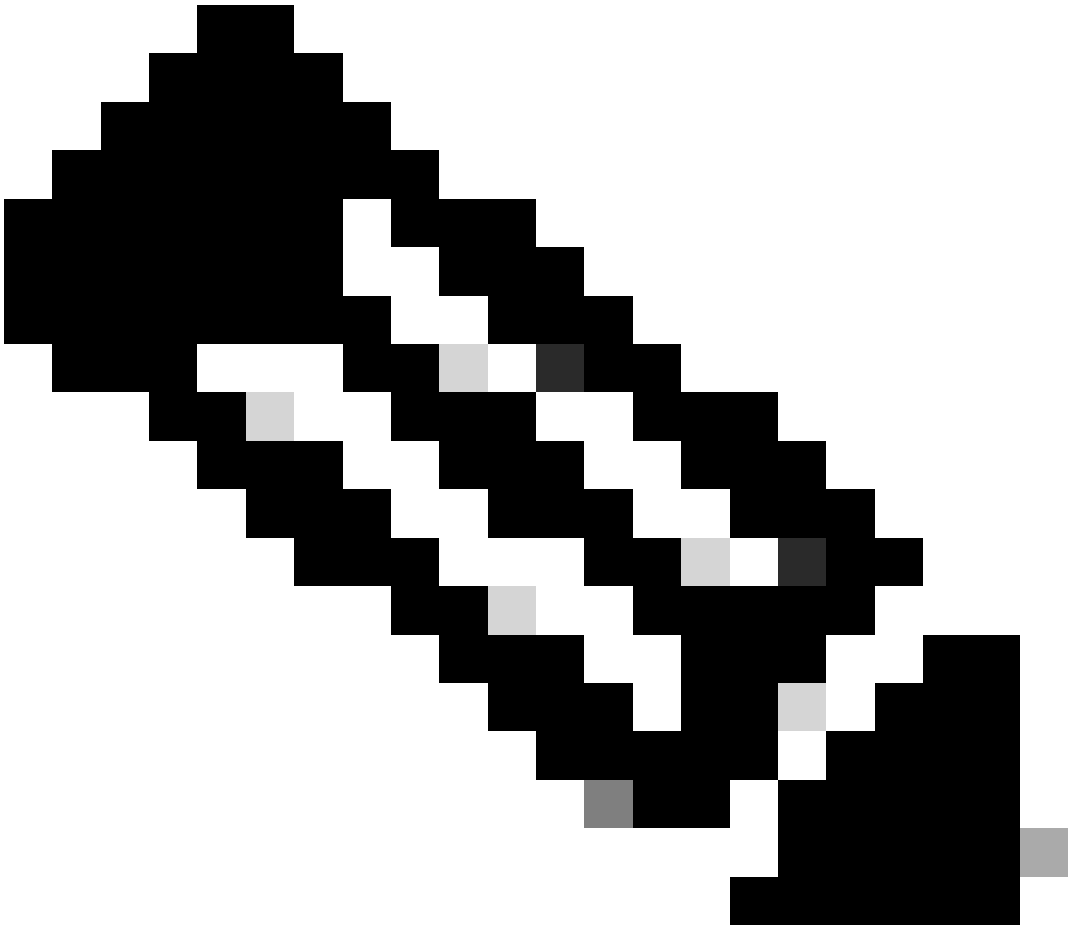
horas antes do início do problema até a hora atual.

2. Confirmação de acessibilidade com logs, ou seja, ping e traceroute para o caminho para o qual são vistas falhas de caminho.

3. Verificação da configuração entre nós problemáticos e não problemáticos.

4. Necessidade de confirmar se houve aumento repentino no tráfego ou aumento na rejeição no mesmo caminho.

5. Bulkstats durante períodos problemáticos cobrindo o período de tempo pelo menos 2-3 dias antes da emissão.



> Observação: dependendo do tipo de problema, os logs mencionados anteriormente podem ser necessários. Nem todos os logs são necessários a cada vez.

Comandos para Troubleshooting

<#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

Armadilhas de 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
```

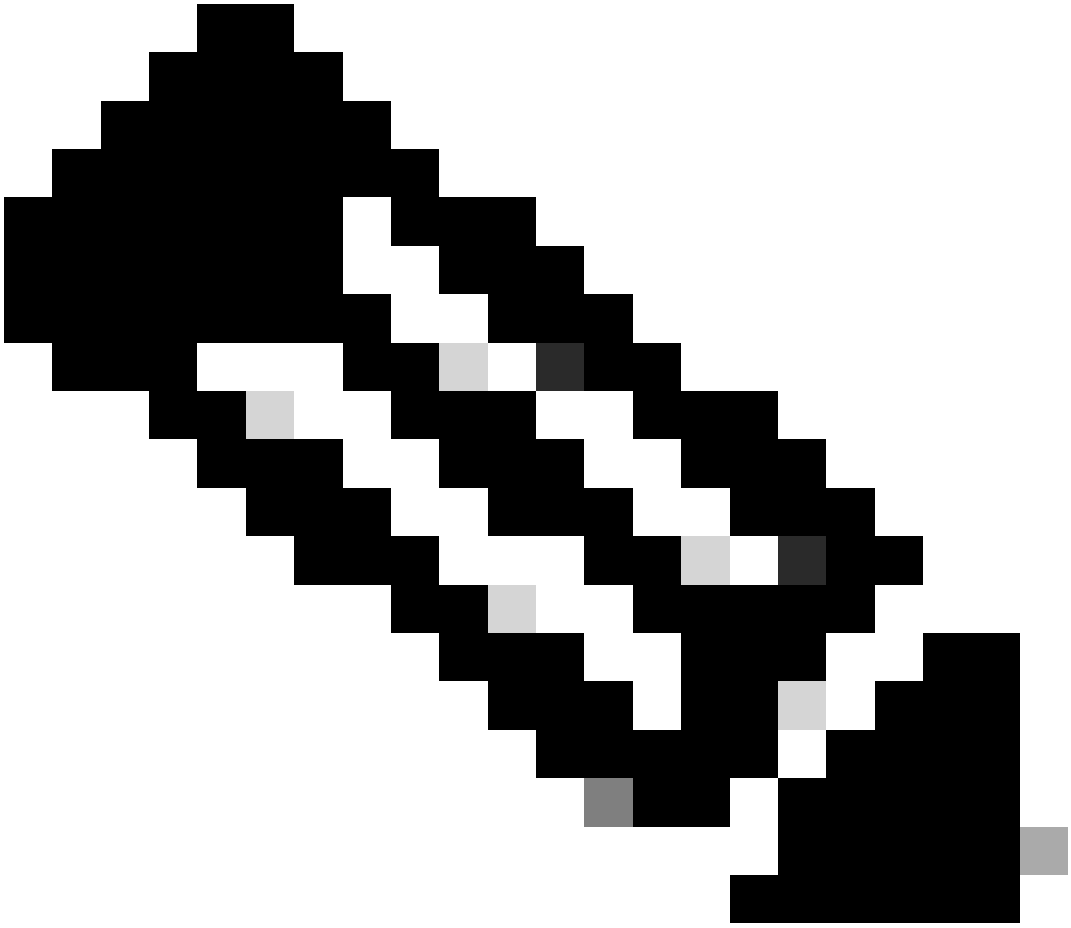
Cenário/Motivos resumidos

Problema de acessibilidade - Problemas de conectividade de rede

Problemas de acessibilidade ocorrem quando um problema no caminho da rota pode estar na extremidade do roteador ou no firewall entre SGSN/MME e SPGW/GGSN.

```
ping <destination IP>

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



> Observação: ambos os comandos para verificar a acessibilidade devem ser verificados no conteúdo em que o serviço EGTP está sendo executado.

Reiniciar Alterações de Valores do Contador

O caminho EGTP mantém os contadores de reinicialização em ambas as extremidades do caminho entre SGSN/MME e GGSN/SPGW.

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

ASR-5000-Series-Troubleshooting-GTPC-and.html para entender esse tipo de problema em detalhes.

Grande solicitação de tráfego de entrada - congestionamento de rede

Sempre que houver transações de alto tráfego repentinas, há uma chance de descarte de pacotes EGTP Tx e Rx. Verificações básicas para confirmar este cenário:

1. Você deve verificar se há alguma utilização alta de 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. Verifique se a solicitação/resposta de eco está falhando (comando compartilhado anteriormente).

3. Pode verificar se há algum descarte de pacote da placa demux.

Todo o tráfego de entrada EGTP deve passar pelo mesmo egtpmgr. Se forem observadas falhas de caminho com um nó, o volume de tráfego de entrada provavelmente aumentará. E você pode observar uma queda de tráfego no nível do processo do egtpmgr. Mesmo o processo co-localizado deve prosseguir pela mesma fila do egtpmgr e ser afetado.

Esta é a etapa para verificar a perda de pacotes que deve ser realizada com várias iterações

<#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. Deve capturar a saída do criador de perfil de CPU egtpinmgr se você vir uma CPU alta para egtpinmgr.

Se todas as condições acima forem válidas, você poderá verificar a possível solução mencionada.

Solução

1. Aumento no tempo limite de eco EGTP - Se 5 segundos não ajudar, você pode tentar 15 ou 25. Você pode discutir isso com sua equipe de AS para ajustar isso.

2. Diminuir o timeout de salvação do peer - Quanto menor o valor do timeout, menor o número de peers inativos, portanto, você pode alterar o valor do tempo com este comando:

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

3. proteção contra sobrecarga - a otimização da proteção contra sobrecarga pode ser feita com base na tendência de tráfego porque, sem saber a taxa exata de tráfego de entrada antes que o egpinmgr atinja o problema, é difícil ajustar isso. Além disso, o ajuste incorreto pode causar tráfego de sinalização adicional devido a quedas silenciosas.

Assim, para a otimização da proteção contra sobrecarga, você pode coletar algumas quedas de pacotes da placa demux para as saídas do egtpinmgr e do criador de perfil da CPU, conforme mencionado anteriormente.

4. Sem assinantes/sessões no link EGTPC - quando não há sessões em um túnel específico, a funcionalidade de eco GTP é interrompida. Se houver zero/nenhum assinante conectado, o eco GTPC não deverá ser enviado.

Estes são os erros que você vê quando a funcionalidade de eco é interrompida:

```
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
```

Solução

Você pode tentar reiniciar a tarefa egtpinmgr para se recuperar. Entretanto, reiniciar o egtpinmgr pode causar um impacto de curto prazo, não perceptível para o usuário final, enquanto os fluxos de NPU são reinstalados na nova tarefa.

Esta operação deve levar menos de 1 segundo para ser concluída.

1. Desative a detecção de falha de caminho:

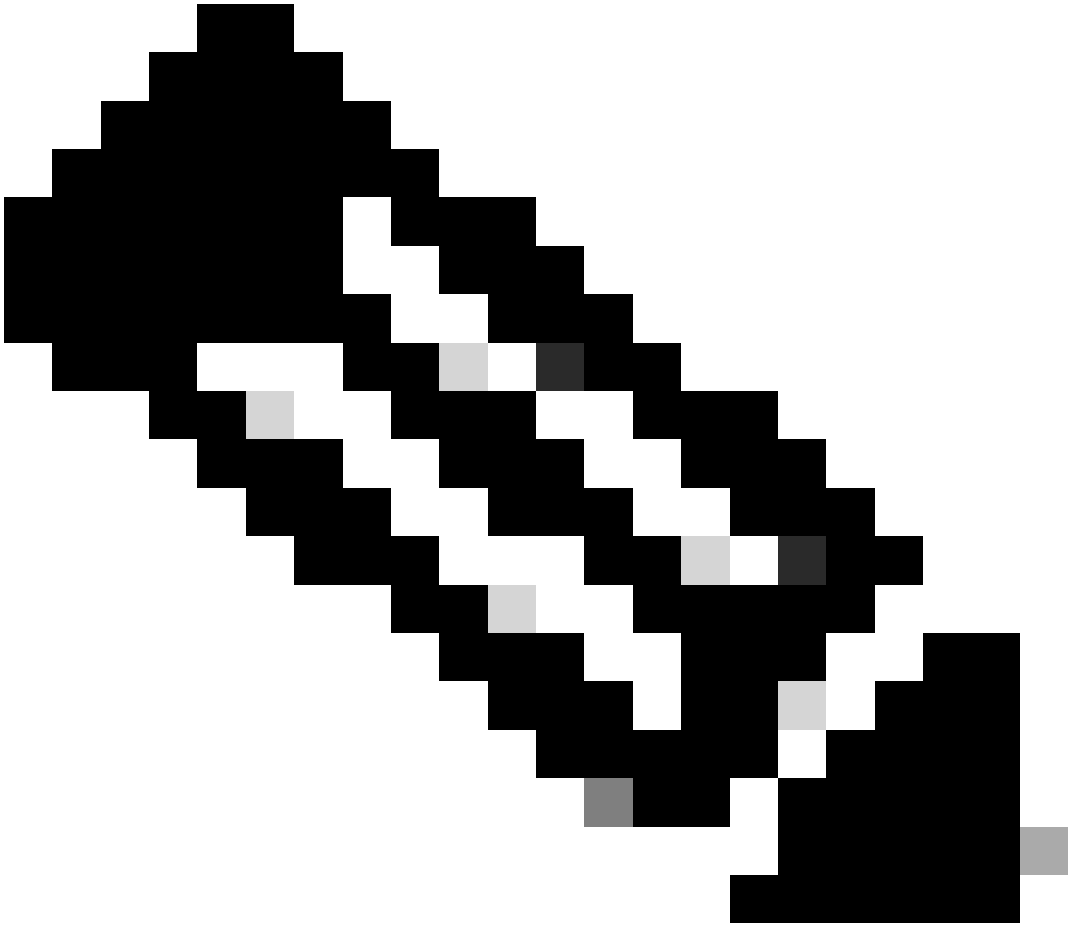
```
egtp-service S5-PGW
   no gtpc path-failure detection-policy
```

2. Eliminar tarefa egtpinmgr:

```
task kill facility egtpinmgr  all
```

3. Ative a detecção de falha de caminho:

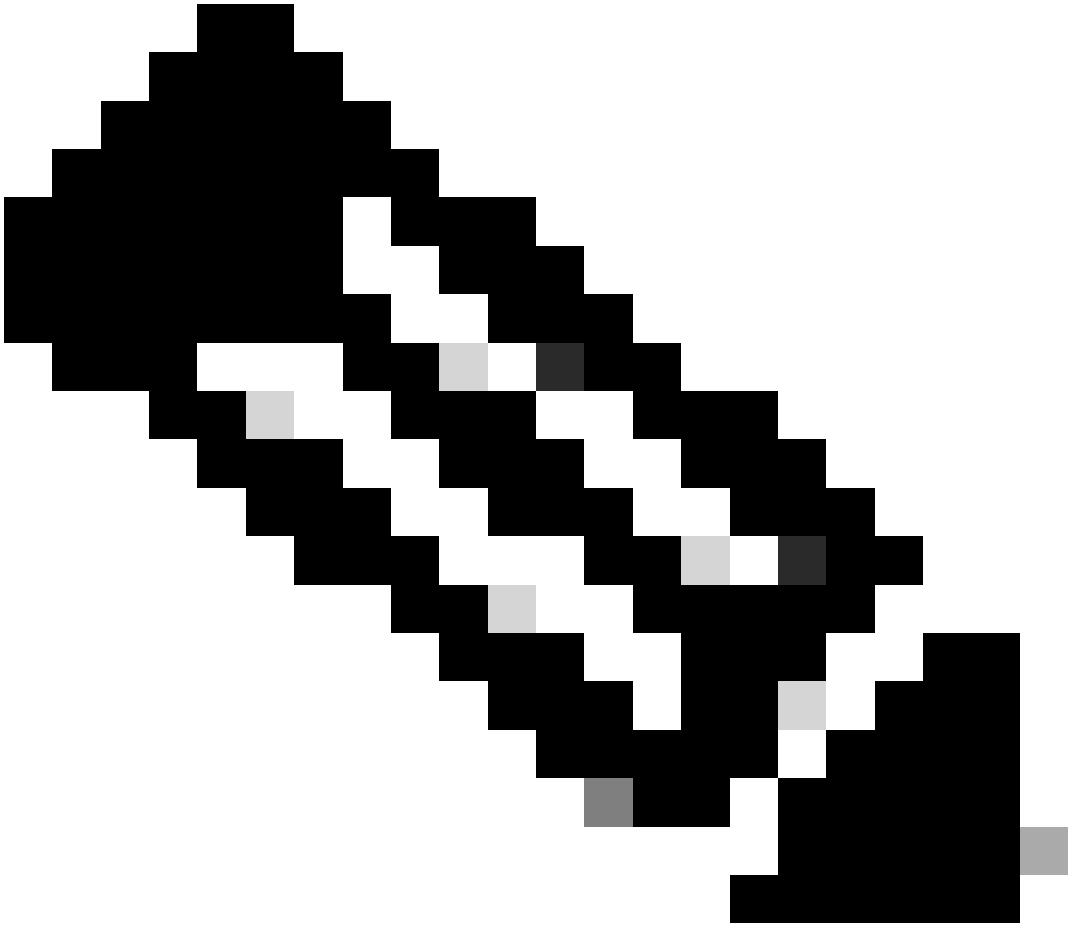
```
egtp-service S5-PGW
   gtpc path-failure detection-policy
```



Observação: essa solução alternativa deve ser implementada apenas em MW, pois pode causar algum impacto.

Alterações de configuração

É possível verificar a configuração em termos de mapeamento de caminho/serviço DSCP/QOS/EGTP IP.



Observação: essas são as principais razões que contribuem para falhas de caminho EGTP, mas caso nenhum dos cenários seja encontrado, você poderá coletar mais alguns rastreamentos e logs de depuração.

Logs de depuração

(Se necessário)

```
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>
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.