Fehlerbehebung bei Problemen mit der Benutzersuche in LTE

Inhalt

Einleitung

Voraussetzungen

Symptome

Protokollerfassung/-tests

Analyse

Paketverlust

Einleitung

In diesem Dokument werden die Probleme beim Durchsuchen von Benutzerdaten im 4G-Netzwerk beschrieben.

Voraussetzungen

Cisco empfiehlt, dass Sie die Funktionen dieser Knoten kennen.

1. Serving Packet Data Gateway (SPGW)

2. Control and User Plane Separation (CUPS)

Symptome

Bevor Sie mit dem Testen und der Protokollerfassung beginnen, müssen Sie die folgenden Details überprüfen:

1. Überprüfen Sie, ob das Problem bei welchem PDN-Datentyp (Packet Data Network) auftritt: IPv4/IPv6/IPv4v6

2. Überprüfen Sie, ob das Problem bei einem bestimmten Access Point-Namen (APN) oder allen APNs vorliegt, da das Problem auch mit bestimmten APNs in Zusammenhang stehen kann.

3. Überprüfen Sie, ob es sich bei der URL um eine Unternehmens-URL bzw. eine Kunden-App-URL oder eine reguläre Service-URL handelt und ob das Problem bei einem bestimmten VPN liegt.

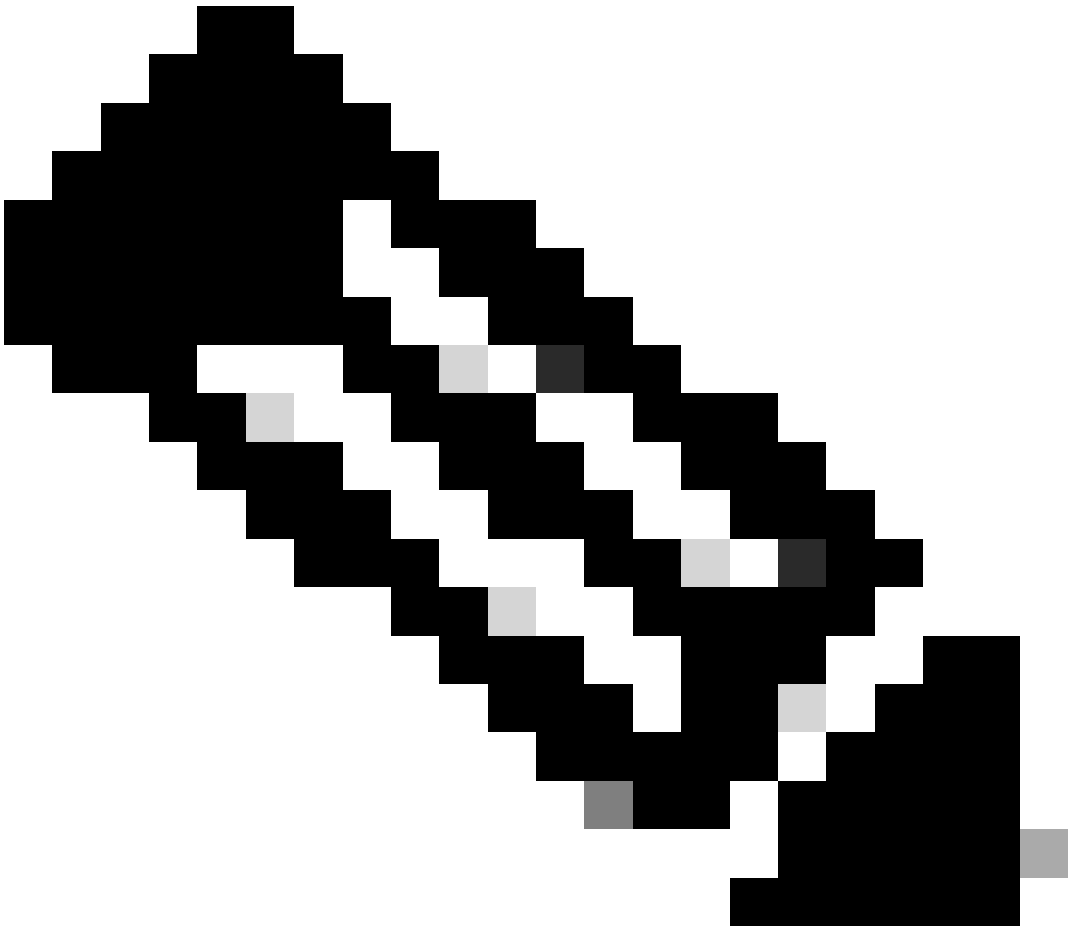
4. Überprüfen Sie, ob das Problem beim Zugriff auf die URL direkt vom Browser oder beim Zugriff auf die Web-App selbst auftritt.

5. Funktioniert das Problem nur gelegentlich, z. B. wenn die Web-URLs nach dem Neustart des

Hörers/der Aktualisierung wieder aktiviert werden, oder ist das Problem konsistent und funktioniert nicht einmal nach dem Neustart des Hörers?

6. Überprüfen Sie die beobachtete Ablehnungsursache und für welche Bewertungsgruppe.

Protokollerfassung/-tests



> Hinweis: Bei diesen Problemen müssen Sie eine Online-Fehlerbehebung in Echtzeit mit dem problematischen Benutzer IMSI durchführen, bei dem Sie die Protokolle/Ablaufverfolgungen entsprechend erfassen müssen.

Bevor Sie mit dem Testen und der Protokollsammlung fortfahren.

```
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. Beginnen Sie mit den Tests für den Teilnehmer mit einem beliebigen PDN-Typ.

2. Protokollieren Sie die Kitesession und starten Sie Monitor Subscriber mit Verbosity 5 und aktivieren Sie diese 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. Bitte aktivieren Sie diese Debug-Protokolle und protokollieren Sie die Kitt-Sitzung und stellen Sie sicher, dass die Sitzung nicht beendet werden darf (drücken Sie die Tabulatortaste/geben Sie alle paar Minuten ein, damit die Sitzung nicht beendet wird).

<#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. Konfigurieren Sie den Modus, aktivieren Sie den Protokollmonitor für den Abonnenten.

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

5. Fügen Sie den Abonnenten und durchsuchen Sie die URL kontinuierlich für 3 bis 5 Minuten und während des Durchsuchens führen Sie diesen Befehl mehrmals und protokollieren Sie die putty-Sitzung für die gleiche.

<#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>
```

no logging active 6. Nach 5 Minuten des Durchsuchens, führen Sie in dem Terminal aus, das bei Schritt 4 geöffnet wird

7. Deaktivieren Sie den Protokollmonitor für den Abonnenten.

Config
no logging monitor msid <imsi>

8. Führen Sie diesen Befehl aus, um die Anruf-ID des Teilnehmers abzurufen und die Putty-Sitzung auch dafür zu protokollieren.

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

9. Wenn die Anruf-ID vorhanden ist, wird deutlich, dass die Protokolle der Teilnehmersitzungen erfasst wurden, andernfalls muss sie erneut ausgeführt werden.

Analyse

1. Überprüfen Sie, ob die DNS-Auflösung erfolgreich ist. Wenn sie erfolgreich ist, liegt kein Problem mit DNS vor.

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

Ablaufverfolgungen der DNS-Auflösung

2. Überprüfen Sie die Statistiken auf Abonnentenebene, um die Paketverluste zu überprüfen.

<#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. Überprüfen Sie die Ausgabe des Befehls show active loading auf ECS/ACS-Paketverlust, und überprüfen Sie, ob Pakete verworfen wurden. Überprüfen Sie anschließend in der Konfiguration, welche Aktion konfiguriert wurde.

<#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. Überprüfen Sie, ob die TCP-Verbindung zwischen UE und dem Server hergestellt wurde.

5. Wenn in keinem dieser Schritte Tropfen festgestellt werden, gibt es kein Problem im Knoten.

Paketverlust

- Überprüfen Sie die Abonnentenveröffentlichungsstatistik, um festzustellen, ob es ähnlich wie hier zu Paketverlusten kommt.

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. Überprüfen Sie den Prozentsatz der Fehler, die in der Ausgabe von Anzeigeabonnenten festgestellt wurden. Wenn das Paket weniger als 1 % verwirft, ist dies höchstwahrscheinlich ein Zufall und hat keine Auswirkungen.

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. Wenn Sie feststellen, dass Pakete in der RX-Bewertungsgruppe und in ITC-Paketen verworfen werden, ist dies höchstwahrscheinlich auf ein Bandbreitenproblem zurückzuführen, und das Abonnentenpaket ist abgelaufen.

ITC Packets Drop: 47235019

4. Auf ECS-Ebene muss die DPI-Konfiguration, einschließlich Regeldefinition, Abrechnungsaktion und Regelbasis, überprüft werden, um festzustellen, ob Blockierungsfaktoren vorliegen. Es gibt verschiedene Arten von Tropfen auf ECS-Ebene, und die nächste Vorgehensweise hängt von der jeweiligen Art des festgestellten Tropfens ab.

5. MTU-Größe für die Paketgröße, die weitergeleitet und nicht verarbeitet wird.

6. Zwischengeschaltete Pfadprobleme, bei denen das Paket verworfen wird, können anhand von TCP-Dump-/Traces auf Benutzerebene identifiziert werden.

Der Aktionsplan für die Rückforderung ist bei dieser Art von Problem nicht identisch, da er je nach Muster der Frage variiert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.