

LTE에서 사용자 검색 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[증상](#)

[로그 수집/테스트](#)

[분석](#)

[패킷 삭제](#)

소개

이 문서에서는 4G 네트워크의 사용자 데이터 브라우징 문제를 설명합니다.

사전 요구 사항

이러한 노드의 기능에 대한 지식이 있는 것이 좋습니다

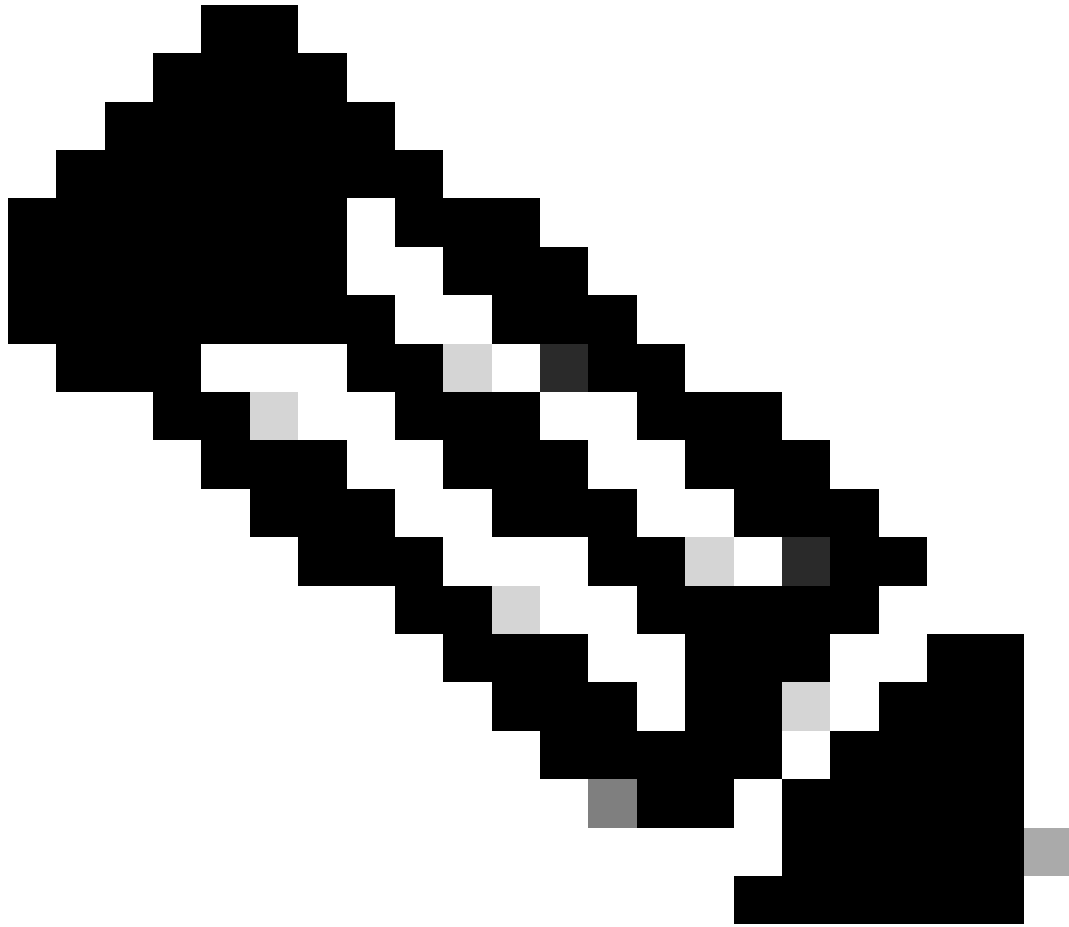
1. SPGW(Packet Data Gateway) 서비스
2. CUPS(Control and User Plane Separation)

증상

테스트 및 로그 수집을 시작하기 전에 앞서 언급된 세부 사항을 확인해야 합니다.

1. PDN(Packet Data Network) 데이터 형식이 어떤 것인지 확인하는 문제: IPv4/IPv6/IPv4v6
2. 특정 APN(Access Point Name) 또는 모든 APN과 관련된 문제인지 확인합니다. 이 문제는 특정 APN과도 관련이 있을 수 있습니다.
3. URL이 기업 URL/고객 앱 URL인지 아니면 일부 일반 서비스 URL인지, 그리고 특정 VPN에 문제가 있는지 확인합니다.
4. 브라우저에서 직접 URL에 액세스하거나 웹 앱 자체에 액세스하는 동안 문제가 발생하는지 확인합니다.
5. 핸드셋 재시작 후/새로 고침 웹 URL이 작동하기 시작하거나 핸드셋 재시작 후에도 문제가 지속되고 작동하지 않는 것처럼 문제가 간헐적으로 발생합니까?
6. 관찰된 거부 사유와 평가 그룹을 확인합니다.

로그 수집/테스트



참고: 이러한 종류의 문제에 대해서는 문제가 있는 사용자 IMSI를 사용하여 실시간 온라인 문제 해결을 수행해야 하며, 이에 따라 로그/추적을 수집해야 합니다.

테스트 및 로그 수집을 진행하기 전에

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. 모든 PDN 유형의 가입자에 대한 테스트로 시작합니다.
2. putty 세션을 기록하고 심각도 5로 모니터 가입자를 시작하고 이 옵션을 활성화합니다.

<#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. 이러한 디버그 로그를 사용하고 putty 세션을 기록하며 세션이 종료되지 않아야 하는지 확인하십시오(세션이 종료되지 않도록 탭/몇 분마다 입력).

<#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. 모드를 구성합니다. 가입자에 대한 로깅 모니터를 사용하도록 설정하십시오.

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

5. 가입자를 연결하고 URL을 3~5분 동안 계속해서 찾아보며, 찾아보는 동안 이 명령을 여러 번 실행하고 putty 세션을 로깅합니다.

<#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. 브라우징 5분 후 no logging active 4단계에서 열었던 단말기에서 실행

7. 가입자에 대한 로깅 모니터를 비활성화합니다.

Config

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

8. 이 명령을 실행하여 가입자의 통화 id를 가져오고 이에 대한 putty 세션도 기록합니다.

```
Show subscriber full imsi <imsi>. --> to get the call id
```

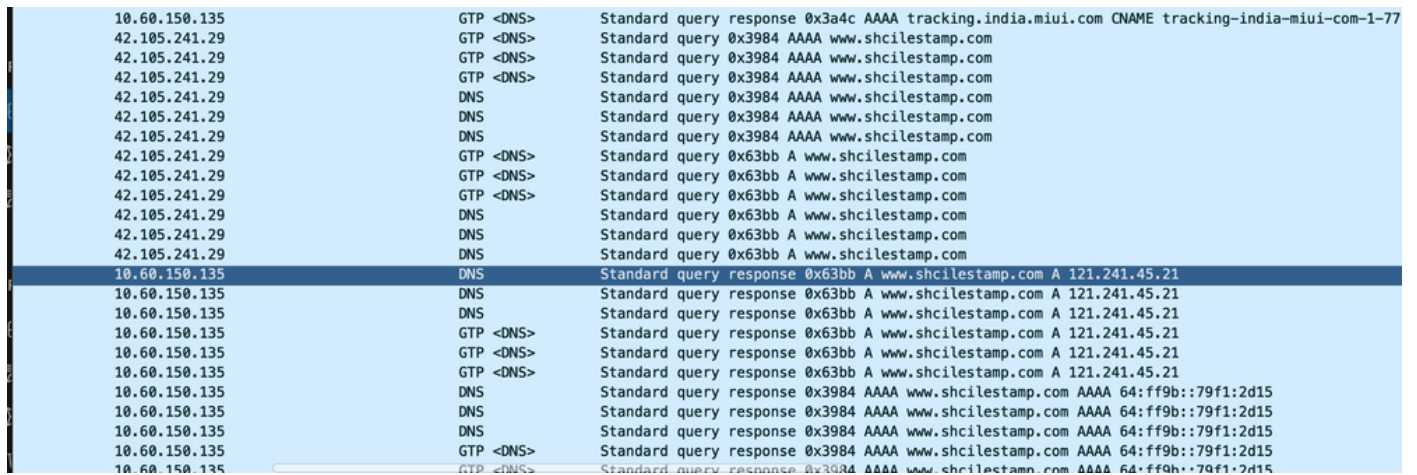
```
show logs callid <call_id>
```

```
show logs
```

9. 통화 id가 있으면 가입자 세션 로그가 수집되지 않은 경우 다시 실행해야 합니다.

분석

1. DNS 확인이 성공했는지 확인합니다. 성공하면 DNS에는 문제가 없습니다.



IP	Protocol	Message
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	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

DNS 확인 추적

2. 가입자 레벨 통계를 확인하여 패킷 삭제를 검토합니다.

<#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. ECS/ACS 레벨 패킷 삭제에 대한 show active charging 명령 출력을 확인하고 패킷 삭제가 있는지 확인한 다음, 구성된 작업을 컨피그레이션에서 확인합니다.

```
<#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. TCP 연결이 UE와 서버 간에 성공적으로 설정되었는지 확인합니다.
- 5. 이 단계에서 관찰된 누락이 없는 경우 노드에는 문제가 없습니다.

패킷 삭제

- 여기에 표시된 것과 유사한 패킷 삭제를 경험하고 있는지 확인하려면 가입자 릴리스 통계를 확인합니다.

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. show subscriber 출력에 관찰된 실패 비율을 확인합니다. 패킷 드랍이 1% 미만인 경우 대부분 폴러크일 가능성이 높으며 아무 영향도 미치지 않습니다.

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. RX 등급 그룹의 패킷 삭제 및 ITC 패킷 삭제를 확인할 경우, 이는 대역폭 문제 및 가입자 패키지 만료 때문일 가능성이 높습니다.

ITC Packets Drop: 47235019

4. ECS 레벨에서, 차단 요소가 있는지 확인하기 위해 규칙 정의, 과금 작업, 규칙 베이스를 포함한 DPI 컨피그레이션을 확인하는 것이 중요합니다. ECS 레벨에는 다양한 유형의 드롭이 있으며, 다음에 수행할 작업은 발생한 드롭의 특정 유형에 따라 달라집니다.

5. 전달 중이고 처리되지 않은 패킷 크기의 MTU 크기입니다.

6. 패킷이 삭제되는 중간 경로 문제는 TCP 덤프/사용자 수준 추적에서 식별할 수 있습니다.

복구 작업 계획은 문제의 패턴에 따라 달라지므로 이 유형의 문제에 대해서는 동일하지 않습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.