

NSP 6.1 Network Configuration Guide

Ericsson Service-Aware Policy Controller

USER GUIDE

Copyright

© Ericsson España S.A. 2017. 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	Introduction	1
1.1	Document Purpose and Scope	1
2	NSP 6.1 Network Configuration Guide Overview	3
2.1	NSP 6.1 Minimal Network Configuration (TSP Legacy)	4
2.2	NSP 6.1 Single Subrack Network Configuration	7
2.3	NSP 6.1 Whole Rack Network Configuration	12
3	NSP 6.1 Networks Allocation	15
3.1	NSP 6.1 DMX Network Allocation	15
3.2	NSP 6.1 VLANs	15
3.3	NSP 6.1 IP Addressing Example	17
3.4	TSP Legacy Considerations	20





List of Tables

Table	Title	Page
1	Collapsed DMX Northbound OAM through SCX logical network settings	15
2	VLANs for One Subrack	15
3	VLANs for Whole Rack	16
4	IPv4 Network and VLAN for SAPC	17
5	Open Shortest Path First (OSPF) Stub Areas	19
6	IP Addresses of External Elements	20
7	Network mapping for TSP Legacy	20





1 Introduction

1.1 Document Purpose and Scope

This document provides information to define the network configuration needed to run the SAPC in a Network Server Platform (NSP).





2 NSP 6.1 Network Configuration Guide Overview

This section provides an overview of the hardware and software components used to configure the SAPC internal and external networks, as well as a general network description.

The configuration described here applies to NSP 6.1 Ericsson Blade System (EBS). For other vendor blade systems similar hardware functional elements must be considered:

— Hardware components

- External routers between the different blades and the external network.
- System Control Switches (SCXs) constitute the cluster backplane.
- Blade system with at least eight blades.

— Software components

- SUSE Linux Enterprise Server, SLES with Kernel-based Virtual Machine (KVM).
- The SAPC software.

A blade system is a hardware system with one complete SAPC running. Each blade has one different role with the following distribution:

- SC-1 and SC-2 are the System Controllers (SC). The Operation and Maintenance (OAM) is done through these blades. These blades are virtualized.
- PL-x is the traffic payloads in the basic scenario. Policy Charging and Control (PCC) deployment traffic (such as Gx, Rx) is handled through these blades. These machines are not virtualized and run directly in the blade hardware.

The blade system can have a variable number of blades. In this network configuration guide, three scenarios are explained. The first scenario is a minimal deployment with eight blades and the OAM is in the SC blades; it is the Ericsson Telecom Server Platform (TSP) Legacy scenario. Then a scenario of one subrack (12 blades) and finally a complete cabinet scenario with three subracks (36 blades). Depending on the number of blades and the delivery needs (external database, geographical redundancy or traffic separation), follow the most adequate scenario. 1-GB interface is needed for internal and external connectivity.

2.1 NSP 6.1 Minimal Network Configuration (TSP Legacy)

In this first scenario, there are eight blades. The fifth and sixth blades are SCs and the other blades are traffic payloads. Each blade has a different role depending on the needs.

2.1.1 System Controller Blades

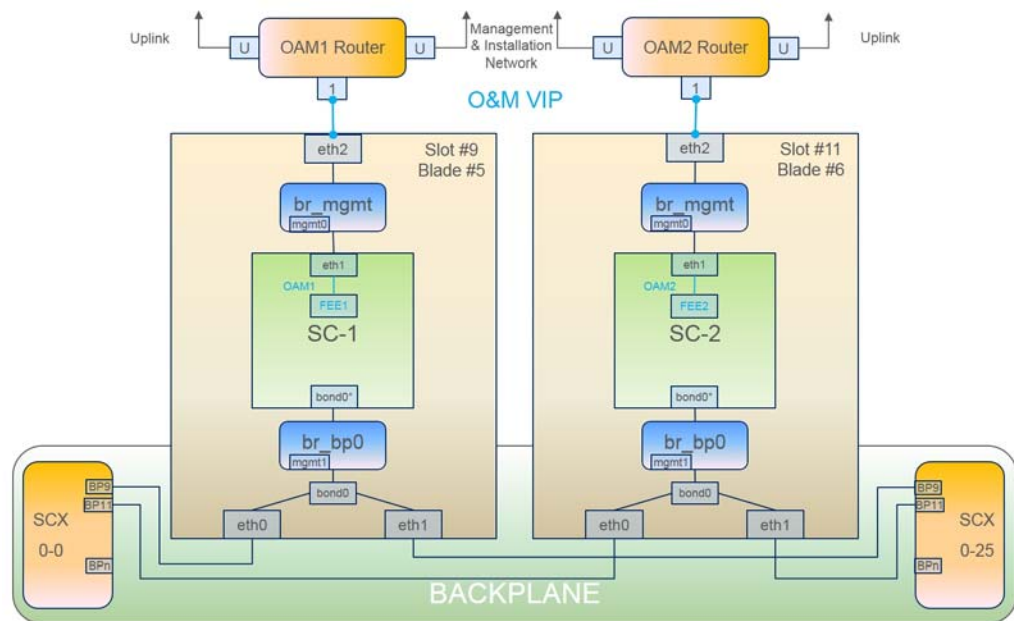


Figure 1 Minimal Configuration.SCs

SCs are virtualized, so virtual bridges are defined.

- Bridge **br_mgmt** is used for management purposes and connects the **eth2** of the virtual machine (VM) with the **eth2** of the physical blades.
- Bridge **br_bp0** is the backplane bridge which connects the first interface of the VMs (**bond0***) with the physical blades through the linux bond (**bond0**) made in the hypervisor between **eth0** and **eth1**.

Attention!

The interface **bond0*** in the VMs is not an actual bond, but a single interface. It has been named like this for convenience.

SCs are connected to the external network through virtual IP (VIP) Front-End Element (FEE). These connections are used for load balancing purposes through a



VIP. For this purpose OAM Virtual Local Area Networks (VLANs) are used. SCs also provide an external OAM IP address independent of the VIP-OAM.

2.1.2 Payload Blades

Traffic payload blades follow different network configuration depending on the customer needs, being these payload blades configured accordingly.

- **PL-3 and PL-4** are used for traffic purposes in this scenario. All external diameter traffic is received through these two.
- In case external database is configured, **PL-3 and PL-4** are used for this purpose.
- In case GeoRed is configured, **PL-7 and PL-8** are used for this purpose.
- In case traffic separation is configured, **PL-3 and PL-4** are used for this purpose.
- Rest of the PLs have no external communication.

Payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1**.

Payloads are connected to the external network through VIP FEE. Four VIPs are defined for Traffic, External Database, GeoRed (Replication), and Traffic Separation in case that traffic exists, and additional FEEs can be defined. These connections are used for load balancing purposes through a VIP.

Traffic, External DB, and Traffic Separation Payload Blades

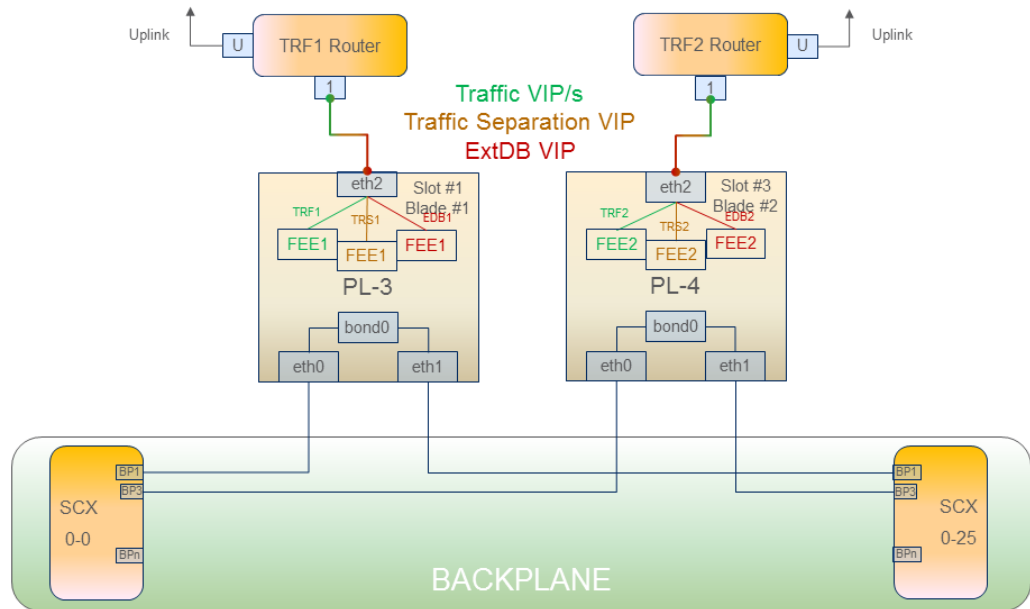


Figure 2 Minimal Configuration. Traffic, External DB, and Traffic Separation Payloads

GeoRed Payload Blades

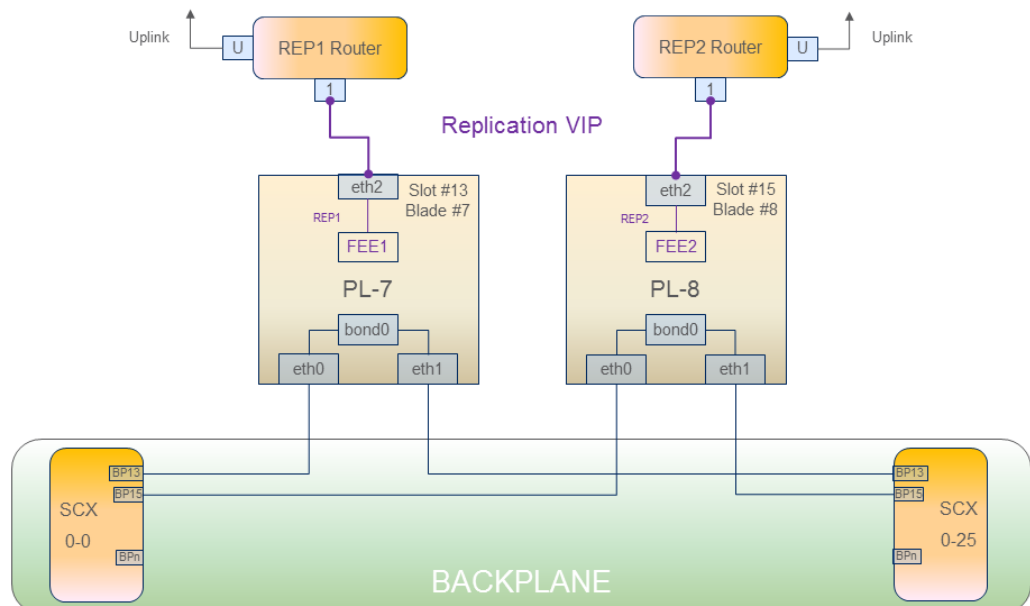


Figure 3 Minimal Configuration. GeoRed Payloads



Remaining Payload Blades

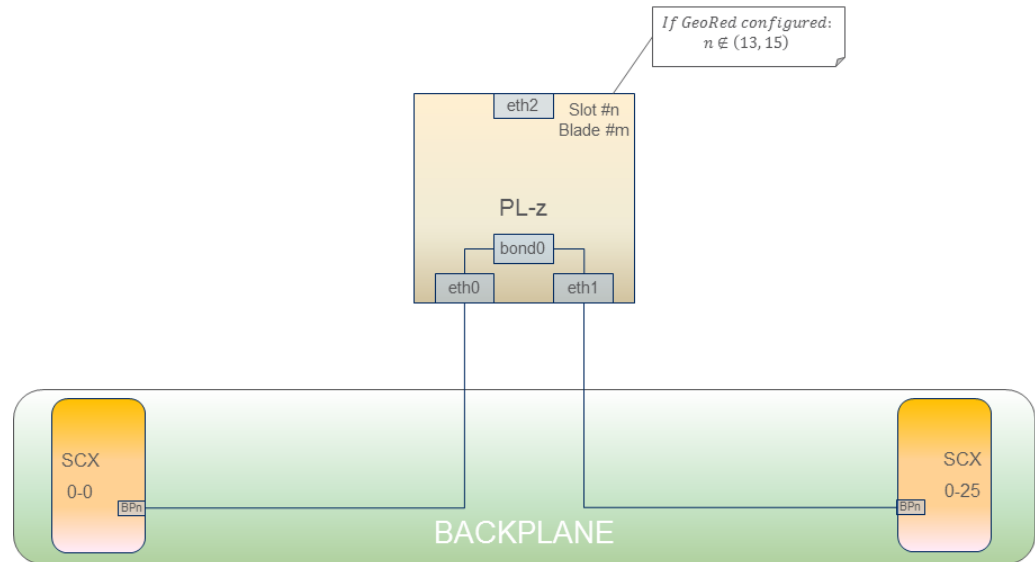


Figure 4 Minimal Configuration. Remaining Payloads

2.2 NSP 6.1 Single Subrack Network Configuration

The fifth and sixth blades are SCs and the other blades are traffic payloads. Each blade has a different role depending on the needs.

2.2.1 System Controller Blades

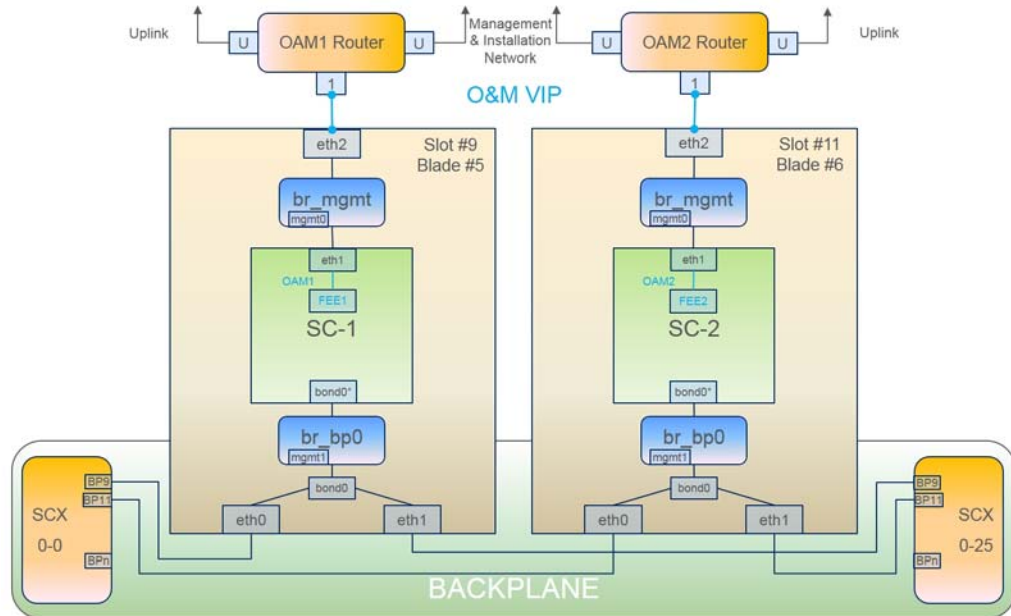


Figure 5 SC in Single Subrack Scenario

SCs are virtualized, so virtual bridges are defined.

- Bridge **br_mgmt** is used for management purposes and connects the **eth2** of the virtual machine with the **eth2** of the physical blades.
- Bridge **br_bp0** is the backplane bridge which connects the first interface of the VMs (**bond0***) with the physical blades through the linux bond (**bond0**) made in the hypervisor between **eth0** and **eth1**.

Attention!

The interface **bond0*** in the virtual machines is not an actual bond, but a single interface. It has been named like this for convenience.

SCs are connected to the external network through VIP FEE. These connections are used for load balancing purposes through aVIP. For this purpose OAM VLANs are used. SCs also provide an external OAM IP address independent of the VIP-OAM.



2.2.2

Payload Blades

Payload blades follow different network configuration depending on the customer needs. This chapter describes a scenario with all functionality. Payload blades are configured according to the customer needs.

- **PL-10 and PL-12** are used for traffic purposes in this scenario. All external diameter traffic is received through these two.
- **PL-9 and PL-11** are used for OAM purposes.
- In case external database is configured, **PL-3 and PL-4** are used for this purpose.
- In case GeoRed is configured, **PL-7 and PL-8** are used for this purpose.
- In case traffic separation is configured, **PL-5 and PL-6** are used for this purpose.
- Rest of the PLs have no external communication.

Payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1**.

Payloads are connected to the external network through VIP FEE. Four VIPs are defined for Traffic, External Database, GeoRed (Replication), and Traffic Separation in case that traffic exists, and additional FEEs can be defined. These connections are used for load balancing purposes through a VIP.

Traffic Payload Blades

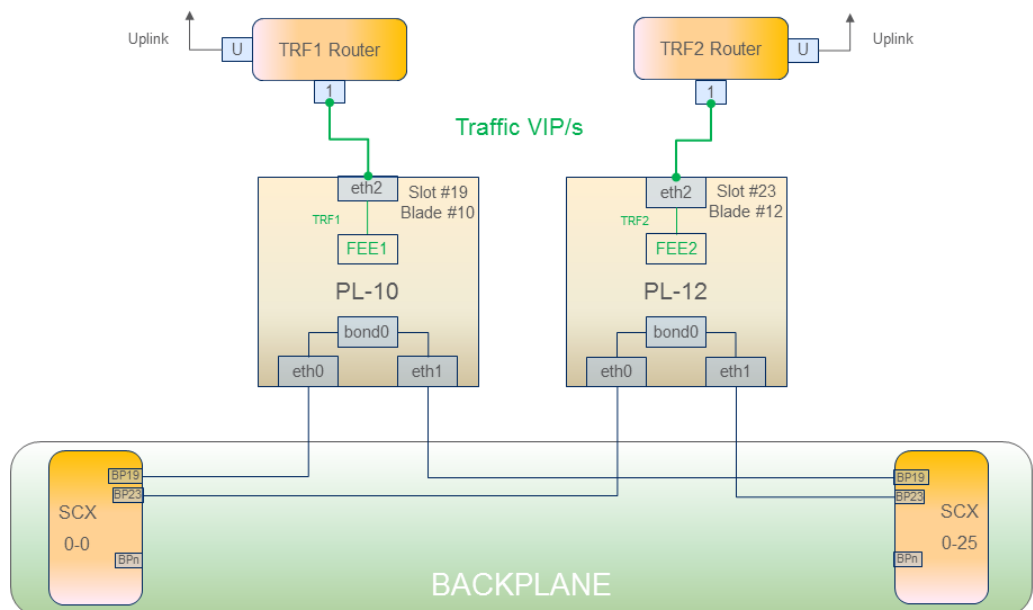


Figure 6 Subrack Configuration. Traffic Payloads



OAM Payload Blades

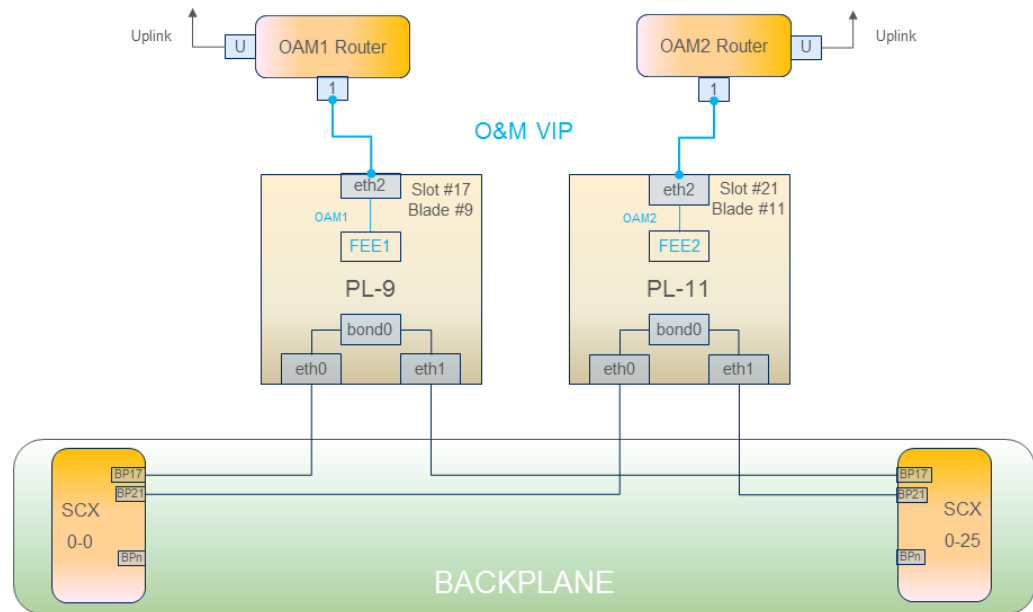


Figure 7 Subrack Configuration. OAM Payloads

External Database Payload Blades

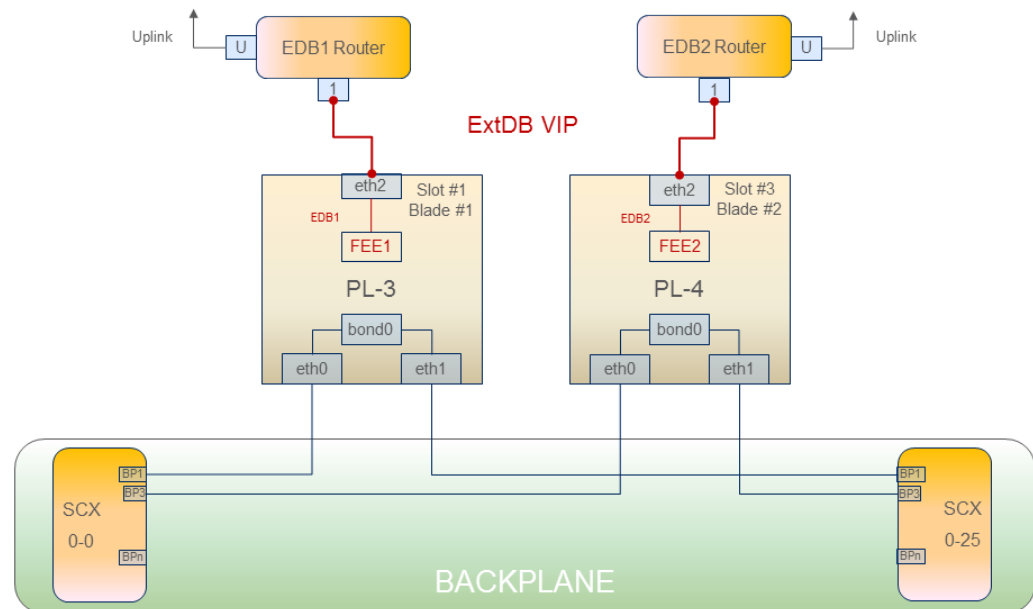


Figure 8 Subrack Configuration. External Database Payloads



GeoRed Payload Blades

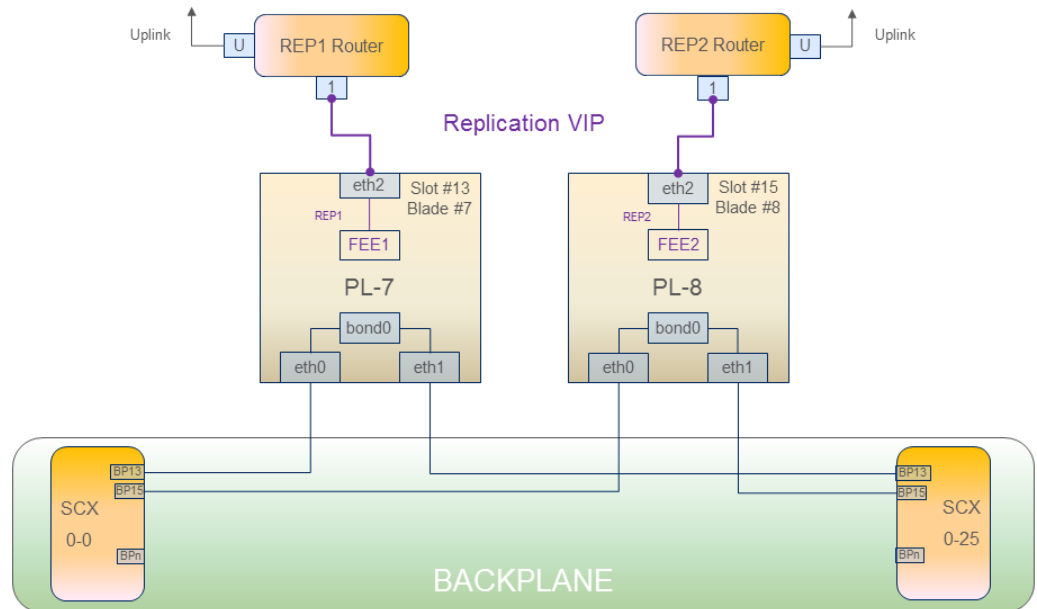


Figure 9 Subrack Configuration. GeoRed Payloads

Traffic Separation Payload Blades

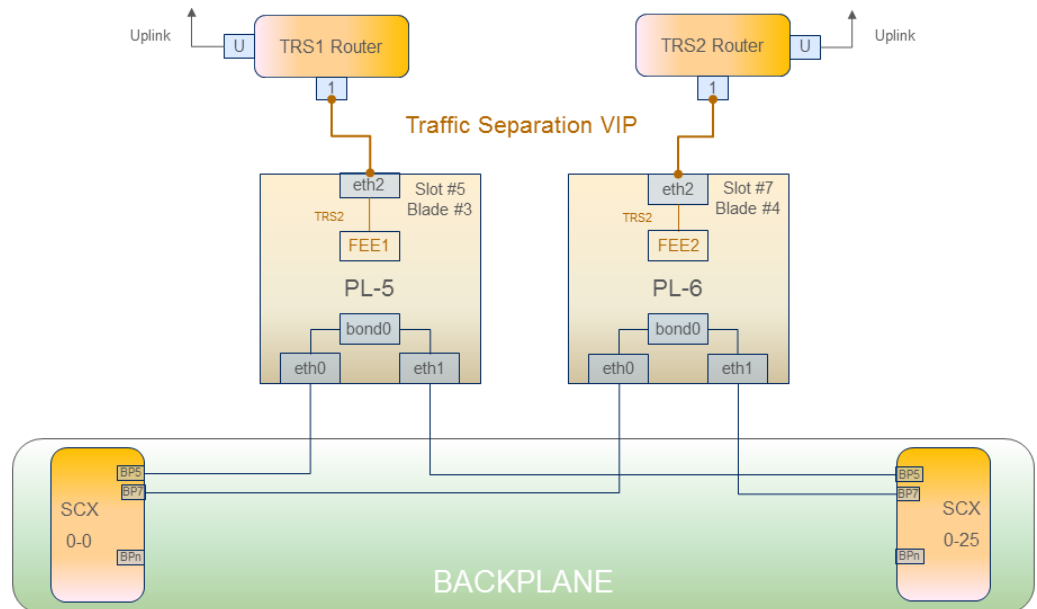


Figure 10 Subrack Configuration. Traffic Separation Payloads



Remaining Payload Blades

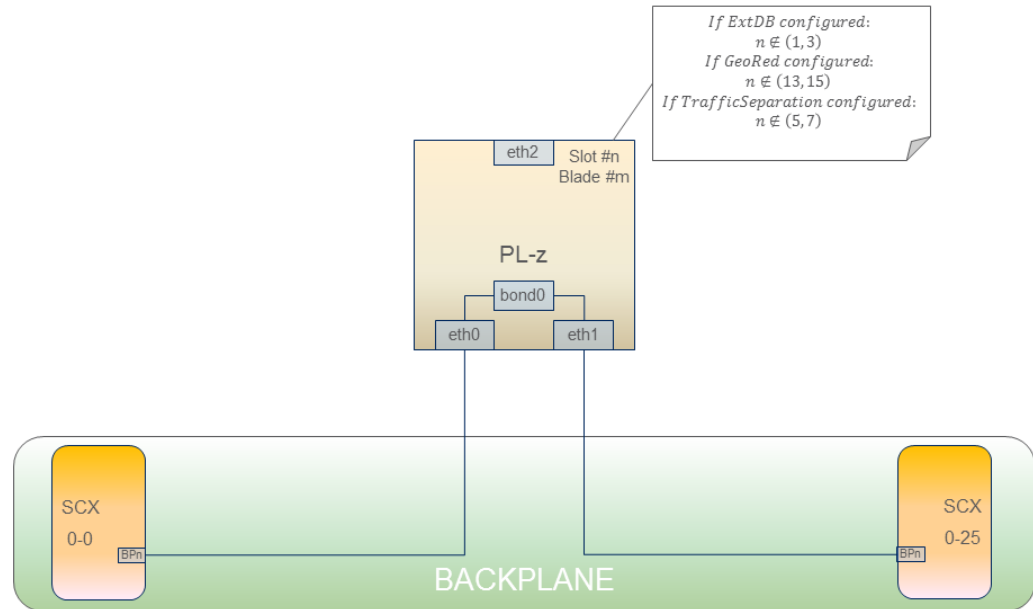


Figure 11 Subrack Configuration. Remaining Payload Blades

Remaining payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1**.

2.3 NSP 6.1 Whole Rack Network Configuration

The fifth and sixth blades are SCs and the other blades are traffic payloads. The installation described in Section 2.2 on page 7 has to be done for the first subrack. In this chapter, additional networking is included for the additional second and third subrack.

Additional FEEs are needed for each type of traffic for the second and third subracks. For a second subrack, in a scenario with External Database, GeoRed, and Traffic Separation, apart from normal diameter traffic, PL-22 and PL-24 are used for Traffic FEEs, PL-15 and PL-16 for External Database FEEs, PL-19 and PL-20 for GeoRed FEEs, and PL-17 and PL-18 for Traffic Separation FEEs. For a third subrack, in a scenario with External Database, GeoRed, and Traffic Separation, apart from normal diameter traffic, PL-34 and PL-36 are used for Traffic FEEs, PL-27 and PL-28 for External Database FEEs, PL-31 and PL-32 for GeoRed FEEs, and PL-29 and PL-30 for Traffic Separation FEEs.

2.3.1 Traffic Blades

Remaining Blades

For all blades, the following extra networking must be done.

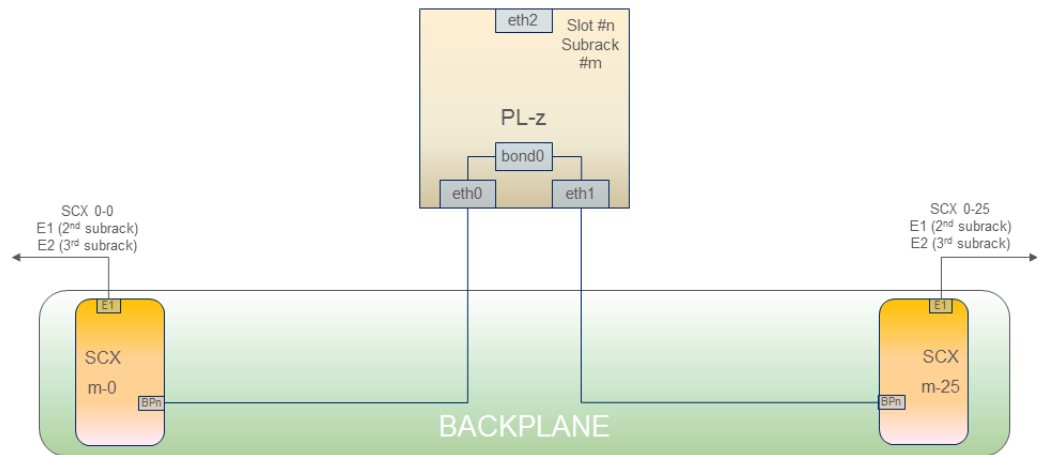


Figure 12 Whole Rack Configuration. All Payloads

Remaining payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1**.

FEE Payload Blades

Additional payload configuration is needed in the new subracks. New FEEs are created in that case as the figure shows.

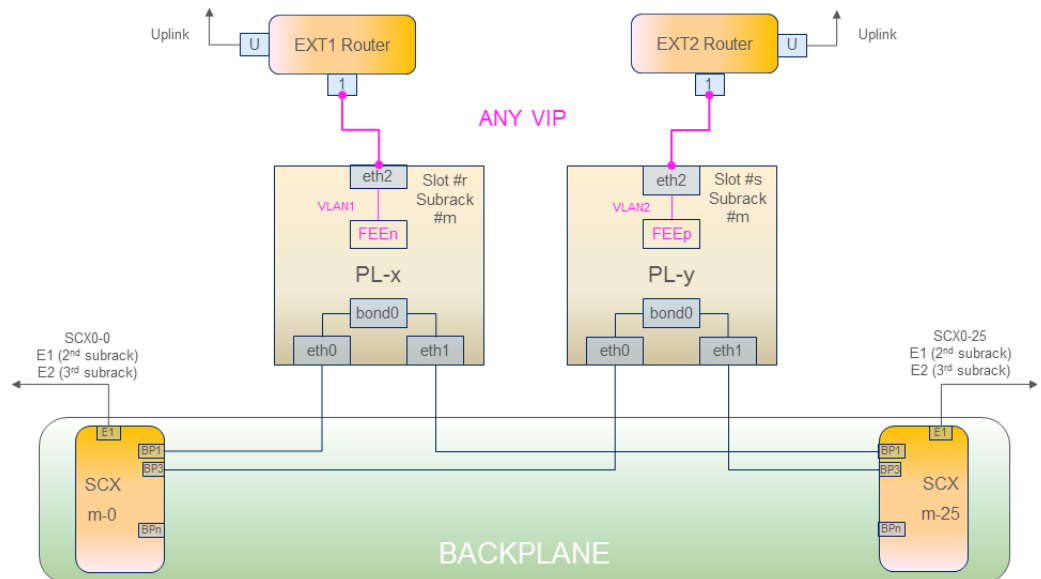


Figure 13 Whole Rack Configuration. FEE Payloads





3 NSP 6.1 Networks Allocation

This section specifies how the SAPC Node is connected to the external network, detailing all the VLANs and networks. Before starting to configure the SAPC Node network, agree with the customer all the details (IP addresses, Network, VLAN Tags, and so on) referenced in this section.

All VLANs are tagged unless explicitly stated.

3.1 NSP 6.1 DMX Network Allocation

Table 1 Collapsed DMX Northbound OAM through SCX logical network settings

Address Type	Name/Tag	Example
Collapsed northbound IP address	%{cnb_net}	172.21.20.186
Collapsed northbound default gateway IP address	%{cnb_defgw}	172.21.20.185
Collapsed northbound network netmask	%{cnb_netmask}	255.255.255.248
Collapsed northbound network VLAN identity	%{cnb_vlanid}	3122
External NTP server for the DMX	%{ntp1_net}	9.9.9.9

3.2 NSP 6.1 VLANs

Table 2 VLANs for One Subrack

VLAN Name	Interface	Ports	Comments
sapc_om2_sp	Blade: mgmt0	N/A	SCs only. Hypervisor Management
sapc_mgmt_sp	Blade: mgmt1 VM: eth1	N/A	SCs only. Service Management
sapc_tipc_pdl	eth0	SCX 0–0: BPn	Left TIPC
sapc_tipc_pdr	eth1	SCX 0–25: BPn	Right TIPC
sapc_om1_sp1	eth2	N/A	VIP Router Link O&M Traffic



VLAN Name	Interface	Ports	Comments
sapc_om1_sp2	eth2	N/A	VIP Router Link O&M Traffic
sapc_sig1_sp1	eth2	N/A	VIP Router Link Signaling Traffic
sapc_sig1_sp2	eth2	N/A	VIP Router Link Signaling Traffic
sapc_sig2_sp1	eth2	N/A	VIP Router Link LDAP Traffic
sapc_sig2_sp2	eth2	N/A	VIP Router Link LDAP Traffic
sapc_sig3_sp1	eth2	N/A	VIP Router Link Replication Traffic
sapc_sig3_sp2	eth2	N/A	VIP Router Link Replication Traffic
sapc_sig4_sp1	eth2	N/A	VIP Router Link Signaling Traffic Rx
sapc_sig4_sp2	eth2	N/A	VIP Router Link Signaling Traffic Rx

Same VLAN configuration for the lower subrack than the single rack configuration, extending it for the lower subrack ports connected to the other subracks. Configuration for extending the lower subrack and configuring the other subracks according to the following tables

Table 3 VLANs for Whole Rack

VLAN Name	Interface	Ports	Comments
sapc_tipc_pdl	eth0	SCX 0-0: E1, E2 SCX m-0: E1	Left TIPC
sapc_tipc_pdr	eth1	SCX 0-25: E1, E2 SCX m-25: E1	Right TIPC
sapc_sig1_sp1	eth2	N/A	VIP Router Link Signaling Traffic
sapc_sig1_sp2	eth2	N/A	VIP Router Link Signaling Traffic
sapc_sig2_sp1	eth2	N/A	VIP Router Link LDAP Traffic



VLAN Name	Interface	Ports	Comments
sapc_sig2_sp2	eth2	N/A	VIP Router Link LDAP Traffic
sapc_sig3_sp1	eth2	N/A	VIP Router Link Replication Traffic
sapc_sig3_sp2	eth2	N/A	VIP Router Link Replication Traffic
sapc_sig4_sp1	eth2	N/A	VIP Router Link Signaling Traffic Rx
sapc_sig4_sp2	eth2	N/A	VIP Router Link Signaling Traffic Rx

3.3 NSP 6.1 IP Addressing Example

Each SAPC Node requires a set of IP addresses agreed with the customer before configuring the SAPC Node.

Table 4 IPv4 Network and VLAN for SAPC

Network Address	Mask	Type	Usage	VLAN ID
192.168.216.0	/27	Private	VIP Router Link for Signaling Traffic	120
192.168.216.32	/27	Private	VIP Router Link for Signaling Traffic	121
192.168.218.0	/29	Private	VIP Router Link for OAM Traffic	130
192.168.218.8	/29	Private	VIP Router Link for OAM Traffic	131
192.168.217.0	/27	Private	VIP Router Link for LDAP Traffic	140



Network Address	Mask	Type	Usage	VLAN ID
192.168.217.32	/27	Private	VIP Router Link for LDAP Traffic	141
192.168.219.0	/27	Private	VIP Router Link for Replication Traffic	150
192.168.219.32	/27	Private	VIP Router Link for Replication Traffic	151
192.168.220.0	/27	Private	VIP Router Link for Signaling Traffic Rx	122
192.168.220.32	/27	Private	VIP Router Link for Signaling Traffic Rx	123
192.168.100.0	/24	Private	System Management Network	138
sapc_hyp_sp_net	/29	Public	Hypervisor Management Network	137
sapc_sig_cn_1_vip	/32	Public	VIP Signaling Address	N/A
sapc_om_cn_vip1	/32	Public	VIP OAM Address	N/A
sapc_om_cn_vip2	/32	Public	VIP Provisioning Address	N/A
sapc_sig_data_1_vip	/32	Public	VIP LDAP Address	N/A
sapc_sig_data_2_vip	/32	Public	VIP Replication Address	N/A
sapc_sig_cn_2_vip	/32	Public	VIP Signaling Rx Address	N/A



Table 5 Open Shortest Path First (OSPF) Stub Areas

Network	Gateways	VLAN	OSPF Area	Comments
192.168.218.0/29	192.168.218.1	130	0.1.1.1	O&M Traffic
192.168.218.8/29	192.168.218.9	131	0.1.1.1	O&M Traffic
192.168.216.0/27	192.168.216.1	120	0.0.1.1	Signaling Traffic
192.168.216.32/27	192.168.216.33	121	0.0.1.1	Signaling Traffic
192.168.217.0/27	192.168.217.1	140	0.0.1.2	LDAP Traffic
192.168.217.32/27	192.168.217.33	141	0.0.1.2	LDAP Traffic
192.168.219.0/27	192.168.219.1	150	0.0.1.3	Replication Traffic
192.168.219.32/27	192.168.219.33	151	0.0.1.3	Replication Traffic
192.168.220.0/27	192.168.220.1	122	0.0.1.4	Signaling Traffic Rx
192.168.220.32/27	192.168.220.33	123	0.0.1.4	Signaling Traffic Rx

Note: In OSPF, a backbone must be defined when routing a packet between two non-backbone areas. The OSPF backbone is the special OSPF Area 0 (written as Area 0.0.0.0, since OSPF Area IDs are typically formatted as IP addresses). The OSPF backbone always contains all Area Border Routers. The backbone is responsible for distributing routing information between non-backbone areas. This is mandatory as VIPs are published to the ABR and thus visible in the backbone only if OSPF Area 0 is defined.

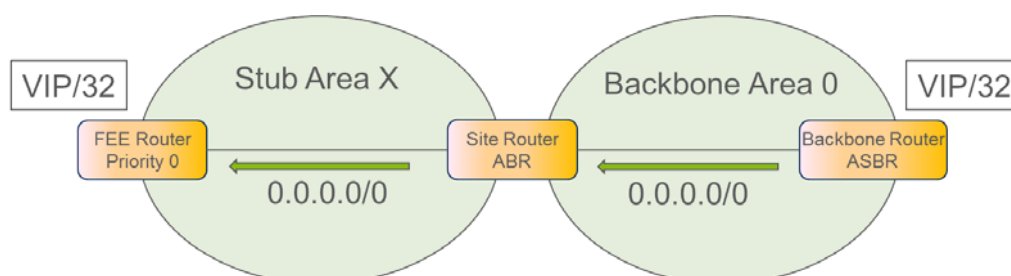


Figure 14 OSPF Backbone Area



3.3.1 NSP 6.1 IP Addresses of External Elements

This section covers all the IP addresses in the customer network that do not belong to the SAPC Node but needed when configuring it.

Table 6 IP Addresses of External Elements

IP Address	Network	Use
<NTP1-SERVER>	<NTP1-NETWORK> / <NTP-NETMASK>	NTP Server
<SNMP1-SERVER>	<SNMP1-NETWORK> / <SNMP-NETMASK>	SNMP Server
<DNS1-SERVER>	<DNS1-NETWORK> / <DNS-NETMASK>	DNS Server

There can be several NTP servers.

3.4 TSP Legacy Considerations

To achieve a maximum reuse of the existing elements, the DMX Collapsed northbound IP address can be one free IP address in subnetwork `sapc_om2_sp`, so that there is no need to provision and route additional networks to the existing ones in TSP configurations.

Table 7 Network mapping for TSP Legacy

TSP Network	PNF Network	Use
I/O Management	<code>sapc_om2_sp</code>	Hypervisor 1 and 2, DMX northbound, SiteRouter1, SiteRouter2 and VRRP
OAM VIP	<code>sapc_om1_sp</code>	eVIP FEE1, eVIP FEE2, SiteRouter1, SiteRouter2
Traffic VIP	<code>sapc_sig1_sp</code>	eVIP FEE1, eVIP FEE2, SiteRouter1, SiteRouter2