

Risoluzione dei problemi relativi all'esplorazione dei dati utente per URL Web specifici

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Identificazione dei sintomi](#)

[Raccolta/test log](#)

[Risoluzione dei problemi](#)

[Perdite di pacchetti](#)

Introduzione

Questo documento descrive i problemi di navigazione dei dati utente sulla rete 4G per tutti gli URL (Uniform Resource Locator).

Prerequisiti

Cisco raccomanda la conoscenza delle funzionalità di questi nodi:

- SPGW (Packet Data Gateway) del server
- Separazione dei piani di controllo e degli utenti (CUPS)

Identificazione dei sintomi



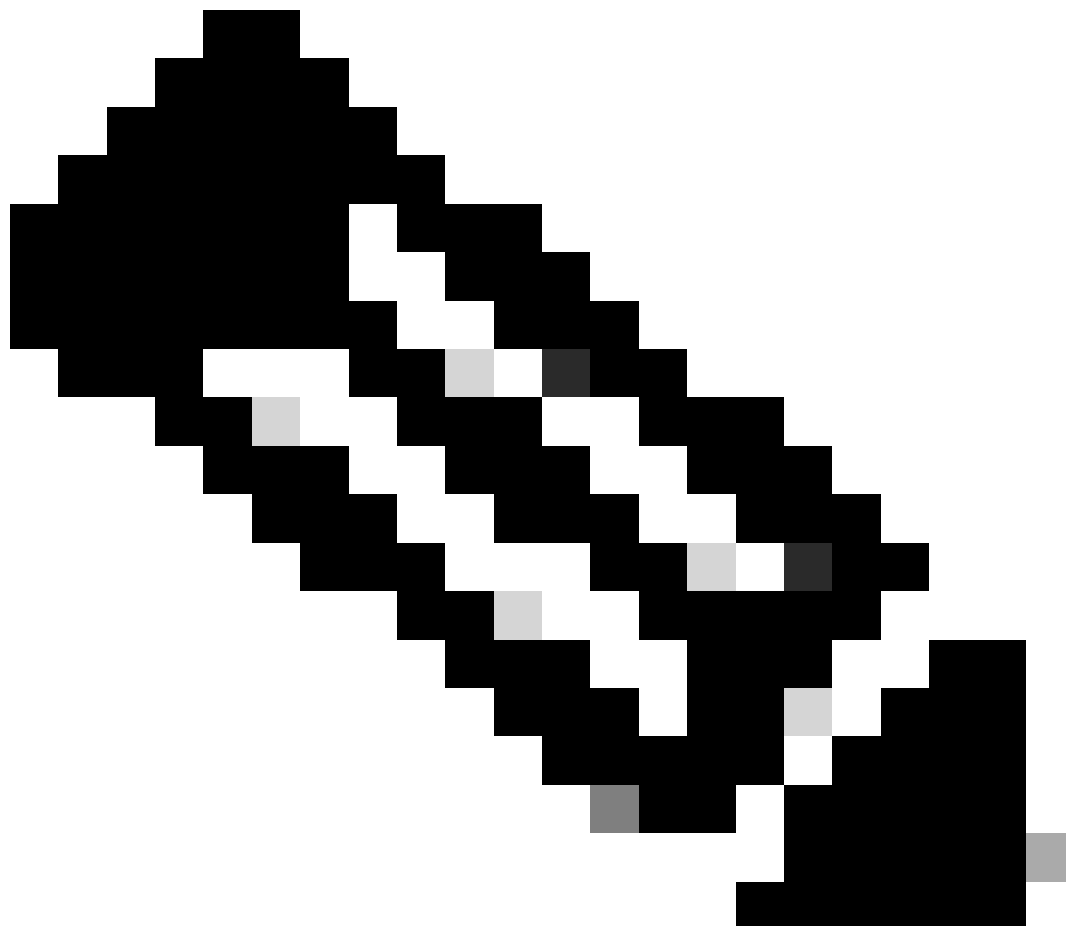
Nota: prima di iniziare con il test e la raccolta dei log, è necessario verificare questi dettagli.

-
1. Verificare quale tipo di dati è il problema: IPv4/IPv6/IPv4v6
 2. Verificare se il problema riguarda un determinato nome di punto di accesso (APN) o tutti i nomi di punto di accesso (APN), in quanto il problema può essere correlato a un APN specifico.
 3. Verificare se il problema si riferisce a URL Web specifici o a più URL.
 4. Verificare se l'URL è un URL aziendale/URL dell'app del cliente o un URL di servizio regolare, nonché verificare se il problema riguarda una VPN specifica.
 5. Verificare se il problema si verifica quando si accede all'URL direttamente dal browser o durante l'accesso all'app Web stessa.
 6. Verificare se il problema è di natura intermittente, ad esempio dopo il riavvio del ricevitore o l'aggiornamento degli URL Web, o se è coerente e non funziona neanche dopo il riavvio del

ricevitore.

7. Controllare la causa del rifiuto osservata e per quale gruppo di rating.

Raccolta/test log



Nota: per questo tipo di problema, è necessario eseguire la risoluzione dei problemi online in tempo reale con IMSI utente problematico su cui è necessario raccogliere log/tracce di conseguenza.

Prima di procedere con il test e la raccolta dei log:

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. Iniziare con il test con un tipo di PDP, come IPv4, in cui viene visualizzato il problema.
2. Abilitare questi registri di debug e registrare la sessione putty. Assicurarsi che la sessione non venga terminata (premere TAB/Invio a intervalli di qualche minuto in modo che la sessione non venga terminata).

<#root>

On SPGW:

```
logging filter active facility sessmgr level debug
logging filter active facility acsmgr level debug
logging filter active facility npumgr-ac1 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-ac1 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. Passare alla modalità di configurazione e quindi abilitare il monitoraggio della registrazione per il sottoscrittore.

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

4. Aprire un altro terminale, registrare la sessione putty e avviare il monitoraggio del sottoscrittore con il livello di dettaglio 5 e abilitare le seguenti opzioni:

```
<#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. Collegare il sottoscrittore e sfogliare l'URL continuamente per 3-5 minuti e durante la navigazione eseguire questi comandi più volte e registrare la sessione putty per lo stesso.

```
<#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. Dopo 5 minuti di navigazione, eseguire il comando `no logging active` nell'altro terminale aperto al punto 3.

7. Disabilitare il monitoraggio della registrazione per il sottoscrittore.

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

8. Non arrestare la funzione `mon sub` e lasciarla in esecuzione finché non si termina di raccogliere le tracce dei numeri, ma tenere d'occhio la CPU.

9. Eseguire questo comando per ottenere l'ID chiamante del sottoscrittore e registrare la sessione putty anche per questo.

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

Se l'ID chiamante è presente, è chiaro che i registri della sessione del sottoscrittore sono stati raccolti. In caso contrario, è necessario eseguirlo di nuovo.

Risoluzione dei problemi

- Eseguire il ping dell'indirizzo IP del server URL Web e verificare se vi sono perdite di pacchetti.

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. Effettuare una verifica dal contesto dell'indicazione geografica e verificare se esistono problemi di raggiungibilitàtracroute.

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

Ex: tracroute 10.52.5.49 src 10.203.144.8

3. Controllare le statistiche del destinatario per controllare le perdite di pacchetti.

<#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. Controllare l'output show active charge per verificare l'impatto del traffico degli utenti.

```
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. Controllare l'output del comando show active charge per verificare se vi sono perdite di pacchetti a livello di ECS/ACS. Quindi, archiviare la configurazione per verificare quale azione è configurata.

```
<#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. Verificare se la risoluzione DNS ha esito positivo o meno. In caso di esito positivo, non vi è alcun problema con il 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. Verificare che la connessione TCP sia stata stabilita correttamente tra l'apparecchiatura utente (UE) e il server.

8. Se in uno di questi passi non si osservano cali, non vi sono problemi nel nodo.

Perdite di pacchetti

1. Controlla le statistiche di rilascio del destinatario predefinito per determinare se si stanno verificando perdite di pacchetti simili a quelle mostrate qui.

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. Controllare la percentuale di errori osservati nell'output del comando show subscriber. Se il pacchetto cade meno dell'1%, è molto probabile che sia un colpo di fortuna e non abbia alcun effetto.

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. Se si notano cali di pacchetti nel gruppo di classificazione RX e cali di pacchetti ITC, è molto probabile che ciò sia dovuto a un problema di larghezza di banda e che il pacchetto dell'utente sia scaduto.

ITC Packets Drop:

47235019

4. A livello di servizio di ricarica avanzato (ECS), è necessario controllare/verificare la configurazione ECS di come sono definite le azioni/la base delle regole di gestione/ricarica e se si dispone di un fattore di blocco. Ci sono diversi tipi di cadute a livello ECS e in base al tipo di caduta è necessario procedere con il prossimo piano d'azione.

5. Dimensioni MTU per le dimensioni del pacchetto che vengono trasferite e non elaborate.

6. I problemi di percorso intermedi in cui il pacchetto viene scartato possono essere identificati dalle tracce TCP dump/livello utente.

Il piano d'azione per la ripresa non è lo stesso per questo tipo di problemi, in quanto varia a seconda del modello del problema.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).