

Resolución de problemas de trampas X3MDConnDown y X3MDConnUp observadas en PGW

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Problema](#)

[Comandos usados](#)

[Solución](#)

Introducción

Este documento describe el proceso para identificar la causa de las trampas X3MDConnDown y X3MDConnUp en Cisco Packet Data Network Gateway (PGW) después de la actualización de 21.18.17 a 21.25.8 en grandes cantidades.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- StarOS/PGW
- Conocimiento de la interfaz y funcionalidad X1, X2 y X3
- Conocimiento del establecimiento de TCP para X3

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router de servicios de agregación (ASR) 5500 de PGW
- Versiones 21.18.17.79434 y 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La solución Lawful Interception tiene tres interfaces discretas entre el elemento de red y el servidor de mediación para proporcionar información de aprovisionamiento, datos de llamadas (señal) y contenido de llamadas (medios). Estas interfaces se crean después de establecer la conexión entre la función de entrega (DF) del servidor de mediación XCIPIO y la función de acceso (AF) del elemento de red. La interfaz del servidor de mediación con la agencia de interceptación legal está estandarizada. Las interfaces entre AF y DF se definen como:

- Interfaz X1 o INI-1 para destinos de aprovisionamiento
- Interfaz X2 o INI-2 para proporcionar información de señalización para el destino
- Interfaz X3 o INI-3 para proporcionar medios o contenido de llamadas para el destino

Donde la interfaz X está definida por el estándar 3GPP mientras que INI está definido por el estándar ETSi.

Problema

Después de la actualización del nodo de 21.18.17 a 21.25.8, una alarma comenzó a venir para **X3MDCConnDown** y **X3MDCConnUp** a granel (alrededor de 3000 en una hora).

Formato de trampa:

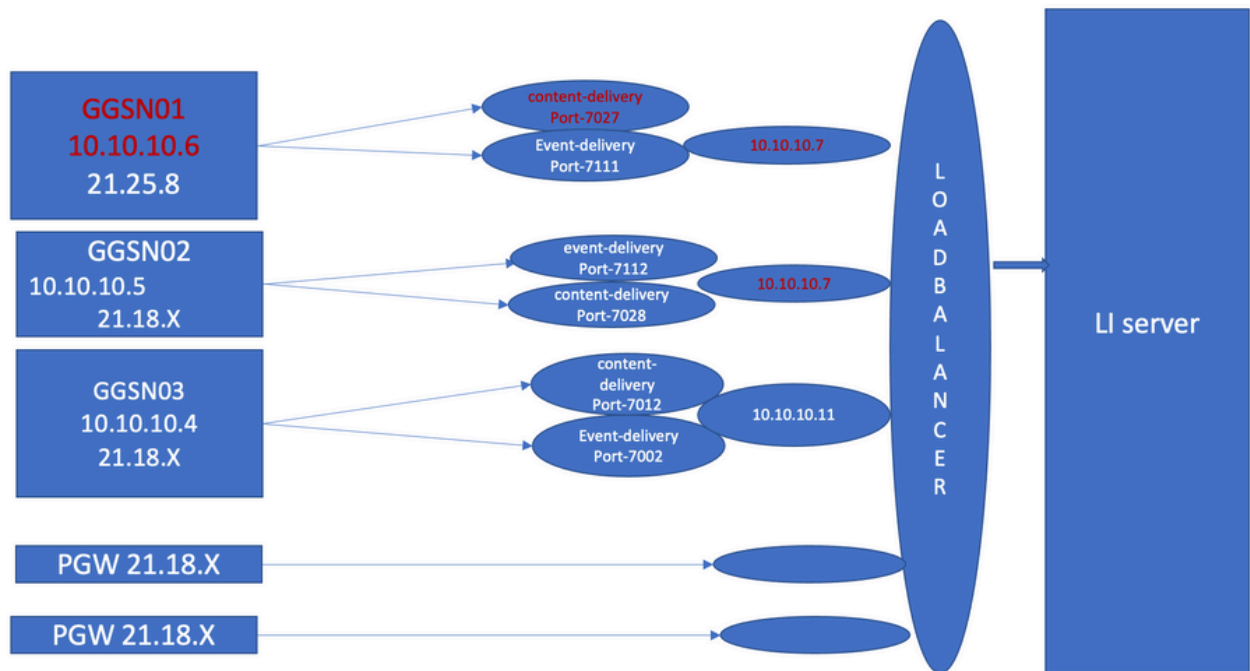
Mon Jul 04 00:44:15 2022 Internal trap notification 1422 (X3MDCConnDown) TCP connection is down. Context Id:8, Local IP/port:10.10.10.1/41833 and Peer IP/port: x.x.x.x/7027 with cause: LI X3 CALEA Connection Down

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

Detalles de trampa en 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		

El problema se resalta en rojo en esta imagen:



Pasos para la resolución de problemas:

1. Verifique los servicios hacia el servidor LI, no encontrará ningún impacto.
2. Los archivos LI se pueden transferir al servidor LI.
3. El ping y el traceroute se encontraron en el servidor LI.
4. No se ha observado latencia ni caída de paquetes.
5. Cuando intenta capturar el TCPdump hacia el servidor LI, los paquetes unidireccionales se capturan en TCPdump para el nodo problemático.

Compárelo con el nodo de trabajo y verá el mismo comportamiento.

1. Cuando crea un puerto diferente en el servidor LI, observa que el problema persiste.
2. Cuando crea otro servidor y puerto de prueba de LI, observa la misma alarma en el nodo de soporte GPRS de la puerta de enlace (GGSN).
3. Cuando captura los seguimientos adicionales, como el seguimiento NPU-PAN, los comandos show y los registros de depuración, observa que FIN ACK proviene del servidor LI justo después del SYN del PGW y esto da como resultado Traps **X3MDConnDown** y **X3MDConnUp**.
4. Según el equipo de ingeniería, la versión 21.25.8 reconoce el FIN ACK y genera la alarma **X3MDConnDown** y a continuación, **X3MDConnUp**. Que no se ve en las versiones anteriores a 21.18.17.
5. Se ha habilitado un **temporizador de latidos de solución alternativa (1m)** en el servidor GGSN y LI publicar que el **X3MDConnDown** y **X3MDConnUp** alarma está en control. Se reduce de alrededor de 3000 a 100 por 1 día.
6. El nodo se controla durante 2 semanas y el **X3MDConnDown** y las alarmas **X3MDConnUp** estaban bajo control.

Comandos usados

1. A partir de estos comandos, los archivos LI se transfieren correctamente al servidor LI. No hay ningún problema con la conexión TCP al servidor LI.

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

Por ejemplo:

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

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

```
Username : -
```

```
ip-address : XXXXXXXXX
```

```
msid/imsi : XXXXXXXXXXXX
```

```
msisdn : XXXXXXXXX
```

```
imei/mei : XXXXXXXX
```

```
session : Session Present
```

```
service-type : pgw
```

```
pdhir : Disabled
```

```
li-context : llictx
```

```
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
```

Estos comandos necesitan acceso LI admin para ver los resultados completos:

```
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. Recopile estos registros de nivel de depuración:

```
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
```

Aquí puede ver cómo cambia la información de puerto si no es estable.

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

3. Entre en el modo oculto y vaya a la tarea Vector Packet Processing (VPP) para comprobar si los paquetes vienen para reconocimiento FIN (ACK).

```
[lictx]GGSN# debug shell
```

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

```
vpp#show hsi sessions
```

Por ejemplo:

```
[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 se puede habilitar bajo el comando test después de habilitar los logs de debug.

```
show clock
```

```
show dhost sockets
```

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

5. Recopile los detalles del soporte Show.

6. Recopile el seguimiento de NPU-PAN para reconocer que el paquete tiene un conexión TCP exitosa con el servidor LI.

Para desactivar:

```
#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
```

Este comando podría detener el seguimiento de panorámica de NPU, por lo que debe volver a configurarse para la siguiente recopilación.

```
#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
```

Ejemplo de seguimiento de 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

Solución

Habilite el tiempo de espera de mensajes de latido a 1 minuto en PGW y XX.XX.XX.147 (Servidor LI) con este comando:

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

Suponga que FIN ACK viene justo después de SYN del servidor LI. En ese caso, PGW no considera que una interfaz X3 esté inactiva porque el latido está habilitado 1 min en PGW y habilitado en el servidor LI, lo que es una indicación de que la conexión X3 está ACTIVA cuando el latido está presente. Por lo tanto, las alarmas se reducen para X3MDCConnDown y X3MDCConnUp.

Análisis de trampas antes y después de 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)				
		X3MDCConnDown	X3MDCConnUP	X3MDCConnDown	X3MDCConnUP		X3MDCConnDown	X3MDCConnUP	X3MDCConnDown	X3MDCConnUP		X3MDCConnDown	X3MDCConnUP	X3MDCConnDown	X3MDCConnUP		
29th June	8 HRS	1	17	1	14	30th June	00 HRS	7	43	4	51	01-Jul	13 HRS	0	1	0	0
29th June	9 HRS	1	9	1	8	30th June	01 HRS	0	2	0	2	01-Jul	14 HRS	0	8	0	8
29th June	10 HRS	1	7	2	6	30th June	2 HRS	0	0	0	0	01-Jul	15 HRS	0	1	0	1
29th June	11 HRS	17	23	14	24	30th June	3 HRS	0	4	0	4	01-Jul	16 HRS	0	1	0	1
29th June	12 HRS	0	4	0	4	30th June	4 HRS	0	0	0	0	01-Jul	17 HRS	0	1	0	1
29th June	13 HRS	0	4	0	4	30th June	5 HRS	0	2	0	2	01-Jul	18 HRS	0	4	0	4
29th June	14 HRS	0	4	0	3	30th June	6 HRS	0	8	0	7	01-Jul	19 HRS	0	0	0	0
29th June	15 HRS	0	22	0	21	30th June	7 HRS	0	2	0	3	01-Jul	20 HRS	0	0	0	0
29th June	16 HRS	1	24	0	21	30th June	8 HRS	2	20	2	19	01-Jul	21 HRS	0	1	0	1
29th June	17 HRS	0	5	0	6	30th June	9 HRS	1	8	1	8	02-Jul	01 HRS	0	5	0	4
29th June	18 HRS	0	0	0	0	30th June	10 HRS	0	1	0	1	02-Jul	2 HRS	0	0	0	0
29th June	19 HRS	0	5	0	6	30th June	11 HRS	0	1	0	1	02-Jul	3 HRS	0	1	0	1
29th June	20 HRS	0	5	0	5	30th June	12 HRS	0	0	0	0	02-Jul	4 HRS	0	2	0	2
29th June	21 HRS	0	2	0	2	30th June	13 HRS	0	0	0	0	02-Jul	5 HRS	0	8	0	8
29th June	22 HRS	5	16	4	16	30th June	14 HRS	0	0	0	0	02-Jul	6 HRS	0	1	0	1
29th June	23 HRS	0	16	0	8	30th June	15 HRS	0	1	0	1	02-Jul	7 HRS	0	0	0	0
30th June	00 HRS	7	44	4	51	30th June	16 HRS	1	18	1	16	02-Jul	8 HRS	0	0	0	0
Total		33	207			30th June	17 HRS	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)				
		X3MDCConnDown	X3MDCConnUP	X3MDCConnDown	X3MDCConnUP		X3MDCConnDown	X3MDCConnUP	X3MDCConnDown	X3MDCConnUP		X3MDCConnDown	X3MDCConnUP	X3MDCConnDown	X3MDCConnUP		
28th June	14 HRS	462	496	443	466	30th June	18 HRS	0	2	0	2	02-Jul	10 HRS	0	0	0	0
28th June	15 HRS		322		280	30th June	19 HRS	0	1	0	1	02-Jul	11 HRS	0	0	0	0
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)				
		X3MDCConnDown	X3MDCConnUP	X3MDCConnDown	X3MDCConnUP		X3MDCConnDown	X3MDCConnUP	X3MDCConnDown	X3MDCConnUP		X3MDCConnDown	X3MDCConnUP	X3MDCConnDown	X3MDCConnUP		
26th June	14 HRS	500	502	497	497	30th June	20 HRS	1	7	1	7	02-Jul	12 HRS	0	1	0	1
26th June	15 HRS	746	748	751	751	30th June	21 HRS	0	0	0	0	02-Jul	13 HRS	0	2	0	2
Old SSD pre enabling heartbeat timer					Old SSD pre enabling heartbeat timer					Old SSD pre enabling heartbeat timer							
Date	Time	10.10.10.6			Date	Time	10.10.10.6			Date	Time	10.10.10.6					
		X3MDCConnDown	X3MDCConnUP				X3MDCConnDown	X3MDCConnUP				X3MDCConnDown	X3MDCConnUP				
4th June	15 HRS	577	578		1st jul	00 HRS	0	7	0	5	01-Jul	00 HRS	0	0	0	0	
4th June	16 HRS	1487	1490		1st jul	1 HRS	0	4	0	4	01-Jul	1 HRS	0	4	0	4	
4th June	17 HRS	417	1490		1st jul	2 HRS	0	0	0	0	01-Jul	2 HRS	0	0	0	0	
					1st jul	3 HRS	0	0	0	0	01-Jul	3 HRS	0	4	0	4	
					1st jul	4 HRS	0	4	0	4	01-Jul	4 HRS	0	4	0	4	
					1st jul	5 HRS	0	4	0	4	01-Jul	5 HRS	0	4	0	4	
					1st jul	6 HRS	0	5	0	6	01-Jul	6 HRS	0	5	0	6	
					Total		31	152									

Tendencias de las trampas SNMP posteriores Solución alternativa:

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: 10.10.10.6/7027with cause: LI X3 CALEA Connection Down

Mon Jul 04 11:13:20 2022 Internal trap notification 1422 (X3MDCConnDown) 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 (X3MDCConnDown) 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

Este es el estado de las trampas observadas por última vez, y observe que no se generan trampas nuevas.

```
[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