Troubleshoot User Data Browsing Issue for Specific Web URLs

Contents

Introduction

This document describes the user data browsing issues on the 4G network for all Uniform Resource Locators (URLs).

Prerequisites

Cisco recommends that you have knowledge of these nodes' functionalities:

- Serving Packet Data Gateway (SPGW)
- Control and User Plane Separation (CUPS)

Identification of Symptoms

> **Note**: Before you start with testing and log collection you must verify these details.

1. Check for which data type is the issue: IPv4/IPv6/IPv4v6

2. Check if the issue is with any particular Access Point Name (APN) or all the APNs because the issue can be related to a specific APN.

3. Check if the issue is for specific web URLs or multiple URLs.

4. Check if the URL is an enterprise URL/Customer app URL or some regular service URL and also check if the problem is with a specific VPN.

5. Check if the issue occurs when accessing the URL directly from the browser or while accessing the web app itself.

6. Check if the issue is intermittent in nature like post restart of the handset or refresh web URLs start working or the issue is consistent and does not work even after handset restart.

7. Check the rejection cause observed and for which rating group.

Logs Collection/Testing

> **Note**: For this kind of issue, you must perform real-time online troubleshooting with problematic user IMSI on which you must collect logs/traces accordingly.

Before proceeding with the testing and log collection:

```
Flush the subscriber from the node and also clear browsing history/database from testing user handset so

clear subscriber imsi <IMSI number>  ------------------ to be executed in the node to clear the subscrib
```

1. Start with the testing with one PDP type first like IPv4 where you see the issue.
2. Enable these debug logs and log the putty session. Ensure the session must not terminate (press tab/enter every few mins so that the session does not terminate).

<#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. Navigate to configuration mode and then enable logging monitor for the subscriber.

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

4. Open another terminal, log the putty session, and start monitoring subscriber with verbosity 5 and enable these 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. Attach the subscriber and browse the URL continuously for 3 to 5 minutes and while browsing execute these commands multiple times and log the putty session for the same.

<#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. After 5 minutes of browsing, execute the `no logging active` in the other terminal which is opened in Step 3.

7. Disable the logging monitor for the subscriber.

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

8. Do not stop the mon sub and let it run until you finish collecting number traces but keep an eye on the CPU.

9. Execute this command in order to get the caller id of the subscriber and log the putty session for this as well.

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

If the caller ID is present then it is clear that subscriber session logs were collected, if not, you need to run it again.

Troubleshooting Performed

1. Ping the Web URL server IP address and check if there are any packet drops.

```
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
```

2. Perform a traceroute from the GI context and check for any reachability issues.

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

Ex: traceroute 10.52.5.49 src 10.203.144.8
```

3. Check the subscriber statistics in order to check the packet drops.

<#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. Check the show active charging output for subscriber traffic impact.

```
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
```

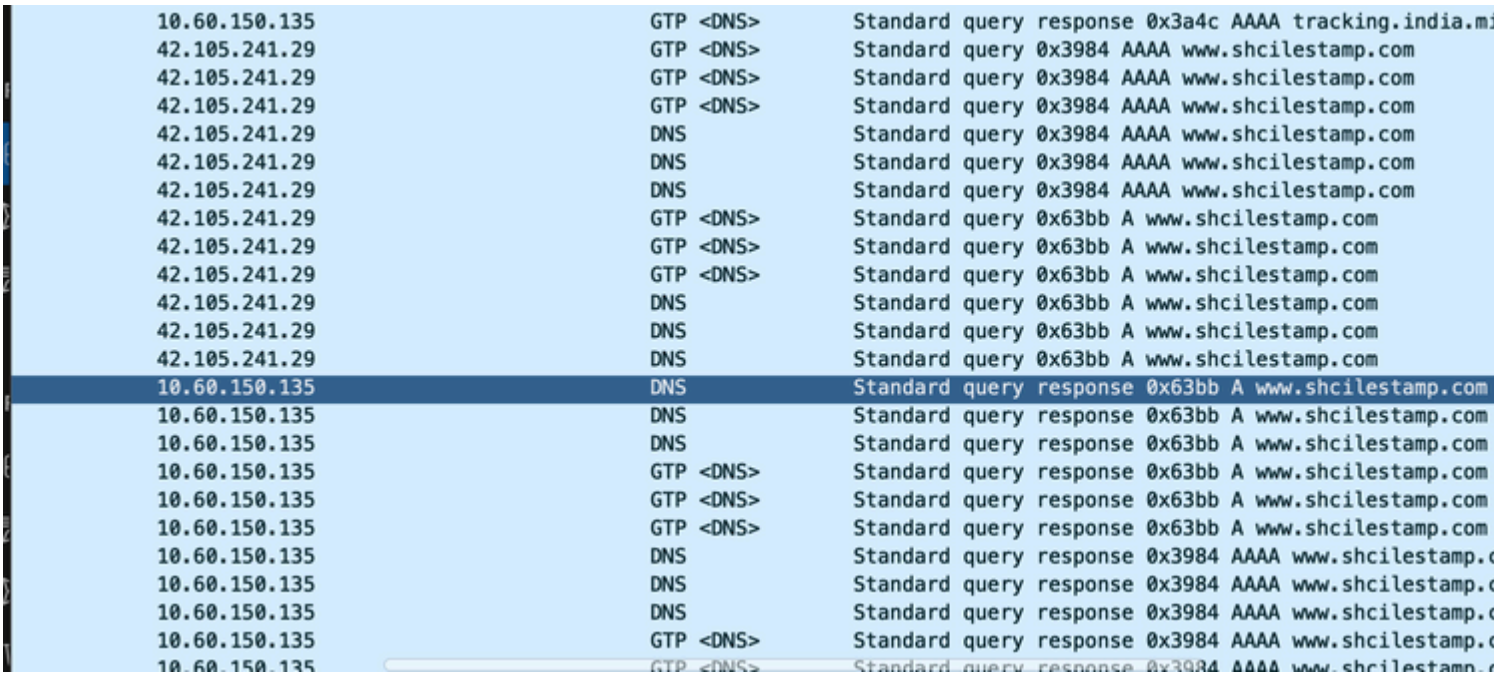
5. Check the show active charging command output for ECS/ACS level packet drop and check if there are any packet drops. Then check in the configuration what action is configured.

<#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. Check if the DNS resolution is successful or not. If it is successful then there is no issue with DNS.



10.60.150.135	GTP <DNS>	Standard query response 0x3a4c AAAA tracking.india.mi
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
10.60.150.135	DNS	Standard query response 0x63bb A www.shcilestamp.com
10.60.150.135	DNS	Standard query response 0x63bb A www.shcilestamp.com
10.60.150.135	GTP <DNS>	Standard query response 0x63bb A www.shcilestamp.com
10.60.150.135	GTP <DNS>	Standard query response 0x63bb A www.shcilestamp.com
10.60.150.135	GTP <DNS>	Standard query response 0x63bb A www.shcilestamp.com
10.60.150.135	DNS	Standard query response 0x3984 AAAA www.shcilestamp.c
10.60.150.135	DNS	Standard query response 0x3984 AAAA www.shcilestamp.c
10.60.150.135	DNS	Standard query response 0x3984 AAAA www.shcilestamp.c
10.60.150.135	GTP <DNS>	Standard query response 0x3984 AAAA www.shcilestamp.c
10.60.150.135	GTP <DNS>	Standard query response 0x3984 AAAA www.shcilestamp.c

7. Check the TCP connection is established successfully between User Equipment (UE) and the server.

8. If no drops are observed in any of these steps, then there is no issue in the node.

Packet Drops

1. Check the subscriber release statistics in order to determine whether you are experiencing packet drops similar to those shown here.

```
 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. Check the percentage of failures observed in the show subscriber output. If the packet drops are less than 1%, it is most likely a fluke and has no effect.

```
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. If you notice packet drops in the RX rating group and ITC packet drops, this is most likely due to a bandwidth issue and the subscriber package expired.

```
ITC Packets Drop:                          47235019
```

4. At Enhanced Charging Service (ECS) level, you must check/verify the ECS configuration of how ruled/charging action/rulebase are defined and if you have any blocking factor. There are different types of drops at the ECS level and based on the kind of drop you need to proceed with the next action plan.

5. MTU size for the packet size which is passing and not processed.

6. Intermediate path issues where the packet is getting dropped can be identified from TCP dump/user-level traces.

The recovery action plan is not the same for this type of issue as it varies as per the pattern of the issue.