

# Risoluzione dei problemi relativi alla trap X3MDConnDown e X3MDConnUp osservata in PGW

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Comandi usati](#)

[Soluzione](#)

## Introduzione

Questo documento descrive il processo per identificare la causa dei trap **X3MDConnDown** e **X3MDConnUp** in Cisco Packet Data Network Gateway (PGW) dopo l'aggiornamento da 21.18.17 a 21.25.8 in grandi numeri.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- StarOS/PGW
- Conoscenza delle interfacce e delle funzionalità di X1, X2 e X3
- Conoscenza della determinazione TCP per X3

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- PGW Aggregation Services Router (ASR) 5500
- Versioni 21.18.17 .79434 e 21.25.8.84257

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

La soluzione Lawful Interception dispone di tre interfacce discrete tra l'elemento di rete e mediation server per fornire informazioni su provisioning, dati di chiamata (segnale) e contenuto di chiamata (supporto). Queste interfacce vengono create dopo che è stata stabilita la connessione tra la funzione di recapito del server di mediazione XCIPIO (DF) e la funzione di accesso agli elementi di rete (AF). L'interfaccia tra il server di mediazione e l'agenzia di intercettazione legale è standardizzata. Le interfacce tra AF e DF sono definite come segue:

- Interfaccia X1 o INI-1 per il provisioning delle destinazioni
- Interfaccia X2 o INI-2 per fornire informazioni di segnalazione per la destinazione
- Interfaccia X3 o INI-3 per fornire contenuti multimediali o di chiamata per la destinazione

Dove l'interfaccia X è definita dallo standard 3GPP mentre INI è definita dallo standard ETSi.

# Problema

Dopo l'aggiornamento del nodo da 21.18.17 a 21.25.8, è iniziato a venire un allarme per **X3MDCConnDown** e **X3MDCConnUp** in Bulk (circa 3000 in un'ora).

Formato trap:

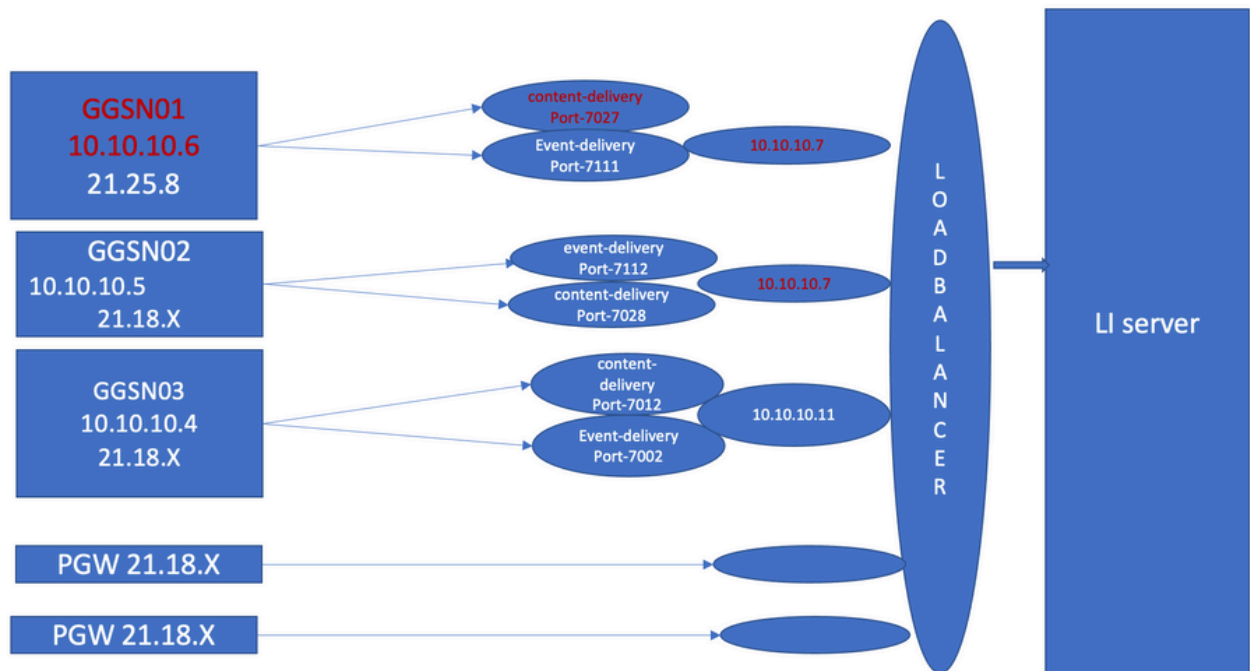
Mon Jul 04 00:44:15 2022 Internal trap notification 1422 (X3MDCConnDown) TCP connection is down. Context Id:8, Local IP/port:10.10.10.1/41833 and Peer IP/port: x.x.x.x/7027 with cause: LI X3 CALEA Connection Down

Mon Jul 04 00:45:29 2022 Internal trap notification 1423 (X3MDCConnUp) TCP connection is up. Context Id:8, Local IP/port:10.10.10.1/56805 and Peer IP/port: x.x.x.x/7027 with cause: LI X3 CALEA Connection UP

Dettagli trap in ore:

Old SSD pre enabling heartbeat timer					
Date	Time	10.10.10.6			
		X3MDCConnDown	X3MDCConnUP		
4th June	15 HRS	577	578		
4th June	16 HRS	1487	1490		
4th June	17 HRS	417	1490		

Il problema è evidenziato in rosso in questa immagine:



Procedura di risoluzione dei problemi:

1. Controllate i servizi verso il server LI, non troverete alcun impatto.
2. I file LI possono essere trasferiti sul server LI.
3. Ping e traceroute sono stati trovati correttamente sul server LI.
4. Non è stata osservata alcuna latenza e perdita di pacchetti.
5. Quando si tenta di acquisire il dump TCP verso il server LI, i pacchetti unidirezionali vengono acquisiti in dump TCP per il nodo problematico.

Confrontatelo con il nodo funzionante e vedrete lo stesso comportamento.

1. Quando si crea una porta diversa sul server LI, si osserva che il problema rimane.
2. Quando si crea un altro LI Test Server e un'altra porta, si osserva lo stesso allarme al Gateway GPRS Support Node (GSN).
3. Quando si acquisiscono le tracce aggiuntive, ad esempio la traccia NPU-PAN, i comandi show e i registri di debug, si nota che FIN ACK proviene dal server LI subito dopo SYN dal PGW e ciò genera trap **X3MDCConnDown** e **X3MDCConnUp**.
4. Come per il team di progettazione, la versione 21.25.8 riconosce il FIN ACK e genera l'allarme **X3MDCConnDown** e quindi **X3MDCConnUp**. Non presente nelle versioni precedenti a 21.18.17 .
5. È stata attivata una soluzione alternativa al timer di heartbeat (1 m) sul server GSN e LI pubblicare che **X3MDCConnDown** e l'allarme **X3MDCConnUp** è in controllo. Viene ridotto da circa 3000 a 100 per 1 giorno.
6. Il nodo viene monitorato per 2 settimane e **X3MDCConnDown** e gli allarmi **X3MDCConnUp**.

## Comandi usati

1. Da questi comandi, i file LI vengono trasferiti correttamente al server LI. Non vi sono problemi con la connessione TCP al server LI.

```
show lawful-intercept full imsi <>
```

### Ad esempio:

```
[llictx]GGSN# show lawful-intercept full msisdn XXXXXXXXXX
```

```
Monday April 25 14:15:11 IST 2022
```

```
Username : -
```

```
ip-address : XXXXXXXXX
```

```
msid/imsi : XXXXXXXXXX
```

```
msisdn : XXXXXXXXX
```

```
imei/mei : XXXXXXXX
```

```
session : Session Present
```

```
service-type : pgw
```

```
pdhir : Disabled
```

```
li-context : lictx
```

```
intercept-id : 58707
```

```
intercept-key: -
```

```
Content-delivery: tcp-format
```

```
TCP connection info
```

```
State : ACTIVE
```

```
Dest. address: XX.XX.XX.XX Dest. Port: XXXX——>>
```

```
Num. Intercepted pkt for Active call: XXXX ——>>>
```

```
Event-delivery: tcp-format——>>
```

```
TCP connection info ——>>
```

```
State : ACTIVE——>>
```

```
Dest. address: XX.XX.XX.XX Dest. Port: XXXX——>>
```

```
Num. Intercepted pkt for Active call: 13 ——>>>
```

```
Provisioning method: Camp-on trigger
```

```
LI-index : 649
```

**Per visualizzare gli output completi di questi comandi è necessario l'accesso come amministratore di sistema:**

```
show lawful-intercept statistics
```

```
show lawful-intercept buffering-stats sessmgr all
```

```
show lawful-intercept statistics
```

```
show connection-proxy sockets all
```

```
show lawful-intercept error-stats
```

## 2. Raccogli i seguenti log del livello di debug:

```
logging filter active facility dhost level debug
```

```
logging filter active facility li level debug
```

```
logging filter active facility connproxy level debug
```

```
logging filter active facility ipsec level debug
```

```
logging filter active facility ipsecdemux level debug
```

```
logging active pdu-verbosity 5
```

```
Logging active
```

```
No logging active
```

In questa finestra è possibile verificare che le informazioni sulla porta cambiano se non sono stabili.

```
show dhost socket (in li context)
```

## 3. Accedere in modalità nascosta e accedere all'attività VPP (Vector Packet Processing) per verificare se i pacchetti sono in arrivo per la conferma FIN (ACK).

```
[l1ctx]GGSN# debug shell
```

```
enter vppct (from deb shell, use cmd "vppctl")
```

```
vpp#show hsi sessions
```

### Ad esempio:

```
[local]g002-laas-ssi-24# deb sh
```

```
Friday May 13 06:03:24 UTC 2022
```

```
Last login: Fri May 13 04:32:03 +0000 2022 on pts/2 from 10.78.41.163.
```

```
g002-laas-ssi-24:ssi# vppctl
```

```
vpp# sho hsi sessions
```

```
[s1] dep 1 thread 10 fib-index 6 dst-src [3.2.1.1:9002]-[3.1.1.1:42906]
```

```
[s2] dep 1 thread 9 fib-index 6 dst-src [3.2.1.1:9003]-[3.1.1.1:60058]
```

```
[s3] dep 1 thread 8 fib-index 6 dst-src [3.2.1.1:9004]-[3.1.1.1:51097]
```

```
[s4] dep 1 thread 6 fib-index 6 dst-src [3.2.1.1:9005]-[3.1.1.1:45619]
```

## 4. Dopo aver abilitato i log di debug, è possibile abilitare Show output logs in LI context con il comando test.

```
show clock
show dhost sockets
show connection-proxy sockets all
show clock
```

5. Raccogliere i dettagli di Mostra supporto.

6. Raccogliere la traccia NPU-PAN per riconoscere che il pacchetto ha unconnessione TCP al server LI riuscita.

Per disabilitare:

```
#configure

#no npumgr pan-trace

#npumgr pan-trace monitor none

#end

#show npumgr pan-trace configuration

#configure

#npumgr pan-trace acc monitor ipv4 id 1 protocol tcp sa X.X.X.X mask 255.255.255.255 da X.X.X.X mask 255.255.255.255

#npumgr pan-trace acc monitor ipv4 id 2 protocol tcp sa X.X.X.X mask 255.255.255.255 da X.X.X.X mask 255.255.255.255

#npumgr pan-trace limit 4096

#npumgr pan-trace

#end
```

(check if disabled/enabled, it should be enabled)

```
#show npumgr pan-trace configuration
```

Questo comando potrebbe arrestare la traccia di panning della NPU, quindi è necessario riconfigurarla per la raccolta successiva.

```
#show npumgr pan-trace summary
```

(We can capture packets based on npu number which can be done during testing if possible)

```
#show npumgr pan-trace detail all
```

Esempio di traccia NPU:

```
3538 6/0/2 Non 6/15 fab 70 Jun 02 16:47:10.05443343 144 Eth() Vlan(2014) IPv4(sa=XX.XX.XX.147, da=XX.XX.XX.201)
TCP(sp=7027, dp=46229, ACK FIN) [ vrf=8 strip=40 flow ] >> MEH(sbia=050717de, dbia=0603800e, flowid=62755625, ln)
IPv4(sa=XX.XX.XX.147, da=XX.XX.XX.201) TCP(sp=7027, dp=46229, ACK FIN)
```

Packet details :

Packet 3538:

SA [4B] = XX.XX.XX.147[0x0aa40693]

DA [4B] = XX.XX.XX.201[0x0aa91ec9]

source port [2B] = 0x1b73 (7027), dest port [2B] = 0xb495 (46229)

seqnum [4B] = 0xc9923207 (3381801479)

acknum [4B] = 0xbbd482ef (3151266543)

flags [6b] = 0x11 ACK FIN

## Soluzione

Abilitare il timeout dei messaggi heartbeat a 1 minuto in PGW e XX.XX.XX.147 (LI Server) con questo comando:

```
lawful-intercept tcp application-heartbeat-messages timeout minutes 1
```

Supponiamo che FIN ACK venga immediatamente dopo SYN dal server LI. In questo caso, PGW non considera inattiva un'interfaccia X3 perché l'heartbeat è abilitato 1 minuto in PGW e abilitato sul server LI, il che indica che la connessione X3 è attiva in quanto l'heartbeat è presente. Gli allarmi vengono quindi ridotti per **X3MDConnDown** e **X3MDConnUp**.

Analisi delle trap pre e post SSD:

GGSN				GGSN				GGSN							
latest (30 June) SSD post enabling heartbeat timer				latest (1st jul) SSD post enabling heartbeat timer				latest (2nd jul) SSD post enabling heartbeat timer							
Date	Time	10.10.10.6(Live LI server)	10.10.10.2(Test LI server)	Date	Time	10.10.10.6(Live LI server)	10.10.10.2(Test LI server)	Date	Time	10.10.10.6(Live LI server)	10.10.10.2(Test LI server)				
29th June	8 HRS	1	17	1	14	7	43	4	51	01-Jul	13 HRS	0	1	0	0
29th June	9 HRS	1	9	1	8	0	2	0	2	01-Jul	14 HRS	0	8	0	8
29th June	10 HRS	1	7	2	6	0	0	0	0	01-Jul	15 HRS	0	1	0	1
29th June	11 HRS	17	23	14	24	0	4	0	4	01-Jul	16 HRS	0	1	0	1
29th June	12 HRS	0	4	0	4	0	0	0	0	01-Jul	17 HRS	0	1	0	1
29th June	13 HRS	0	4	0	4	0	2	0	2	01-Jul	18 HRS	0	4	0	4
29th June	14 HRS	0	4	0	3	0	8	0	7	01-Jul	19 HRS	0	0	0	0
29th June	15 HRS	0	22	0	21	0	2	0	3	01-Jul	20 HRS	0	0	0	0
29th June	16 HRS	1	24	0	21	2	20	2	19	01-Jul	21 HRS	0	1	0	1
29th June	17 HRS	0	5	0	6	1	8	1	8	02-Jul	01 HRS	0	5	0	4
29th June	18 HRS	0	0	0	0	0	1	0	1	02-Jul	2 HRS	0	0	0	0
29th June	19 HRS	0	5	0	6	0	1	0	1	02-Jul	3 HRS	0	1	0	1
29th June	20 HRS	0	5	0	5	0	0	0	0	02-Jul	4 HRS	0	2	0	2
29th June	21 HRS	0	2	0	2	0	0	0	0	02-Jul	5 HRS	0	8	0	8
29th June	22 HRS	5	16	4	16	0	0	0	0	02-Jul	6 HRS	0	1	0	1
29th June	23 HRS	0	16	0	8	0	1	0	1	02-Jul	7 HRS	0	0	0	0
30th June	00 HRS	7	44	4	51	1	18	1	16	02-Jul	8 HRS	0	0	0	0
<b>Total</b>		<b>33</b>	<b>207</b>			<b>31</b>	<b>152</b>			<b>Total</b>		<b>0</b>	<b>37</b>	<b>0</b>	<b>2</b>
GGSN				GGSN				GGSN							
latest (28 June) SSD post enabling heartbeat timer				latest (26 June) SSD post enabling heartbeat timer				Old SSD pre enabling heartbeat timer							
Date	Time	10.10.10.6(Live LI server)	10.10.10.2(Test LI server)	Date	Time	10.10.10.6(Live LI server)	10.10.10.2(Test LI server)	Date	Time	10.10.10.6	X3MDConnUP				
28th June	14 HRS	462	496	443	466	500	502	497	497	4th June	15 HRS	577	578		
28th June	15 HRS		322		280	746	748	751	751	4th June	16 HRS	1487	1490		
										4th June	17 HRS	417	1490		

Tendenze delle trap SNMP dopo la soluzione:

Mon Jul 04 00:44:15 2022 Internal trap notification: 1422 (X3MDConnDown) TCP connection is down. Context Id:8, Local IP/port:10.10.10.1/41833 and Peer IP/port: 10.10.10.6/7027with cause: LI X3 CALEA Connection Down

Mon Jul 04 11:13:20 2022 Internal trap notification: 1422 (X3MDConnDown) TCP connection is down. Context Id:8, Local IP/port:10.10.10.1/47122 and Peer IP/port: 10.10.10.6/7027with cause: LI X3 CALEA Connection Down

=====

Tue Jul 05 09:45:11 2022 Internal trap notification: 1422 (X3MDConnDown) TCP connection is down. Context Id:8, Local IP/port:10.10.10.1/34489 and Peer IP/port: 10.10.10.6/7027 with cause: LI X3

CALEA Connection Down

Tue Jul 05 09:45:56 2022 Internal trap notification 1423 (X3MDConnUp) TCP connection is up.  
Context Id:8, Local IP/port:10.10.10.1/51768 and Peer IP/port: 10.10.10.6/7027 with cause: LI X3  
CALEA Connection UP

Tue Jul 05 09:57:57 2022 Internal trap notification 1423 (X3MDConnUp) TCP connection is up.  
Context Id:8, Local IP/port:10.10.10.1/34927 and Peer IP/port: 10.10.10.6/7027 with cause: LI X3  
CALEA Connection UP

Tue Jul 05 17:10:30 2022 Internal trap notification 1423 (X3MDConnUp) TCP connection is up.  
Context Id:8, Local IP/port:10.10.10.1/59164 and Peer IP/port: 10.10.10.6/7027 with cause: LI X3  
CALEA Connection UP

Tue Jul 05 17:11:00 2022 Internal trap notification 1423 (X3MDConnUp) TCP connection is up.  
Context Id:8, Local IP/port:10.10.10.1/52191 and Peer IP/port: 10.10.10.6/7027 with cause: LI X3  
CALEA Connection UP

Tue Jul 05 17:11:07 2022 Internal trap notification 1423 (X3MDConnUp) TCP connection is up.  
Context Id:8, Local IP/port:10.10.10.1/46619 and Peer IP/port: 10.10.10.6/7027 with cause: LI X3  
CALEA Connection UP

Tue Jul 05 17:14:23 2022 Internal trap notification 1423 (X3MDConnUp) TCP connection is up.  
Context Id:8, Local IP/port:10.10.10.1/59383 and Peer IP/port: 10.10.10.6/7027 with cause: LI X3  
CALEA Connection UP

Tue Jul 05 17:17:31 2022 Internal trap notification 1423 (X3MDConnUp) TCP connection is up.  
Context Id:8, Local IP/port:10.10.10.1/59104 and Peer IP/port: 10.10.10.6/7027 with cause: LI X3  
CALEA Connection UP

**Di seguito è riportato lo stato delle ultime trap osservate e si noti che non vengono generate nuove trap.**

```
[local]GGSN# show snmp trap statistics verbose | grep X3MDConn
```

Thursday July 21 12:36:38 IST 2022

X3MDConnDown	12018928	0	9689294	2022:07:05:11:36:23
X3MDConnUp	12030872	0	9691992	2022:07:05:17:17:31

```
[local]GGSN# show snmp trap history verbose | grep x.x.x.x
```

Thursday July 21 12:36:57 IST 2022