

Configuration of Supervised Gateways for IPv6-only with OSPF

Ericsson Service-Aware Policy Controller

OPERATING INSTRUCTIONS

Copyright

© Ericsson España, S.A., 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Configuration of Supervised Gateways for IPv6-only with OSPF Introduction	1
1.1	Configuration of Supervised Gateways for IPv6-only with OSPF Prerequisites	1
2	Configuration of Supervised Gateways	2
2.1	IPv6 Link-local Addresses Retrieval Procedure	2
2.2	Supervised Gateway Creation	3





1 Configuration of Supervised Gateways for IPv6-only with OSPF Introduction

This operating instruction is applicable to both PNF and VNF deployments for IPv6-only scenarios with OSPF configured.

This operating instruction is not applicable to IPv6-only with static routing, IPv4 or dual stack.

As OSPFv3 protocol works with IPv6 interfaces having only link-local IPv6 addresses (valid within the network segment), and interfaces get link-local IPv6 addresses automatically, these addresses are not known beforehand.

Since eVIP component considers a configured gateway "available" if and only if the eVIP FEE has a default route via that address, and when using IPv6 in an OSPF scenario the ABR injects only default routes into the OSPF area by using the link-local address instead of using the customer IPv6 unique local address (ULA) configured, if supervised gateways were automatically configured following the customer IP plan (using ULAs), an alarm per FEE per supervised gateway configured were always present in the system, as the injected default route and the configured supervised gateway wouldn't match ever.

To avoid this situation and get the alarm properly raised, the manual configuration of these supervised gateways is needed.

1.1 Configuration of Supervised Gateways for IPv6-only with OSPF Prerequisites

This section provides the prerequisites, which must be addressed before using the procedure.

Conditions

The following conditions must apply:

- The operator must be familiar with IPv6, OSPFv3, eVIP common component, COM command line interface, switch/router configuration.
- The deployment scenario is IPv6-only with OSPF configured.
- The operator must have access to the following, depending on the deployment type, to be able to retrieve link-local addresses from IPv6 interfaces involved in OSPFv3 connectivity:
 - PNF:
 - BSP 8100: DMX interface.



- NSP 6.1: gateway routers connected to the FEE (frontal interfaces), per type of traffic configured.
- VNF: gateway routers connected to the FEE, per type of traffic configured.
- The SAPC accessible. The OAM virtual IP address to access the SAPC and the password for sapcadmin and root users are known.

2 Configuration of Supervised Gateways

2.1 IPv6 Link-local Addresses Retrieval Procedure

To retrieve the link-local addresses from IPv6 interfaces involved in OSPFv3 connectivity, the following steps must be followed, depending on the type of deployment.

Attention!

For any other type of involved routers, follow the steps using the proper equivalent commands, PNF BSP 8100 commands are specified as examples.

1. Access the gateway router CLI.

For PNF BSP 8100, execute:

```
External Machine> ssh -p 2024 advanced@<DMX>
```

2. Retrieve the virtual routers used for the SAPC connectivity.

For PNF BSP 8100, note down the routerId of the VRs present defined in the system by executing:

```
DMX:> show-table ManagedElement=1,Transport=1 -m Router -p  
routerId -c routerId=~"0-2(6|8)-(om|sig)"
```

3. For each VR obtained in Step 2, note down the area ID and OSPF area ID attributes.

For PNF BSP 8100, write down the areaId and ospfAreaId values returned executing the following command:



```
DMX:> show-table ManagedElement=1,Transport=1,Router=<routerId>
>,OspfV3=1,AFIPv6Uc=1 -m Area -c areaId=~sapc
```

Result:

```
=====
| routerId                |
=====
| 0-26-om_cn_sp           |
| 0-26-sig_cn_1_sp       |
| 0-26-sig_data_1_sp     |
| 0-28-om_cn_sp           |
| 0-28-sig_cn_1_sp       |
| 0-28-sig_data_1_sp     |
=====
```

4. Per OSPF area returned in Step 3, per VR obtained in Step 2, retrieve the interfaces of the VR involved in that OSPFv3 area.

For PNF BSP 8100: per <areaId> area, per <routerId> VR, write down the **interface** values returned by executing:

```
DMX:> show-table ManagedElement=1,Transport=1,Router=<routerId>
>,OspfV3=1,AFIPv6Uc=1,Area=<areaId> -m Interface -p interface
```

5. For each interface retrieved in Step 4, get the automatically assigned IPv6 link-local address and write it down removing the network size suffix.

For PNF BSP 8100, write down the address value without the network size suffix returned executing:

```
DMX:> show-table <interface> -m AddressIPv6 -p address -c
addressIPv6Id=~DYNAMIC
```

2.2 Supervised Gateway Creation

To create the supervised gateway objects to get the alarms properly generated, follow the steps below.

1. Access the SAPC COM CLI for administration node operations:

```
External Machine> ssh sapcadmin@<OAM_VIP> -p <COM_port> -t -s
cli
```

where <COM_port> is the COM port, normally 830.

2. Navigate and show the eVIP ALBs list:


```
>ManagedElement=1,Transport=1,Evip=1,EvipAlbs=1
(EvipAlbs=1)>show
EvipAlbs=1
  EvipAlb=<alb1>
  EvipAlb=<alb2>
```



3. Are all **<alb>** elements retrieved in Step 2 already processed?

Yes: go to Step 11.

No: execute the following command and go to Step 4:

```
(EvipAlb=<alb>)>up  
(EvipAlbs=1)>
```

4. Navigate to the first **<alb>** obtained in Step 2 not processed yet and list the FEE elements as follows:

```
(EvipAlbs=1)>EvipAlb=<alb>  
(EvipAlb=<alb>)>show EvipFees=1  
EvipFees=1  
    EvipFee=<fee1>  
    EvipFee=<fee2>
```

5. Are all **<fee>** elements retrieved in Step 4 already processed?

Yes: go to Step 3.

No: execute the following command and go to Step 6:

```
(EvipFee=<fee>)>up  
(EvipFees=1)>up  
(EvipAlb=<alb>)>
```

6. Navigate to the first **<fee>** retrieved in Step 4 not processed yet and show the OSPFv3 area ID as follows:

```
(EvipAlb=<alb>)>EvipFees=1,EvipFee=<fee>  
(EvipFee=<fee>)>show EvipRoutingSetup=ospfv3,EvipParam=area,value  
value="<ospfAreaId>"
```

7. Using the OSPF area **<ospfAreaId>** retrieved in Step 6 and matching it to the **<ospfAreaId>** IDs obtained in Step 3 of Section 2.1 on page 2, the matching **<areaId>** in the proper virtual router is found.

Using this **<areaId>** to get the interfaces **<interface>** returned in Step 4 of Section 2.1 on page 2, and using the information retrieved in Step 5 of Section 2.1 on page 2 for these interfaces, the link-local IPv6 addresses for the interfaces participating as designated routers in the same OSPF area than the current **<fee>** are obtained.

8. Are all designated router IPv6 link-local addresses obtained in step 7 added as supervised gateways for the current **<fee>**?

Yes: go to Step 5.

No: go to Step 9.



9. Using the first designated router link-local IPv6 <address> retrieved in Step 7 not processed yet, an EvipSupervisedRemoteGateway object under <fee> must be created as follows:
(EvipFee=<fee>)>configure
(config-EvipFee=<fee>)>EvipSupervisedRemoteGateway=<address>
(config-EvipSupervisedRemoteGateway=<address>)>commit
(EvipSupervisedRemoteGateway=<address>)>up
(EvipFee=<fee>)>

This object enables the connectivity supervision between the <fee> FEE and the <address> designated router and if any connectivity issue is detected, the eVIP, Gateway Unavailable alarm is raised accordingly.

10. Go to Step 8.
11. Perform a system backup following [Create Backup Operational Instruction](#) document.