Dépannage des problèmes de navigation des utilisateurs dans LTE

Table des matières

Introduction

Ce document décrit les problèmes de navigation des données utilisateur sur le réseau 4G.

Conditions préalables

Cisco vous recommande de connaître les fonctionnalités de ces noeuds

1. Passerelle de données de paquets de service (SPGW)

2. Contrôle et séparation du plan utilisateur (CUPS)

Symptômes

Avant de commencer le test et la collecte des journaux, vous devez vérifier les détails mentionnés ci-dessous :

1. Le problème de vérification concerne le type de données PDN (Packet Data Network) : IPv4/IPv6/IPv4v6

2. Vérifiez que le problème est lié à un nom de point d'accès (APN) particulier ou à tous les APN, car le problème peut également être lié à des APN spécifiques.

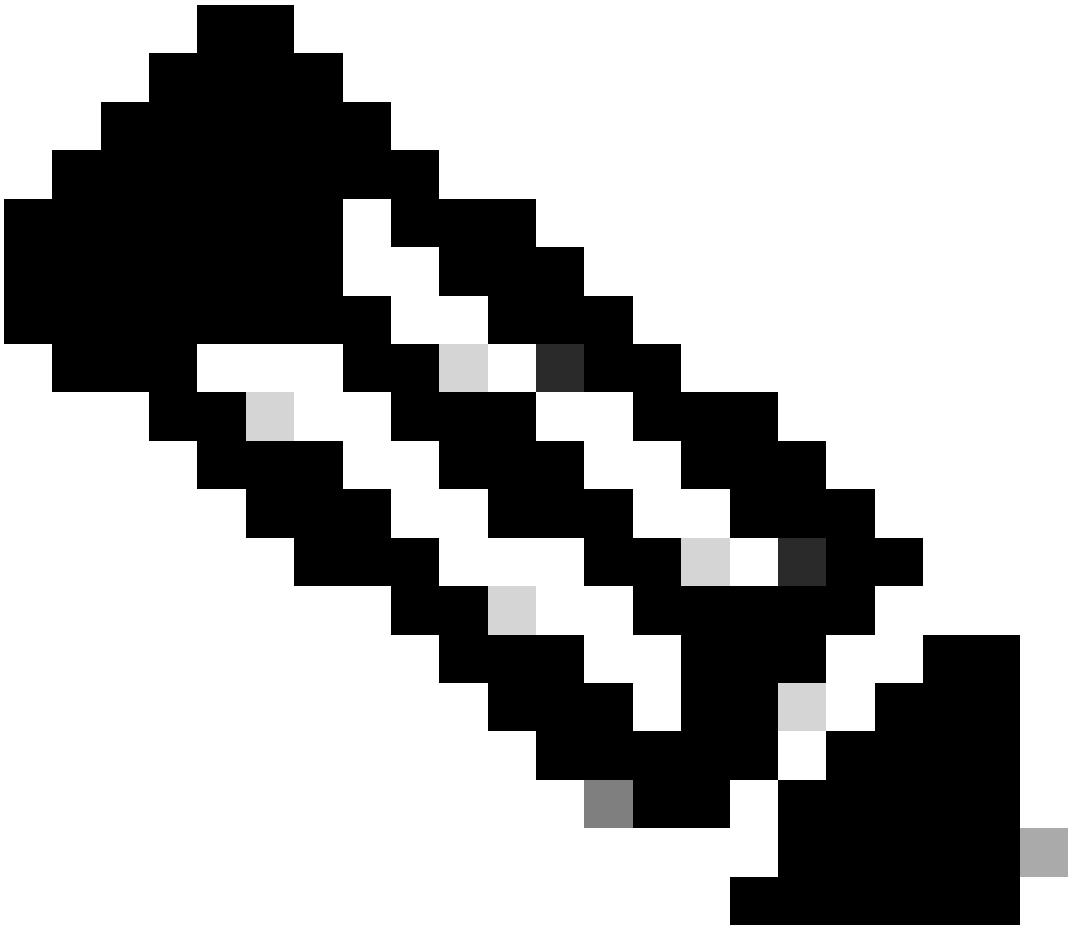
3. Vérifiez si l'URL est une URL d'entreprise/d'application client ou une URL de service standard et, par conséquent, si le problème concerne un VPN spécifique.

4. 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.

5. Le problème est-il de nature intermittente, par exemple après le redémarrage du combiné/l'actualisation des URL Web, ou le problème est-il constant et ne fonctionne-t-il pas même après le redémarrage du combiné ?

6. Cochez la cause de rejet observée et pour quel groupe d'évaluation.

Collecte/test des journaux



> Remarque : pour ce type de problèmes, vous devez effectuer un dépannage en ligne en temps réel avec l'utilisateur problématique IMSI 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 tester l'abonné avec n'importe quel type de PDN.

2. Consignez la session mastic et démarrez l'abonné de surveillance avec verbosity 5 et activez cette option.

<#root>

SPGW:

```
Press + for times then it collects the logs verbosity 5 logs then select next options
+++++
S,X,A,Y,56,26,33,34,19,37,35,88,89
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
```

3. Activez ces journaux de débogage et consignez la session putty et assurez-vous que la session ne doit pas être interrompue (appuyez sur tab/enter 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 vpnmgr level debug
logging active   ---------------- to enable the logging
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
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
```

4. Configurez le mode, veuillez activer le moniteur de journalisation pour l'abonné

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

5. Joignez l'Abonné et parcourez l'URL en continu pendant 3 à 5 minutes et tout en parcourant exécuter cette commande plusieurs fois et enregistrer 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 no logging active dans le terminal qui est ouvert à l'étape 4

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

Config
no logging monitor msid <imsi>

8. Exécutez cette commande pour obtenir l'ID d'appel de l'abonné et consigner la session putty pour cela également.

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

9. Si l'ID d'appel est présent, il est clair que les journaux de session de l'abonné ont été collectés, sinon, il faut réexécuter.

Analyse

1. Vérifiez si la résolution DNS a réussi ou non. Si elle réussit, alors il n'y a aucun problème avec DNS.

Traces de résolution DNS

2. Vérifiez les statistiques au niveau de l'abonné pour examiner les abandons de paquets.

<#root>

SPGW/CP:
Show subscriber full imsi <imsi number>

CUPS UP:

show user-plane-only full imsi <>

```
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
```

3. 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, puis vérifiez dans la configuration quelle est 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
```

4. Vérifiez que la connexion TCP est correctement établie entre UE et le serveur.

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

Abandons de paquets

- Vérifiez les statistiques de libération de l'abonné pour 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 ECS, il est important de vérifier la configuration DPI, y compris la définition de la règle, l'action de facturation et la base de règles, afin de déterminer s'il existe des facteurs de blocage. Il existe différents types de pertes au niveau de l'ECS, et la suite à donner dépend du type spécifique de perte rencontré.

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.