

Dépannage du problème de navigation des données utilisateur pour des URL Web spécifiques

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Identification des symptômes](#)

[Collecte/test des journaux](#)

[Dépannage effectué](#)

[Abandons de paquets](#)

Introduction

Ce document décrit les problèmes de navigation des données utilisateur sur le réseau 4G pour toutes les URL (Uniform Resource Locator).

Conditions préalables

Cisco vous recommande de connaître les fonctionnalités de ces noeuds :

- Passerelle de données de paquets de service (SPGW)
- Contrôle et séparation du plan utilisateur (CUPS)

Identification des symptômes



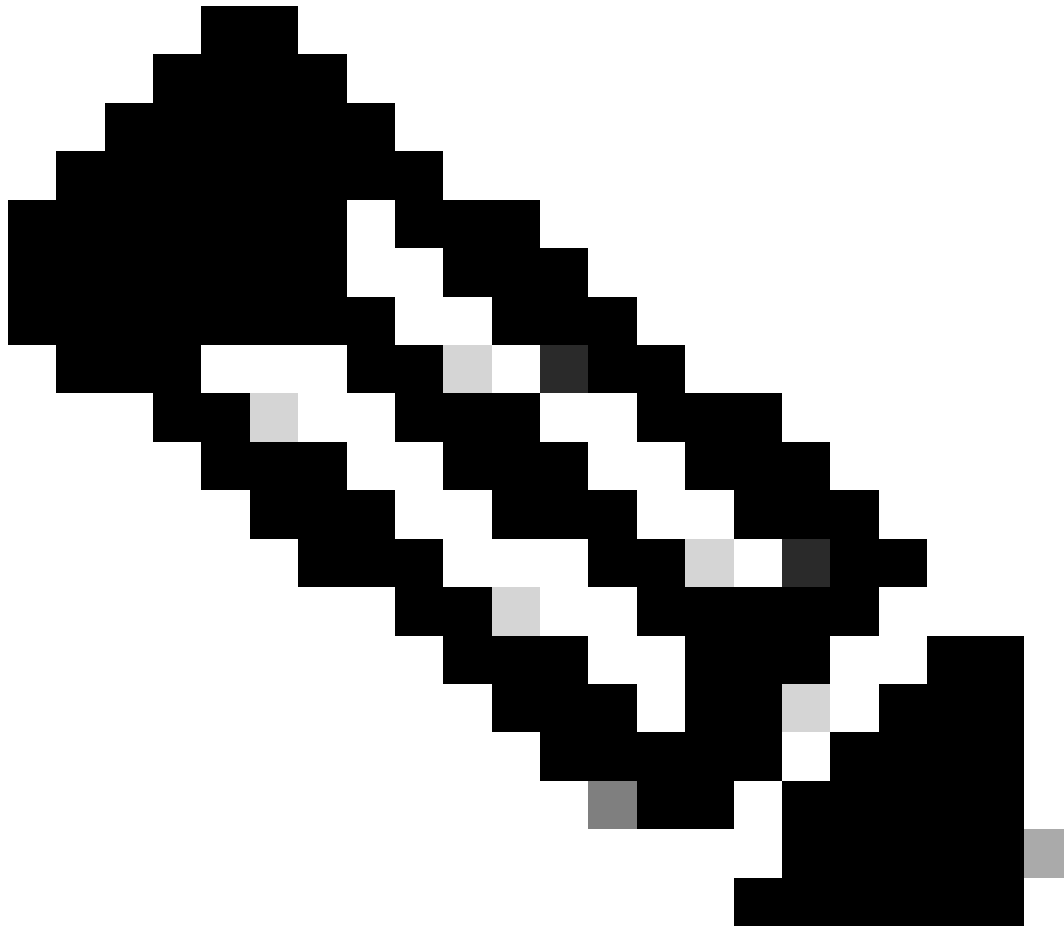
Remarque : avant de commencer les tests et la collecte des journaux, vous devez vérifier ces détails.

-
1. Vérifiez quel type de données pose problème : IPv4/IPv6/IPv4v6
 2. Vérifiez si le problème est lié à un nom de point d'accès (APN) particulier ou à tous les APN, car le problème peut être lié à un APN spécifique.
 3. Vérifiez si le problème concerne des URL Web spécifiques ou plusieurs URL.
 4. Vérifiez si l'URL est une URL d'entreprise/URL d'application client ou une URL de service standard et vérifiez également si le problème provient d'un VPN spécifique.
 5. Vérifiez si le problème se produit lors de l'accès à l'URL directement à partir du navigateur ou lors de l'accès à l'application Web elle-même.
 6. Vérifiez si le problème est de nature intermittente, par exemple après le redémarrage du combiné ou si l'actualisation des URL Web commence à fonctionner ou si le problème est

cohérent et ne fonctionne pas même après le redémarrage du combiné.

7. Vérifiez la cause de rejet observée et pour quel groupe de notation.

Collecte/test des journaux



Remarque : pour ce type de problème, vous devez effectuer un dépannage en ligne en temps réel avec l'IMSI de l'utilisateur problématique sur lequel vous devez collecter des journaux/traces en conséquence.

Avant de procéder au test et à la collecte des journaux :

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. Commencez par le test avec un type de protocole PDP comme IPv4, où vous voyez le problème.
2. Activez ces journaux de débogage et consignez la session putty. Assurez-vous que la session ne doit pas se terminer (appuyez sur la touche Tab/Entrée toutes les quelques minutes pour que la session ne se termine pas).

<#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 vpmgr 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 vpmgr 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 vpmgr 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. Passez en mode de configuration, puis activez le moniteur de journalisation pour l'abonné.

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

4. Ouvrez un autre terminal, enregistrez la session putty et commencez à surveiller l'abonné avec verbosity 5 et activez ces options :

```
<#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. Joignez l'abonné et parcourez l'URL en continu pendant 3 à 5 minutes et tout en parcourant exécuter ces commandes plusieurs fois et consigner la session mastic pour le même.

```
<#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. Après 5 minutes de navigation, exécutez le `no logging active` dans l'autre terminal qui est ouvert à l'étape 3.

7. Désactivez le moniteur de journalisation pour l'abonné.

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

8. N'arrêtez pas le sous-réseau mon et laissez-le fonctionner jusqu'à ce que vous ayez fini de collecter les traces de numéros, mais gardez un oeil sur le processeur.

9. Exécutez cette commande afin d'obtenir l'id appelant de l'abonné et de consigner la session putty pour cela aussi.

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

Si l'ID de l'appelant est présent, il est clair que les journaux de session de l'abonné ont été collectés. Sinon, vous devez le réexécuter.

Dépannage effectué

- Envoyez une requête ping à l'adresse IP du serveur d'URL Web et vérifiez s'il y a des abandons de paquets.

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. Effectuez une analysetraceroute à partir du contexte GI et vérifiez si des problèmes d'accessibilité se produisent.

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

Ex: traceroute 10.52.5.49 src 10.203.144.8

3. Vérifiez les statistiques de l'abonné afin de vérifier les abandons de paquets.

<#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. Vérifiez l'impact du trafic de l'abonné dans la sortie show active charge.

```
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. Vérifiez le résultat de la commande show active chargement pour la suppression de paquets de niveau ECS/ACS et vérifiez s'il y a des pertes de paquets. Vérifiez ensuite dans la configuration l'action configurée.

```
<#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. Vérifiez si la résolution DNS a réussi ou non. Si elle réussit, alors il n'y a aucun problème avec 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	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. Vérifiez que la connexion TCP est correctement établie entre l'équipement utilisateur (UE) et le serveur.

8. Si aucune baisse n'est observée au cours de l'une de ces étapes, le noeud ne présente aucun problème.

Abandons de paquets

1. Vérifiez les statistiques de libération de l'abonné afin de déterminer si vous rencontrez des pertes de paquets similaires à celles indiquées ici.

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. Vérifiez le pourcentage d'échecs observés dans le résultat de la commande show subscriber. Si les pertes de paquets sont inférieures à 1 %, il s'agit très probablement d'un coup de chance et n'a aucun effet.

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. Si vous remarquez des pertes de paquets dans le groupe de classification RX et des pertes de paquets ITC, cela est probablement dû à un problème de bande passante et à l'expiration du package de l'abonné.

ITC Packets Drop:

47235019

4. Au niveau du service de facturation améliorée (ECS), vous devez vérifier la configuration ECS de la manière dont les règles/l'action de facturation/la base de règles sont définies et si vous avez un facteur de blocage. Il existe différents types de chutes au niveau ECS et en fonction du type de chute dont vous avez besoin pour poursuivre le plan d'action suivant.

5. Taille de MTU pour la taille de paquet qui est en cours de transmission et non traitée.

6. Les problèmes de chemin intermédiaire où le paquet est abandonné peuvent être identifiés à partir des traces TCP dump/user-level.

Le plan d'action pour le rétablissement n'est pas le même pour ce type de problème, car il varie selon la tendance du problème.

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.