

Prepared (Subject resp) ZGRIOLG Olga Grishina		No. 24/1543-ANA 901 37 Uen		
Approved (Document resp) BDGSGHH [Hans Fernqvist]	Checked	Date 2019-04-11	Rev D	Reference

**SS7 CAF SCTP IP Path is Down**

**Contents**

1	Overview	2
1.1	Description	2
2	Procedure	2

Prepared (Subject resp) ZGRIOLG Olga Grishina		No. 24/1543-ANA 901 37 Uen		
Approved (Document resp) BDGSGHH [Hans Fernqvist]	Checked	Date 2019-04-11	Rev D	Reference

## 1 Overview

**Note:** This alarm is deprecated.

### 1.1 Description

Normally this is a non-fatal alarm; SCTP will use other paths in the association for communicating with the remote peer. SCTP will automatically make new attempts to make this IP path available.

The alarm is issued when one of the SCTP IP paths become inactive, unavailable or unreachable.

Major type	193
Minor type	1586601228
MO Class	N/A
Source	RemoteAddress=<*>,LocalAddress=<*>,FEID_Association=<*>,AssociationID=<*>,Sctp.InstanceID=<*>
Specific Problem	SS7 CAF Sctp IP Path Is Down
Severity	SEVERITY_WARNING
Additional Text	Sctp IP Path Is Down

Path becomes inactive due to:

- many retransmissions. The number of retransmission exceeds Path.Max.Rtx or Peer.Max.Rtx and all IP paths in SCTP path become inactive in this case;
- there are no HEARTBEAT\_ACKs during Initial Path Probing.

Path becomes unreachable when during the Unreachable IP Paths Detecting procedure:

- there are no HEARTBEAT\_ACKs (path Unreachable IP Paths Detecting Error Counter becomes equal to the association property Number of Attempts to Probe Unreachable IP Paths);
- ICMP message "Destination Unreachable Message" is received in response to the sent HEARTBEAT.

Path becomes unavailable when local IP address unavailable, and in this case t3counter property is set by SCTP to the maximum value.

## 2 Procedure

### Prerequisites:

- Alarm is raised.

Prepared (Subject resp) ZGRIOLG Olga Grishina		No. 24/1543-ANA 901 37 Uen		
Approved (Document resp) BDGSGHH [Hans Fernqvist]	Checked	Date 2019-04-11	Rev D	Reference

**Steps:**

- 1 Identify IPs related to the path from the alarm (LocalAddress, RemoteAddress).

- 2 Identify path status (inactive, unavailable or unreachable) using SM CLI:

```
ssh user@<SC hostname>

ss7caf-sm-cli

cli> STNFO: LIP="<LocalAddress>", RIP="<RemoteAddress>", ToFetch="1551";
```

- 3 Locate the issue by steps below and try to solve it:

- 3.1 If status of IP link is active but alarm is raised, contact the next level of maintenance support;

- 3.2 If status of IP link is inactive or unreachable it means that there is problem with remote side, check:

- 3.2.1 if traffic is sent to the network (local network settings, firewall etc.);

- 3.2.2 if the traffic can reach the remote side (network configuration between the nodes, routers, etc.);

```
ping <remote IP address>

traceroute <remote IP address>
```

- 3.2.3 if remote side can receive and send acknowledgements (network configuration on remote side);

- 3.2.4 network configuration on local side. Check the value of path t3counter, Path.Max.Rtx and Assoc.Max.Rtx using SM CLI:

```
ssh user@<SC hostname>

ss7caf-sm-cli

cli> STNFO: LIP="<LocalAddress>", RIP="<RemoteAddress>", ToFetch="1547";
cli> STNFO: LIP="<LocalAddress>", RIP="<RemoteAddress>", ToFetch="2094";
cli> STNFO: LIP="<LocalAddress>", RIP="<RemoteAddress>", ToFetch="2060";
```

If value of path t3counter exceeds the Path.Max.Rtx, try to set Path.Max.Rtx to recommended value (Assoc.Max.Rtx) if it different.

If value of path t3counter is not exceeds the Path.Max.Rtx, check the peer. Get the value of peer t3counter and Peer.Max.Rtx:

```
cli> STNFO: LIP="<LocalAddress>", RIP="<RemoteAddress>", ToFetch="1281";
cli> STNFO: LIP="<LocalAddress>", RIP="<RemoteAddress>", ToFetch="1282";
```

If value of peer t3counter exceeds the Peer.Max.Rtx, try to set Peer.Max.Rtx to recommended value (Assoc.Max.Rtx) if it is different.

- 3.3 If status is unavailable it means problems with local IP address. Use the Sctp.InstanceID and LocalAddress from the alarm and perform:

Prepared (Subject resp) ZGRIOLG Olga Grishina		No. 24/1543-ANA 901 37 Uen		
Approved (Document resp) BDGSGHH [Hans Fernqvist]	Checked	Date 2019-04-11	Rev D	Reference

3.3.1 identify the corresponding host by checking Sctp.InstanceID value in SM CLI:

```
ssh user@<SC hostname>  
  
ss7caf-sm-cli  
  
cli> procp
```

and find which PL SCTP\_FEP:<Sctp.InstanceID> belongs to;

3.3.2 log on via ssh to host and check IP interface on OS level using the linux commands:

```
ssh user@<PL hostname>  
  
ip addr  
  
ifconfig
```

3.3.3 check that eVIP is available using the following command:

```
systemctl status evip
```

or via eVIP CLI:

```
evip-cli  
  
EVIP> show evip-status
```

- 4 If after you actions the alarm is persistent contact the next level of maintenance support.