

Solucionar problemas de navegação de dados do usuário para URLs da Web específicos

Contents

[Introdução](#)

[Pré-requisitos](#)

[Identificação dos sintomas](#)

[Coleta/teste de registros](#)

[Troubleshooting Executado](#)

[Quedas de pacotes](#)

Introdução

Este documento descreve os problemas de navegação de dados do usuário na rede 4G para todos os URLs (Uniform Resource Locators).

Pré-requisitos

A Cisco recomenda que você tenha conhecimento das funcionalidades desses nós:

- Serving Packet Data Gateway (SPGW)
- Controle e separação de plano de usuário (CUPS)

Identificação dos sintomas



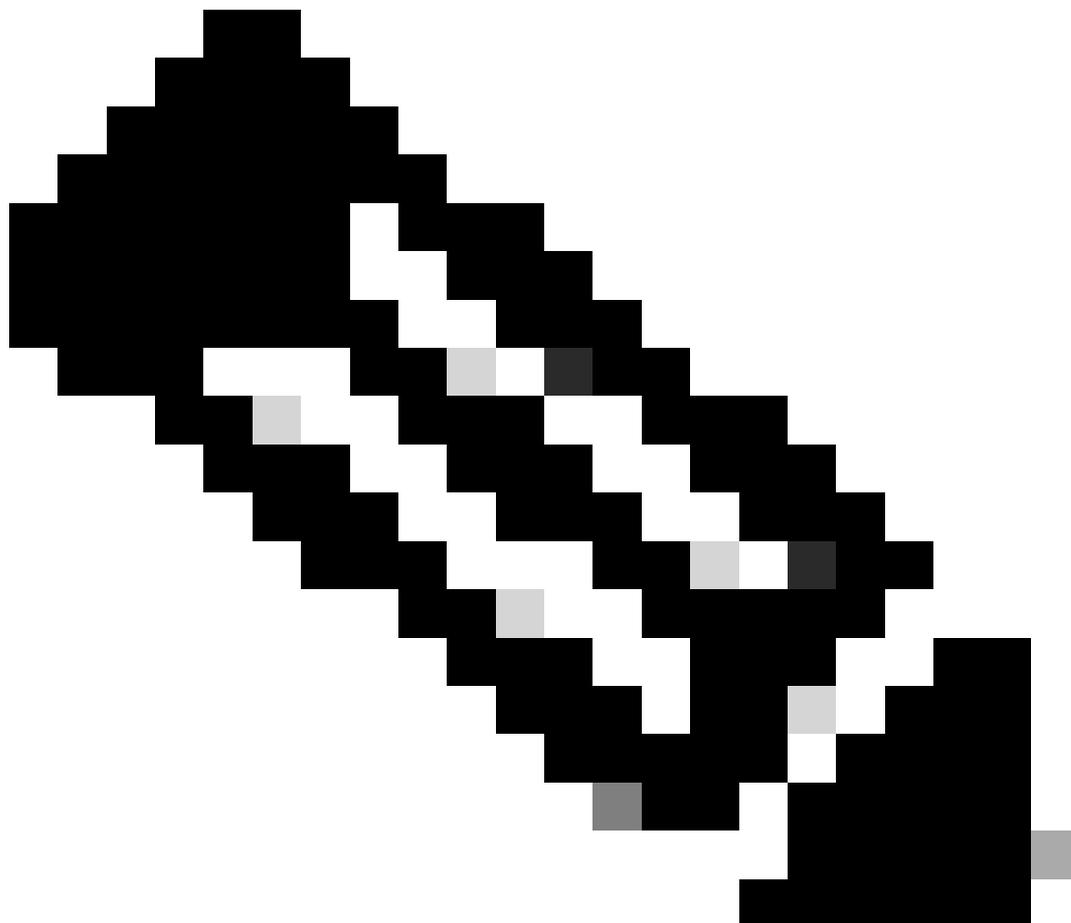
Observação: antes de iniciar o teste e a coleta de logs, você deve verificar esses detalhes.

-
1. Verifique qual tipo de dados é o problema: IPv4/IPv6/IPv4v6
 2. Verifique se o problema está relacionado a algum nome de ponto de acesso (APN) específico ou a todos os APNs, pois o problema pode estar relacionado a um APN específico.
 3. Verifique se o problema se refere a URLs da Web específicos ou a várias URLs.
 4. Verifique se o URL é um URL de aplicativo do cliente/URL da empresa ou algum URL de serviço regular e também verifique se o problema está em uma VPN específica.
 5. Verifique se o problema ocorre ao acessar o URL diretamente do navegador ou ao acessar o próprio aplicativo Web.
 6. Verifique se o problema é intermitente por natureza, como a reinicialização do monofone ou a atualização de URLs da Web começam a funcionar, ou se o problema é consistente e não

funciona mesmo após a reinicialização do monofone.

7. Verifique a causa da rejeição observada e para qual grupo de classificação.

Coleta/teste de registros



Observação: para esse tipo de problema, você deve executar a solução de problemas on-line em tempo real com o usuário problemático IMSI, no qual deve coletar os registros/rastreamentos de acordo.

Antes de prosseguir com o teste e a coleta de logs:

Flush the subscriber from the node and also clear browsing history/database from testing user handset s
clear subscriber imsi <IMSI number> ----- to be executed in the node to clear the subscri

1. Comece com o teste com um tipo de PDP primeiro, como o IPv4, onde você vê o problema.
2. Ative esses logs de depuração e registre a sessão putty. Verifique se a sessão não deve ser encerrada (pressione Tab/insira a cada alguns minutos para que a sessão não seja encerrada).

<#root>

On SPGW:

```
logging filter active facility sessmgr level debug
logging filter active facility acsmgr level debug
logging filter active facility npumgr-acl level debug
logging filter active facility firewall level debug
logging filter active facility vpn level debug
logging filter active facility vpnmgr level debug
logging active ----- to enable the logging
```

after 5 mins

```
no logging active ----- to disable the logging
```

On CP:

```
logging filter active facility sessmgr level debug
logging filter active facility sxdemux level debug
logging filter active facility firewall level debug
logging filter active facility vpn level debug
logging filter active facility vpnmgr level debug
logging active ----- to enable the logging
```

after 5 mins

```
no logging active ----- to disable the logging
```

On UP:

```
logging filter active facility sessmgr level debug
logging filter active facility sxdemux level debug
logging filter active facility npumgr-acl level debug
logging filter active facility firewall level debug
logging filter active facility vpn level debug
logging filter active facility vpnmgr level debug
logging active ----- to enable the logging
no logging active ----- to disable the logging
```

Note :: These logging has to be enabled for short time depending on the CPU utilization because it increase the utilization so while enabling logging need to keep a watch on CPU

3. Navegue até o modo de configuração e ative o monitor de registro para o assinante.

```
config
logging monitor msid <imsi>
end
```

4. Abra outro terminal, registre a sessão putty, e comece a monitorar o assinante com verbosidade 5 e ative estas opções:

```
<#root>
```

```
SPGW:
```

```
Press + for times then it collects the logs verbosity 5 logs then select next options
+++++
X, A, Y, 19, 33, 34, 35, 22, 26, 75
Once option 75 is pressed then select 3,4,8 then press esc
```

```
CUPS::
```

```
on CP:
```

```
monitor subscriber imsi <IMSI> +++++ S, X,A,Y,56,26,33,34,19,37,35,88,89
```

```
on UP:
```

```
monitor subscriber imsi <IMSI> +++++ S,X,A,Y,56,26,33,34,19,37,35,88,89
```

5. Anexe o assinante e navegue o URL continuamente por 3 a 5 minutos e, durante a navegação, execute esses comandos várias vezes e registre a sessão putty para o mesmo.

```
<#root>
```

```
ON SPGW/SAEGW:
```

```
show subscriber full imsi <>
show active-charging session full imsi <>
show subscriber pgw-only full imsi <>
show subscriber sgw-only full imsi <>
show subscribers data-rate summary imsi <>
show ims-authorization sessions full imsi <>
show subscribers debug-info msid <>
```

```
On CP node:
```

```
Show subscriber full imsi <imsi>
```

```
Show active-charging session full imsi <imsi>
show subscribers pgw-only full imsi <>
show subscribers sgw-only full imsi <>
show session subsystem facility sessmgr instance <> verbose
show logs
```

On UP node:

```
show sub user-plane-only full callid <>
show sub user-plane-only callid <> urr full all
show sub user-plane-only callid <> far full all
show sub user-plane-only callid <> pdr full all
show subscribers user-plane-only callid <> far all
show subscribers user-plane-only callid <> far
show subs data-rate call <callid>
show subscribers user-plane-only flows
show user-plane-service statistics all
show user-plane-service statistic rulebase name <rulebase_name>
```

6. Após 5 minutos de navegação, execute o `no logging active` no outro terminal que está aberto na Etapa 3.

7. Desative o monitor de log para o assinante.

```
Config
no logging monitor msid <imsi>
end
```

8. Não pare o `mon sub` e deixe-o rodar até que você termine de coletar rastros de números, mas fique de olho na CPU.

9. Execute este comando para obter o identificador de chamada do assinante e registre a sessão putty para isso também.

```
Show subscriber full imsi <imsi>. -à get the call id
show logs callid <call_id>
show logs
```

Se o ID do chamador estiver presente, ficará claro que os logs da sessão do assinante foram coletados; caso contrário, será necessário executá-lo novamente.

Troubleshooting Executado

- Faça ping no endereço IP do servidor de URL da Web e verifique se há descartes de pacotes.

ping <URL IP address> ----- from Gi context

--- ping statistics ---

3 packets transmitted, 0 received, 100% packet loss, time 12160ms. >.>>>> There are packet drops, now we need to check were it is dropping

2. Realize uma avaliação traceroute a partir do contexto da IG e verifique se há problemas de acessibilidade.

traceroute <peer ip address> src <local diameter origin host ip address>

Ex: traceroute 10.52.5.49 src 10.203.144.8

3. Verifique as estatísticas do assinante para verificar as quedas de pacotes.

<#root>

Show subscriber full imsi <imsi number>

```
input pkts: 455 output pkts: 474
input bytes: 75227 output bytes: 103267
input bytes dropped: 0 output bytes dropped: 0
input pkts dropped: 0 output pkts dropped: 0
input pkts dropped due to lorc : 0 output pkts dropped due to lorc : 0
input bytes dropped due to lorc : 0
in packet dropped suspended state: 0 out packet dropped suspended state: 0
in bytes dropped suspended state: 0 out bytes dropped suspended state: 0
in packet dropped sgw restoration state: 0 out packet dropped sgw restoration state: 0
in bytes dropped sgw restoration state: 0 out bytes dropped sgw restoration state: 0
pk rate from user(bps): 18547 pk rate to user(bps): 25330
ave rate from user(bps): 6182 ave rate to user(bps): 8443
sust rate from user(bps): 5687 sust rate to user(bps): 7768
pk rate from user(pps): 13 pk rate to user(pps): 14
ave rate from user(pps): 4 ave rate to user(pps): 4
sust rate from user(pps): 4 sust rate to user(pps): 4
link online/active percent: 92
ipv4 bad hdr: 0 ipv4 ttl exceeded: 0
ipv4 fragments sent: 0 ipv4 could not fragment: 0
ipv4 input acl drop: 0 ipv4 output acl drop: 0
ipv4 bad length trim: 0
ipv6 input acl drop: 0 ipv6 output acl drop: 0
ipv4 input css down drop: 0 ipv4 output css down drop: 0
ipv4 input css down drop: 0 ipv4 output css down drop: 0
ipv4 output xoff pkts drop: 0 ipv4 output xoff bytes drop: 0
ipv6 output xoff pkts drop: 0 ipv6 output xoff bytes drop: 0
ipv6 input ehrpd-access drop: 0 ipv6 output ehrpd-access drop: 0
input pkts dropped (0 mbr): 0 output pkts dropped (0 mbr): 0
ip source violations: 0 ipv4 output no-flow drop: 0
ipv6 egress filtered: 0
ipv4 proxy-dns redirect: 0 ipv4 proxy-dns pass-thru: 0
ipv4 proxy-dns drop: 0
ipv4 proxy-dns redirect tcp connection: 0
ipv6 bad hdr: 0 ipv6 bad length trim: 0
```

```
ip source violations no acct: 0
ip source violations ignored: 0
dormancy total: 0 handoff total: 0
ipv4 icmp packets dropped: 0
APN AMBR Input Pkts Drop: 0 APN AMBR Output Pkts Drop: 0
APN AMBR Input Bytes Drop: 0 APN AMBR Output Bytes Drop: 0
APN AMBR UE Overload Input Pkts Drop: 0 APN AMBR UE Overload Output Pkts Drop: 0
APN AMBR UE Overload Input Bytes Drop: 0 APN AMBR UE Overload Output Bytes Drop: 0
Access-flows:0
Num Auxiliary A10s:0
```

4. Verifique a saída do comando show active charge para o impacto do tráfego do assinante.

```
Show active-charging session full imsi <imsi num>
```

```
PP Dropped Packets: 0
CC Dropped Uplink Packets: 0 CC Dropped Uplink Bytes: 0
CC Dropped Downlink Packets: 0 CC Dropped Downlink Bytes: 0
```

5. Verifique a saída do comando show active charge para a queda de pacotes no nível ECS/ACS e verifique se há alguma queda de pacotes. Em seguida, verifique na configuração qual ação está configurada.

```
<#root>
```

```
Show active-charging session full imsi <imsi num> or show sub user-plane-only full callid <>
```

```
Ruledef Name Pkts-Down Bytes-Down Pkts-Up Bytes-Up Hits Match-Bypassed
```

```
-----
dns_free_covid 4 428 4 340 8 0
icmpv6 0 0 5 1423 5 0
ip-pkts 479 103670 432 74488 764 429
```

6. Verifique se a resolução DNS foi bem-sucedida ou não. Se for bem-sucedido, não há nenhum problema com o DNS.

10.60.150.135	GTP <DNS>	Standard query response 0x3a4c AAAA tracking.india.miui.com CNAME tracking-india-miui-com-1-77
42.105.241.29	GTP <DNS>	Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29	GTP <DNS>	Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29	GTP <DNS>	Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29	DNS	Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29	DNS	Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29	GTP <DNS>	Standard query 0x63bb A www.shcilestamp.com
42.105.241.29	GTP <DNS>	Standard query 0x63bb A www.shcilestamp.com
42.105.241.29	GTP <DNS>	Standard query 0x63bb A www.shcilestamp.com
42.105.241.29	DNS	Standard query 0x63bb A www.shcilestamp.com
42.105.241.29	DNS	Standard query 0x63bb A www.shcilestamp.com
42.105.241.29	DNS	Standard query 0x63bb A www.shcilestamp.com
10.60.150.135	DNS	Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135	DNS	Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135	DNS	Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135	GTP <DNS>	Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135	GTP <DNS>	Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135	GTP <DNS>	Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135	DNS	Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15
10.60.150.135	DNS	Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15
10.60.150.135	DNS	Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15
10.60.150.135	GTP <DNS>	Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15
10.60.150.135	GTP <DNS>	Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15

7. Verifique se a conexão TCP foi estabelecida com êxito entre o equipamento do usuário (UE) e o servidor.

8. Se nenhum descarte for observado em qualquer uma dessas etapas, não haverá nenhum problema no nó.

Quedas de pacotes

1. Verifique as estatísticas de liberação do assinante para determinar se você está enfrentando quedas de pacotes semelhantes às mostradas aqui.

Total Dropped Packets : 132329995

Total Dropped Packet Bytes: 14250717212

Total PP Dropped Packets : 0

Total PP Dropped Packet Bytes: 0

R7Gx Rule-Matching Failure Stats:

Total Dropped Packets : 871921

Total Dropped Packet Bytes : 86859232

P2P random drop stats:

Total Dropped Packets : 0

Total Dropped Packet Bytes : 0

2. Verifique o percentual de falhas observadas na saída do comando show subscriber. Se as quedas de pacotes forem menores que 1%, é mais provável que seja um acaso e não tenha efeito.

input pkts: 455 output pkts: 474

input bytes: 75227 output bytes: 103267

input bytes dropped: 0 output bytes dropped: 0

input pkts dropped: 0 output pkts dropped: 0

3. Se você perceber quedas de pacotes no grupo de classificação RX e quedas de pacotes ITC, isso provavelmente ocorre devido a um problema de largura de banda e o pacote do assinante expirou.

4. No nível do Serviço de Cobrança Avançada (ECS), você deve verificar/verificar a configuração do ECS de como as ações/bases de regras de cobrança são definidas e se você tem algum fator de bloqueio. Há diferentes tipos de descartes no nível do ECS e, com base no tipo de descarte, você precisa prosseguir com o próximo plano de ação.

5. Tamanho da MTU para o tamanho do pacote que está passando e não processado.

6. Os problemas de caminho intermediário em que o pacote está sendo descartado podem ser identificados a partir de despejo TCP/rastreamentos em nível de usuário.

O plano de ação de recuperação não é o mesmo para esse tipo de problema, pois varia de acordo com o padrão do problema.

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.