

# Troubleshoot X3MDConnDown and X3MDConnUp Trap Observed in PGW

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Problem](#)

[Commands Used](#)

[Solution](#)

## Introduction

This document describes the process to identify the cause of the Traps **X3MDConnDown** and **X3MDConnUp** in **Cisco Packet Data Network Gateway (PGW)** post upgrade from 21.18.17 to 21.25.8 in large numbers.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- StarOS/PGW
- Knowledge of X1, X2, and X3 interface and functionality
- Knowledge of TCP establishment for X3

### Components Used

The information in this document is based on these software and hardware versions:

- PGW Aggregation Services Router (ASR) 5500
- Versions 21.18.17.79434 and 21.25.8.84257

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

The Lawful Interception solution has three discrete interfaces between the network element and mediation server to provide provisioning, call data (signal) and call content (media) information.

These interfaces are created after the connection is established between the XCIPIO mediation server Delivery Function (DF) and the network element Access Function (AF). The interface from the mediation server to the lawful interception agency is standardized. The interfaces between AF and DF are defined as:

- X1 or INI-1 interface for provisioning targets
- X2 or INI-2 interface to provide signaling information for the target
- X3 or INI-3 interface to provide media or call content for the target

Where the X interface is defined by the 3GPP standard while INI is defined by the ETSi standard.

## Problem

Post the node upgrade from 21.18.17 to 21.25.8, an alarm started to come for **X3MDCConnDown and X3MDCConnUp** in Bulk (around 3000 in one hour).

Trap format:

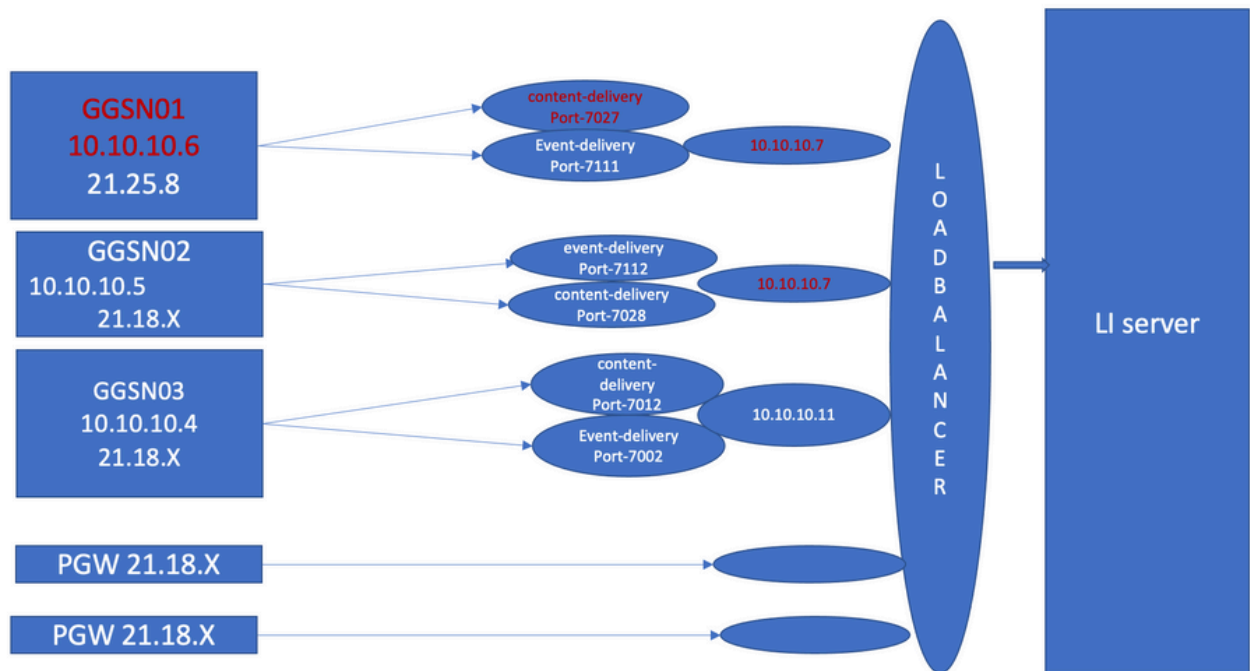
Mon Jul 04 00:44:15 2022 Internal trap notification 1422 (X3MDCConnDown) TCP connection is down. Context Id:8, Local IP/port:10.10.10.1/41833 and Peer IP/port: x.x.x.x/7027 with cause: LI X3 CALEA Connection Down

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

Trap details in HRS:

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		

The problem is highlighted in red in this image:



### Troubleshooting steps:

1. Check the services towards the LI server, you will find no impact.
2. LI files are able to transfer to the LI server.
3. Ping and traceroute were found OK to the LI server.
4. No latency and packet drop has been observed.
5. When you try to capture the TCPdump towards the LI server, one-way packets are captured in TCPdump for the problematic node.

Compare it with the working node and you see the same behaviour.

1. When you create a different port at the LI server, you observe that the issue remains.
2. When you create another LI Test server and port, you observe the same alarm at Gateway GPRS Support Node (GGSN).
3. When you capture the additional traces, such as the NPU-PAN trace, show commands, and debug logs, you see that FIN ACK comes from the LI server just after the SYN from the PGW and this results in Traps **X3MDCConnDown** and **X3MDCConnUp**.
4. As per the Engineering team, the 21.25.8 version recognises the FIN ACK and generates the alarm **X3MDCConnDown** and then **X3MDCConnUp**. Which is not seen in releases earlier than 21.18.17.
5. A workaround **Heartbeat Timer (1m)** has been enabled at the GGSN and LI server post that the **X3MDCConnDown** and **X3MDCConnUp** alarm is in control. It is reduced from around 3000 to 100 for 1 day.
6. Node is monitored for 2 weeks, and the **X3MDCConnDown** and **X3MDCConnUp** alarms came under control.

## Commands Used

1. From these commands, LI files are transferred to the LI server properly. There is no issue with the TCP connection to the LI server.

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

### For example:

```
[lictx]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
```

**These commands need LI admin access to see full outputs:**

```
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. Collect these debug level logs:

```
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
```

Here, you can see port information change if they are not stable.

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

## 3. Enter into Hidden mode and go into Vector Packet Processing (VPP) task to check if packets come for FIN acknowledge (ACK).

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

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

```
vpp#show hsi sessions
```

### For example:

```
[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. Show output logs in LI context can be enabled under test command after you enable debug logs.

```
show clock
```

```
show dhost sockets
```

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

5. Collect the Show support details.

6. Collect NPU-PAN trace to recognise that the packet has a successful TCP connection with the LI server.

To disable:

```
#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
```

This command could stop the NPU pan trace, so it needs to be reconfigured for the next collection.

```
#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
```

Example of NPU Trace:

```
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, In)
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

## Solution

Enable heartbeat messages timeout to 1 minute at PGW & XX.XX.XX.147 (LI Server) with this command:

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

Suppose FIN ACK comes just after the SYN from the LI server. In that case, PGW does not consider an X3 interface down because the heartbeat is enabled 1 min in PGW and enabled at the LI server too which is an indication that the X3 connection is UP as the heartbeat is present. So, the alarms are reduced for **X3MDConnDown** and **X3MDConnUp**.

Pre and Post SSD Trap analysis:

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	3	9	1	8	02-Jul	01 HRS	0	5	0	4		
29th June	18 HRS	0	0	0	0	0	1	0	1	02-Jul	10 HRS	0	0	0	0		
29th June	19 HRS	0	5	0	6	0	1	0	1	02-Jul	2 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		
Total		33	207			0	8	0	9	02-Jul	9 HRS	0	0	0	0		
GGSN				GGSN				GGSN									
latest (28 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)						
28th June	14 HRS	462	496	443	466	30th June	20 HRS	1	7	1	7	02-Jul	11 HRS	0	0	0	
28th June	15 HRS		322		280	30th June	21 HRS	0	0	0	0	02-Jul	12 HRS	0	1	0	1
GGSN				GGSN				GGSN									
latest (26 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)						
26th June	14 HRS	500	502	497	497	30th June	22 HRS	0	0	0	0	02-Jul	13 HRS	0	2	0	2
26th June	15 HRS	746	748	751	751	1st Jul	00 HRS	0	7	0	5						
Old SSD pre enabling heartbeat timer				Old SSD pre enabling heartbeat timer				Old SSD pre enabling heartbeat timer									
Date	Time	10.10.10.6	X3MDConnDown	X3MDConnUP	Date	Time	10.10.10.6	X3MDConnDown	X3MDConnUP	Date	Time	10.10.10.6	X3MDConnDown	X3MDConnUP			
4th June	15 HRS		577	578	1st Jul	1 HRS	0	4	0	4							
4th June	16 HRS		1487	1490	1st Jul	2 HRS	0	0	0	0							
4th June	17 HRS		417	1490	1st Jul	3 HRS	0	0	0	0							

Trends of SNMP traps post Workaround:

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 (X3MDCConnUp) 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 (X3MDCConnUp) 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 (X3MDCConnUp) 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 (X3MDCConnUp) 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 (X3MDCConnUp) 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 (X3MDCConnUp) 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 (X3MDCConnUp) 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

**Here is the status of the traps last observed, and note that no new traps get generated.**

```
[local]GGSN# show snmp trap statistics verbose | grep X3MDCConn
```

Thursday July 21 12:36:38 IST 2022

X3MDCConnDown	12018928	0	9689294	2022:07:05:11:36:23
X3MDCConnUp	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