

BSP 8100 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	BSP 8100 Network Configuration Guide Overview	3
2.1	BSP 8100 Minimal Configuration. Four Physical Blades	4
2.2	BSP 8100 Single Subrack Configuration. 12 Physical Blades	6
2.3	BSP 8100 Whole Rack Configuration. 36 Physical Blades	11
3	BSP 8100 Networks Allocation	15
3.1	BSP 8100 VLANs	15
3.2	BSP 8100 IP Addressing	19





List of Tables

Table	Title	Page
1	VLANs for One Subrack	15
2	VLANs for Whole Rack	18
3	IPv4 Network and VLAN for BSP Management	19
4	IPv4 Network and VLAN for SAPC	20
5	IP Allocation of Internal Networks for SAPC	25
6	OSPF Stub Areas	25
7	IP Addresses of External Elements	26





1 Introduction

1.1 Document Purpose and Scope

This document provides information to define the hardware, software and network components, and the network configuration needed to run the SAPC in a blades BSP system.





2 BSP 8100 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 BSP 8100 Ericsson Blade System. For other vendor blade systems similar hardware functional elements must be considered:

— Hardware components

- CMXs constitute the cluster 10-GB backplane and work as routers and switches between the different blades and the external network.
- SCXs constitute the cluster 1-GB backplane and work as switches for booting, scaling, and OAM purposes between the different blades and the external network.
- Blade system with at least four blades.

— Software components

- BSP software R10.1.
- SUSE Linux Enterprise Server, SLES with 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 (SCs). The Operation and Maintenance (OAM) traffic is done through these blades. They are virtualized.
- PL-x are the traffic payloads in the basic scenario. PCC deployment traffic (such as Gx, Rx) is handled through these blades. These machines are not virtualized and run directly in the blade hardware.

Attention!

The blade system can have a variable number of blades. In this network configuration guide, three scenarios are explained. A first scenario with four blades, minimum deployment 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. In all scenarios, the 1-GB interfaces are connected to the SCX while the 10-GB interfaces are connected to the CMX.

Refer to SAPC Network Description.

2.1 BSP 8100 Minimal Configuration. Four Physical Blades

In this first scenario, the two first blades are system controllers and the two next blades are traffic payloads.

2.1.1 System Controller Blades

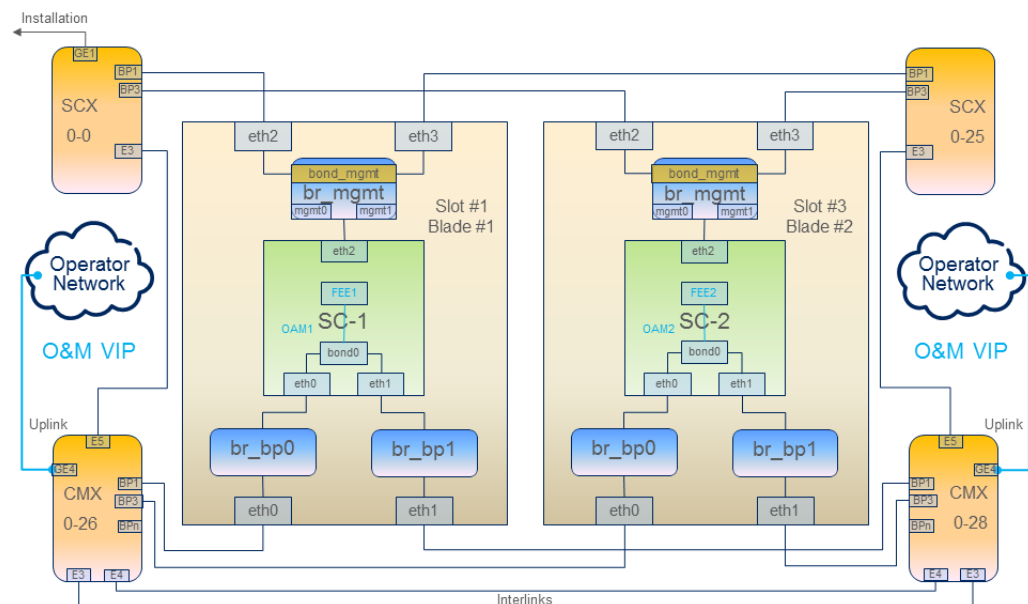


Figure 1 Minimal Configuration. System Controllers

System controllers are virtualized, so virtual bridges are defined.



- Bridge **br_mgmt** is used for management purposes and connects the **eth2** of the Virtual Machines with the **eth2** and **eth3** of the physical blades through a bond to provide High Availability for the 1-GB backplane.
- Bridge **br_bp0** and **br_bp1** are the 10-GB backplane bridges which connect the **eth0** and the **eth1** of the Virtual Machines with the physical blades. A bond is created between these **eth0** and **eth1** interfaces of the Virtual Machines to provide High Availability for the 10-GB backplane.

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

Internal connectivity is done through the 10 GB interfaces connected to both CMX routers (which also provide switching capabilities). Both CMXs are interconnected to achieve High Availability.

2.1.2

Payload Blades

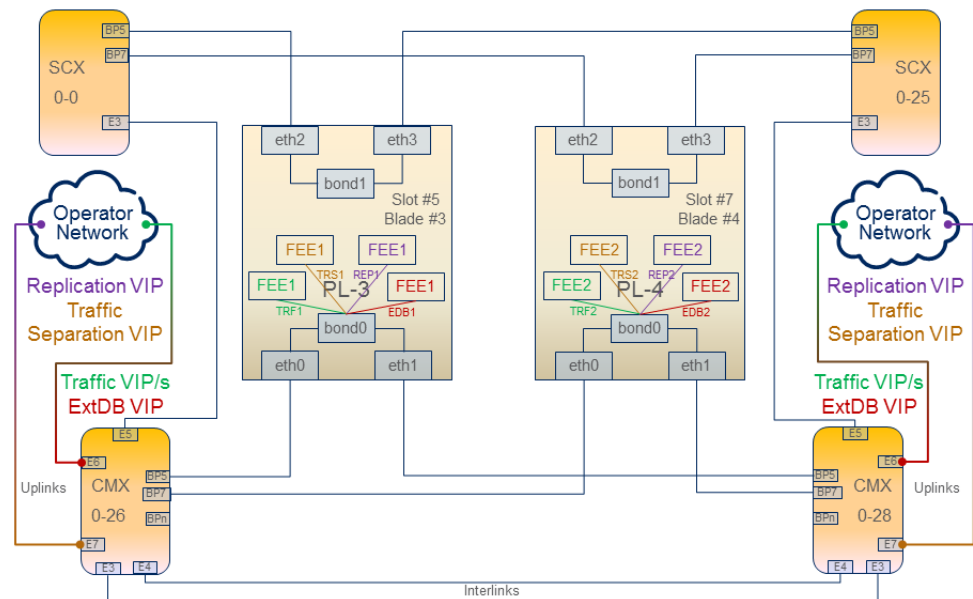


Figure 2 Minimal Configuration. Traffic Payloads

Payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1** to provide High Availability for the 10-GB backplane. Besides, another bond is created between **eth2** and **eth3** to provide High Availability for the 1-GB backplane.

Payloads are connected to the external network through VIP FEEs. 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 virtual IP.



Internal connectivity is done through the 10 GB interfaces connected to both CMX routers (which also provide switching capabilities). Both CMXs are interconnected to achieve High Availability.

2.2 BSP 8100 Single Subrack Configuration. 12 Physical Blades

The two first blades are system controllers and the rest blades are traffic payloads. Each blade has a different role depending on the needs.

2.2.1 System Controller Blades

Configuration applies the same as in Section 2.1.1 on page 4.

2.2.2 Traffic Blades

Traffic payload blades follow different network configuration depending on the customer needs. This chapter describes a scenario with all functionality. Depending on the customer needs, PLs are configured accordingly.

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



Traffic Payload Blades

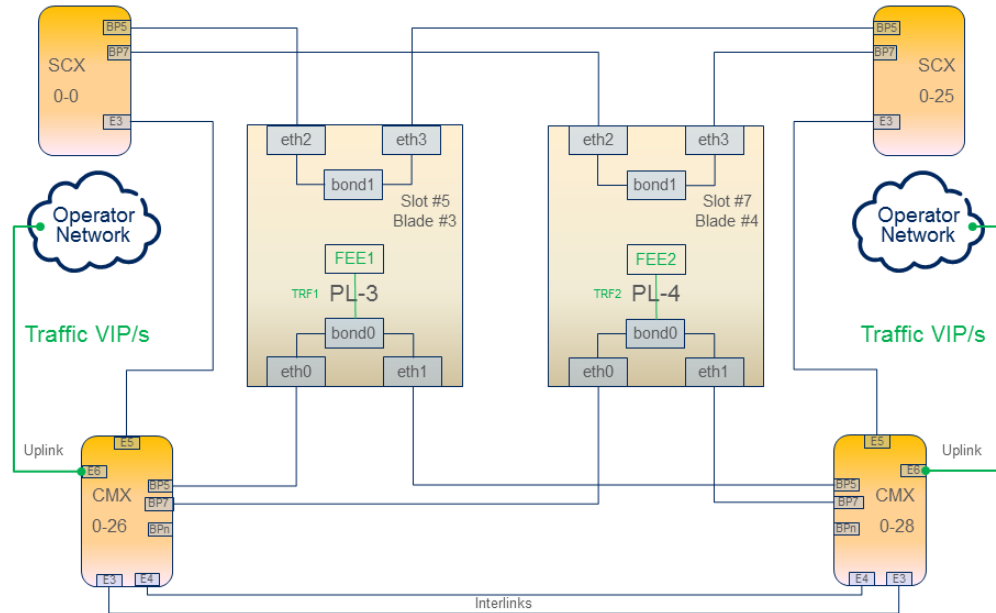


Figure 3 Subrack Configuration. Traffic Payloads

Traffic payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1** to provide High Availability for the 10-GB backplane. Besides, another bond is created between **eth2** and **eth3** to provide High Availability for the 1-GB backplane.

Traffic payloads are connected to the external network through VIP Traffic FEEs. These connections are used for load balancing purposes through a virtual IP.

Internal connectivity is done through the 10 GB interfaces connected to both CMX routers (which also provide switching capabilities). Both CMXs are interconnected to achieve High Availability.

External Database Payload Blades

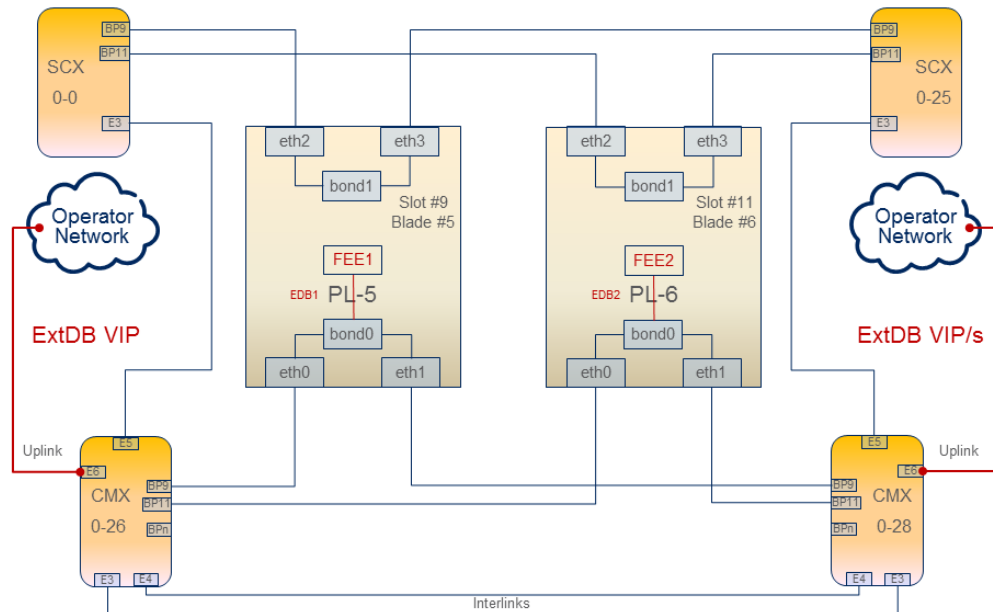


Figure 4 Subrack Configuration. External Database Payloads

External database payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1** to provide High Availability for the 10-GB backplane. Besides, another bond is created between **eth2** and **eth3** to provide High Availability for the 1-GB backplane.

External database payloads are connected to the external network through VIP ExtDB FEEs. These connections are used for load balancing purposes through a virtual IP.

Internal connectivity is done through the 10 GB interfaces connected to both CMX routers (which also provide switching capabilities). Both CMXs are interconnected to achieve High Availability.



GeoRed Payload Blades

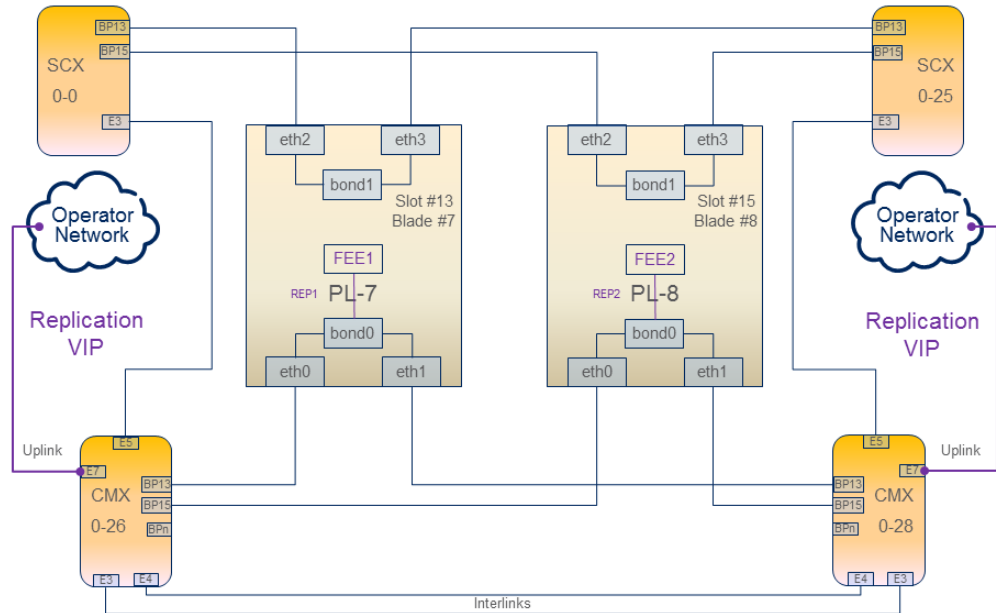


Figure 5 Subrack Configuration. GeoRed Payloads

GeoRed payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1** to provide High Availability for the 10-GB backplane. Besides, another bond is created between **eth2** and **eth3** to provide High Availability for the 1-GB backplane.

GeoRed payloads are connected to the external network through VIP Replication FEEs. These connections are used for load balancing purposes through a virtual IP.

Internal connectivity is done through the 10 GB interfaces connected to both CMX routers (which also provide switching capabilities). Both CMXs are interconnected to achieve High Availability.

Traffic Separation Payload Blades

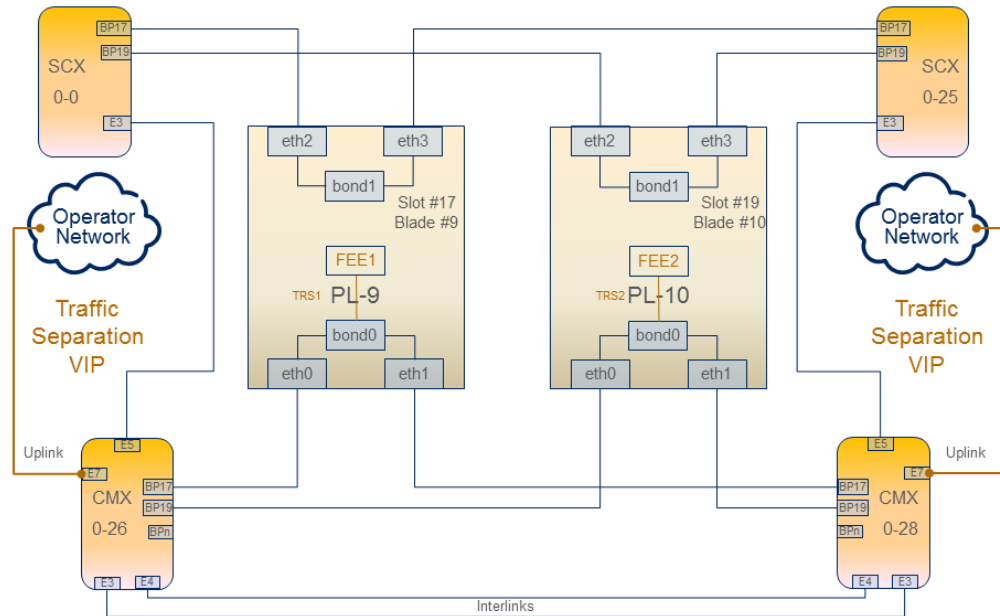


Figure 6 Subrack Configuration. Traffic Separation Payloads

Traffic separation payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1** to provide High Availability for the 10-GB backplane. Besides, another bond is created between **eth2** and **eth3** to provide High Availability for the 1-GB backplane.

Traffic separation payloads are connected to the external network through VIP Replication FEEs. These connections are used for load balancing purposes through a virtual IP.

Internal connectivity is done through the 10 GB interfaces connected to both CMX routers (which also provide switching capabilities). Both CMXs are interconnected to achieve High Availability.



Remaining Payload Blades

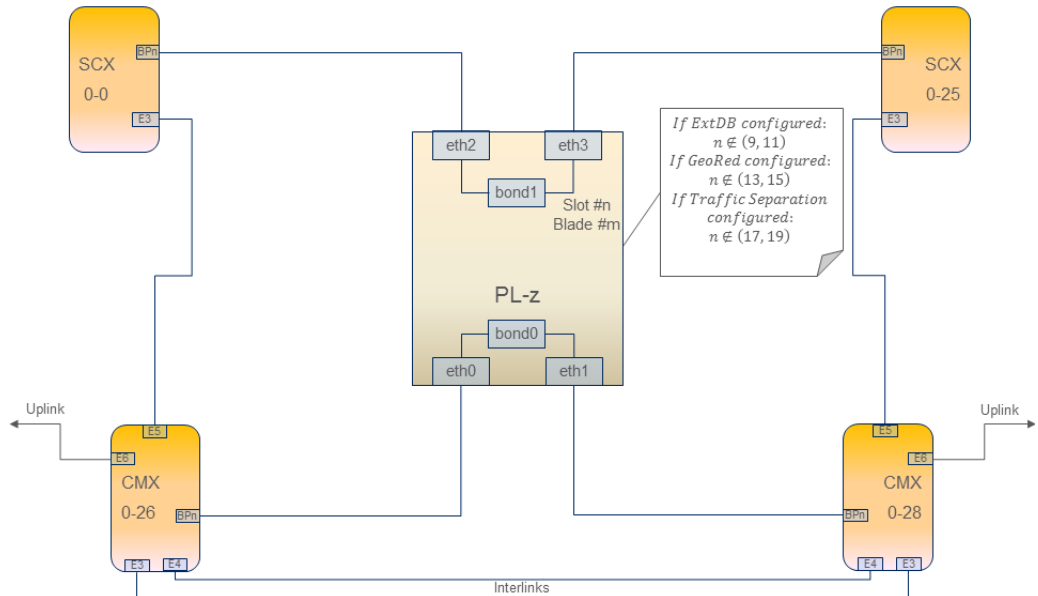


Figure 7 Subrack Configuration. Remaining Payload Blades

Remaining payloads are not virtualized, so no virtual bridges are defined. A bond is created between **eth0** and **eth1** to provide High Availability for the 10-GB backplane. Besides, another bond is created between **eth2** and **eth3** to provide High Availability for the 1-GB backplane.

Internal connectivity is done through the 10 GB interfaces connected to both CMX routers (which also provide switching capabilities). Both CMXs are interconnected to achieve High Availability.

2.3 BSP 8100 Whole Rack Configuration. 36 Physical Blades

The two first blades are system controllers and the rest blades are traffic payloads. The installation described in Section 2.2 on page 6 has to be done for the first subrack. In this chapter, additional networking is included for the additional second and third subracks.

Warning!

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-15 and PL-16 are used for Traffic FEEs, PL-17 and PL-18 for External Database FEEs, PL-19 and PL-20 for GeoRed FEEs, and PL-21 and PL-22 for Traffic Separation FEEs. For a third subrack, in a scenario with External Database, GeoRed, and Traffic Separation, apart from normal diameter traffic, PL-27 and PL-28 are used for Traffic FEEs, PL-29 and PL-30 for External Database FEEs, PL-31 and PL-32 for GeoRed FEEs, and PL-33 and PL-34 for Traffic Separation FEEs. Same configuration described above is applied.

2.3.1

Traffic Blades

Apart from the traditional networking we do as the other subrack, an extra networking to intercommunicate the second and third subracks with the first one is needed.

Non-Front End Blades

For non-front end blades, the following extra networking must be done.

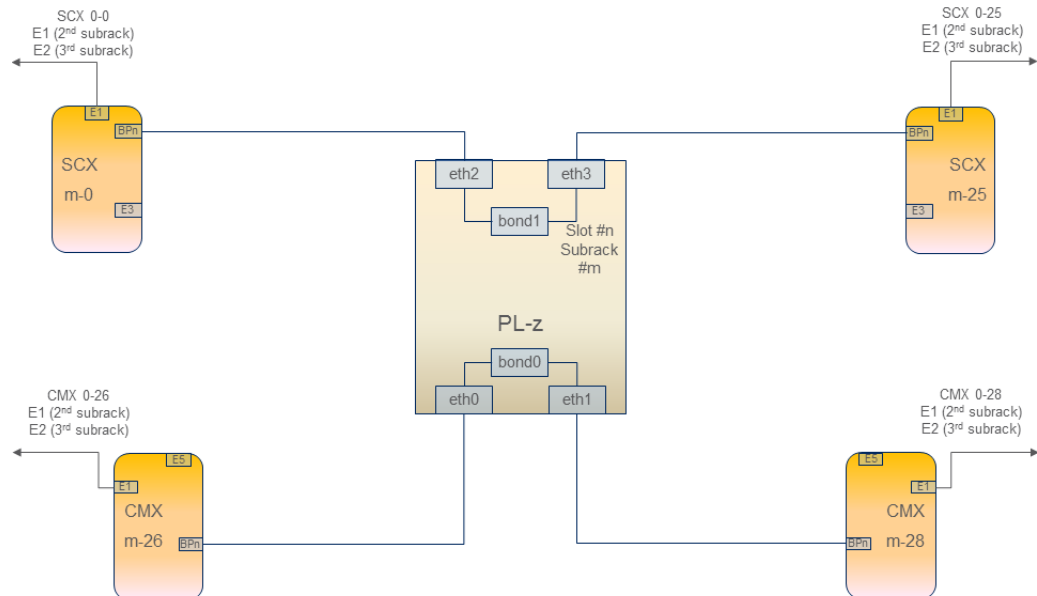


Figure 8 Whole Rack Configuration. Non-Front End Payload Blades



Front End Payload Blades

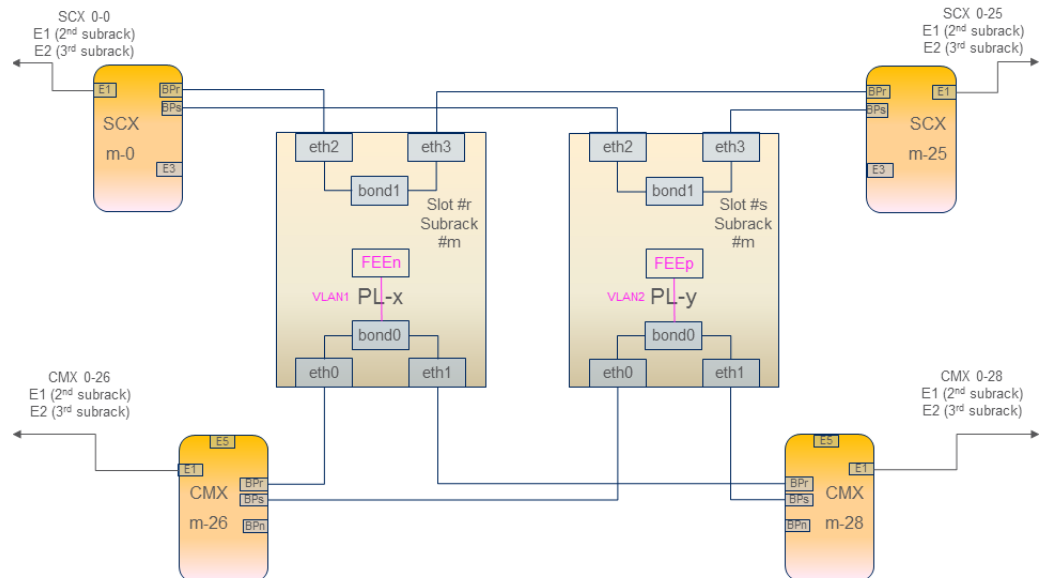


Figure 9 Whole Rack Configuration. Front End Payload Blades

Additional front end payload blades are needed in the new subracks. New FEEs are created in that case as Page 13 shows.





3 BSP 8100 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 BSP 8100 VLANs

Table 1 VLANs for One Subrack

VLAN Name	VLAN ID	Interface	Ports	Comments	Attributes
sapc_om2_sp	137	Blade: mgmt0	SCX 0-X: BP1, BP3, E3 CMX 0-Y: E3, E4, E5, GE4	SCs only. Hypervisor Management	vlanType = PRIVATE lanTopology = BASE_AND_DATA switchSide = COLLAPSED portAssignment = MANUAL AdditionalPort=0-X:BP1 AdditionalPort=0-X:BP3
sapc_mgmt_sp	138	Blade: mgmt1 VM: eth2	SCX 0-X: BP1, BP3, E3 CMX 0-Y: E3, E4, E5	SCs only. System Management	vlanType = PRIVATE lanTopology = BASE_AND_DATA switchSide = COLLAPSED portAssignment = MANUAL AdditionalPort=0-X:BP1 AdditionalPort=0-X:BP3
sapc_boot_sp	4001	VM: eth2 PL: bond1	SCX 0-X: BPn* (untagged)	LDE Boot and Scaling	vlanType = DEFAULT lanTopology = BASE switchSide = COLLAPSED



VLAN Name	VLAN ID	Interface	Ports	Comments	Attributes
sapc_int_sp	4003	bond0	CMX 0-Y: BPn* (untagged), E3, E4	Cluster Internal	vlanType = DEFAULT lanTopology = DATA switchSide = COLLAPSED
sapc_tipc_pdl	100	eth0	CMX 0-26: BPn	Left TIPC	vlanType = PRIVATE lanTopology = DATA switchSide = LEFT
sapc_tipc_pdr	101	eth1	CMX 0-28: BPn	Right TIPC	vlanType = PRIVATE lanTopology = DATA switchSide = RIGHT
sapc_om1_sp1	130	bond0	CMX 0-Y: BP1, E3, E4	eVIP Router Link O&M Traffic	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED portAssignment = MANUAL AdditionalBlade=0- -1
sapc_om1_sp2	131	bond0	CMX 0-Y: BP3, E3, E4	eVIP Router Link O&M Traffic	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED portAssignment = MANUAL AdditionalBlade=0- -3
sapc_sig1_sp1	120	bond0	CMX 0-Y: BPn (n not 1 nor 3), E3, E4	eVIP Router Link Signaling Traffic	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED ExcludedBlade=0- 1 ExcludedBlade=0- 3



VLAN Name	VLAN ID	Interface	Ports	Comments	Attributes
sapc_sig1_sp2	121	bond0	CMX 0-Y: BPn (n not 1 nor 3), E3, E4	eVIP Router Link Signaling Traffic	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED ExcludedBlade=0-1 ExcludedBlade=0-3
sapc_sig2_sp1	140	bond0	CMX 0-Y: BPn (n not 1 nor 3), E3, E4	eVIP Router Link LDAP Traffic	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED ExcludedBlade=0-1 ExcludedBlade=0-3
sapc_sig2_sp2	141	bond0	CMX 0-Y: BPn (n not 1 nor 3), E3, E4	eVIP Router Link LDAP Traffic	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED ExcludedBlade=0-1 ExcludedBlade=0-3
sapc_sig3_sp1	150	bond0	CMX 0-Y: BPn (n not 1 nor 3), E3, E4	eVIP Router Link Replication Traffic	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED ExcludedBlade=0-1 ExcludedBlade=0-3
sapc_sig3_sp2	151	bond0	CMX 0-Y: BPn (n not 1 nor 3), E3, E4	eVIP Router Link Replication Traffic	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED ExcludedBlade=0-1 ExcludedBlade=0-3



VLAN Name	VLAN ID	Interface	Ports	Comments	Attributes
sapc_sig4_sp1	122	bond0	CMX 0-Y: BPn (n not 1 nor 3), E3, E4	eVIP Router Link Signaling Traffic Rx	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED ExcludedBlade=0-1 ExcludedBlade=0-3
sapc_sig4_sp2	123	bond0	CMX 0-Y: BPn (n not 1 nor 3), E3, E4	eVIP Router Link Signaling Traffic Rx	vlanType = PRIVATE lanTopology = DATA switchSide = COLLAPSED ExcludedBlade=0-1 ExcludedBlade=0-3

For multiple subracks, additional ports are added for the previous VLANs.

Table 2 VLANs for Whole Rack

VLAN Name	VLAN ID	Interface	Ports	Comments
sapc_boot_sp	4001	SCs: eth2 PLs: bond1	SCX 0-X: E1, E2 SCX m-X: BPn* (untagged), E1	LDE Boot and Scaling
sapc_int_sp	4003	bond0	CMX 0-Y: E1, E2 CMX m-Y: BPn* (untagged), E1	Cluster Internal
sapc_tipc_pdl	100	eth0	CMX 0-26: E1, E2	Left TIPC
sapc_tipc_pdr	101	eth1	CMX 0-28: E1, E2	Right TIPC
sapc_sig1_sp1	120	bond0	CMX 0-Y: E1, E2 CMX m-Y: BPn, E1	eVIP Router Link Signaling Traffic
sapc_sig1_sp2	121	bond0	CMX 0-Y: E1, E2 CMX m-Y: BPn, E1	eVIP Router Link Signaling Traffic
sapc_sig2_sp1	140	bond0	CMX 0-Y: E1, E2 CMX m-Y: BPn, E1	eVIP Router Link LDAP Traffic
sapc_sig2_sp2	141	bond0	CMX 0-Y: E1, E2 CMX m-Y: BPn, E1	eVIP Router Link LDAP Traffic
sapc_sig3_sp1	150	bond0	CMX 0-Y: E1, E2 CMX m-Y: BPn, E1	eVIP Router Link Replication Traffic
sapc_sig3_sp2	151	bond0	CMX 0-Y: E1, E2 CMX m-Y: BPn, E1	eVIP Router Link Replication Traffic



VLAN Name	VLAN ID	Interface	Ports	Comments
sapc_sig4_sp1	122	bond0	CMX 0-Y: E1, E2 CMX m-Y: BPn, E1	eVIP Router Link Signaling Traffic Rx
sapc_sig4_sp2	123	bond0	CMX 0-Y: E1, E2 CMX m-Y: BPn, E1	eVIP Router Link Signaling Traffic Rx

3.2 BSP 8100 IP Addressing

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

Table 3 IPv4 Network and VLAN for BSP Management

Network Address	Mask	Type	Usage	VLAN ID	Virtual Router	VLAN Name/Tag
bsp_om_net	/29	Public	BSP Northbound OAM network	4054	dmx_om_vr	%{bsp_om_net}
			Collapsed IP for BSP Northbound OAM			%{bsp_om_addr}
			VRRP IP for BSP Northbound OAM			%{bsp_om_gw}
			CMX26 IP for BSP Northbound OAM			%{bsp_om_cmx26_addr}
			CMX28 IP for BSP Northbound OAM			%{bsp_om_cmx28_addr}
	N/A	N/A	VR ID for BSP Northbound OAM	N/A		%{bsp_om_vrid}
om_sibb_sp_net	N/A	Private	Uplink VLAN connected to external network for BSP Northbound traffic	om_sibb_sp_id	dmx_om_vr	%{om_sibb_sp_id}
	/29		Uplink VRRP IP connected to external network for BSP Northbound traffic			%{om_sibb_sp_addr}
			Uplink CMX26 IP connected to external network for BSP Northbound traffic			%{om_sibb_sp_addr1} with net suffix (CIDR)
			Uplink CMX28 IP connected to external network for BSP Northbound traffic			%{om_sibb_sp_addr2} with net suffix (CIDR)
			Uplink CMX26 gateway for BSP Northbound traffic			%{om_sibb_sp_gw1}
			Uplink CMX28 gateway for BSP Northbound traffic			%{om_sibb_sp_gw2}
	N/A	N/A	Uplink VR ID for BSP Northbound traffic	N/A	%{om_sibb_sp_vrid}	



Table 4 IPv4 Network and VLAN for SAPC

Network Address	Mask	Type	Usage	VLAN ID	Virtual Router	VLAN Name/Tag
169.254.69.0	/24	Link-Local	Backplane booting & scaling network	4001	om_cn_sp	sapc_boot_sp
172.16.100.0	/24	Link-Local	Backplane cluster internal communication network	4003	om_cn_sp	sapc_int_sp
192.168.206.4	/30	Private	Cross shelf link internal AS network for signaling traffic	25	sig_cn_1_sp	sig_cn_1_sp_incl
sig_cn_1_sp_ncl_net	/30	Private ⁽¹⁾ ₍₂₎	Cross shelf link external AS network for signaling traffic	26	sig_cn_1_sp	sig_cn_1_sp_ncl
			Cross shelf link external AS CMX26 IP for signaling traffic			%{sig_cn_1_sp_ncl_addr1} without net suffix
			Cross shelf link external AS CMX26 IP for signaling traffic with network suffix			%{sig_cn_1_sp_ncl_addr1_cidr} with net suffix (CIDR)
			Cross shelf link external AS CMX28 IP for signaling traffic			%{sig_cn_1_sp_ncl_addr2} without net suffix
			Cross shelf link external AS CMX28 IP for signaling traffic with network suffix			%{sig_cn_1_sp_ncl_addr2_cidr} with net suffix (CIDR)
192.168.205.4	/30	Private	Cross shelf link internal AS network for signaling 2 traffic	15	sig_cn_2_sp	sig_cn_2_sp_incl
sig_cn_2_sp_ncl_net	/30	Private ⁽¹⁾ ₍₂₎	Cross shelf link external AS network for signaling 2 traffic	16	sig_cn_2_sp	sig_cn_2_sp_ncl
			Cross shelf link external AS CMX26 IP for signaling 2 traffic			%{sig_cn_2_sp_ncl_addr1} without net suffix
			Cross shelf link external AS CMX26 IP for signaling 2 traffic with network suffix			%{sig_cn_2_sp_ncl_addr1_cidr} with net suffix (CIDR)
			Cross shelf link external AS CMX28 IP for signaling 2 traffic			%{sig_cn_2_sp_ncl_addr2} without net suffix
			Cross shelf link external AS CMX28 IP for signaling 2 traffic with network suffix			%{sig_cn_2_sp_ncl_addr2_cidr} with net suffix (CIDR)
192.168.208.4	/30	Private	Cross shelf link internal AS network for OAM traffic	35	om_cn_sp	om_cn_sp_incl



Network Address	Mask	Type	Usage	VLAN ID	Virtual Router	VLAN Name/Tag
om_cn_sp_ncl_net	/30	Private ⁽¹⁾ (2)	Cross shelf link external AS network	36	om_cn_sp	om_cn_sp_ncl
			Cross shelf link external AS CMX26 IP for OAM traffic			%{om_cn_sp_ncl_addr1} without net suffix
			Cross shelf link external AS CMX26 IP for OAM traffic with network suffix			%{om_cn_sp_ncl_addr1_cidr} with net suffix (CIDR)
			Cross shelf link external AS CMX28 IP for OAM traffic			%{om_cn_sp_ncl_addr2} without net suffix
			Cross shelf link external AS CMX28 IP for OAM traffic with network suffix			%{om_cn_sp_ncl_addr2_cidr} with net suffix (CIDR)
192.168.207.4	/30	Private	Cross shelf link internal AS network for LDAP traffic	45	sig_data_1_sp	sig_data_1_sp_incl
sig_data_1_sp_ncl_net	/30	Private ⁽¹⁾ (2)	Cross shelf link external AS network for LDAP traffic	46	sig_data_1_sp	sig_data_1_sp_ncl
			Cross shelf link external AS CMX26 IP for LDAP traffic			%{sig_data_1_sp_ncl_addr1} without net suffix
			Cross shelf link external AS CMX26 IP for LDAP traffic with network suffix			%{sig_data_1_sp_ncl_addr1_cidr} with net suffix (CIDR)
			Cross shelf link external AS CMX28 IP for LDAP traffic			%{sig_data_1_sp_ncl_addr2} without net suffix
			Cross shelf link external AS CMX28 IP for LDAP traffic with network suffix			%{sig_data_1_sp_ncl_addr2_cidr} with net suffix (CIDR)
192.168.209.4	/30	Private	Cross shelf link internal AS network for replication traffic	55	sig_data_2_sp	sig_data_2_sp_incl
192.168.206.1	/32	Private ⁽²⁾	CMX26 internal AS local address	N/A	sig_cn_1_sp	N/A
192.168.206.2	/32	Private ⁽²⁾	CMX28 internal AS local address	N/A	sig_cn_1_sp	N/A
192.168.205.1	/32	Private ⁽²⁾	CMX26 internal AS local address	N/A	sig_cn_2_sp	N/A
192.168.205.2	/32	Private ⁽²⁾	CMX28 internal AS local address	N/A	sig_cn_2_sp	N/A
192.168.208.1	/32	Private ⁽²⁾	CMX26 internal AS local address	N/A	om_cn_sp	N/A
192.168.208.2	/32	Private ⁽²⁾	CMX28 internal AS local address	N/A	om_cn_sp	N/A
192.168.207.1	/32	Private ⁽²⁾	CMX26 internal AS local address	N/A	sig_data_1_sp	N/A



Network Address	Mask	Type	Usage	VLAN ID	Virtual Router	VLAN Name/Tag
192.168.207.2	/32	Private ⁽²⁾	CMX28 internal AS local address	N/A	sig_data_1_sp	N/A
N/A	N/A	N/A	TIPC VLAN through left CMX	100	N/A	sapc_tipc_pdl
N/A	N/A	N/A	TIPC VLAN through right CMX	101	N/A	sapc_tipc_pdr
192.168.216.0	/27	Private	eVIP router link for signaling traffic	120	sig_cn_1_sp	sapc_sig1_sp1
192.168.216.32	/27	Private	eVIP router link for signaling traffic	121	sig_cn_1_sp	sapc_sig1_sp2
192.168.218.0	/29	Private	eVIP router link for OAM traffic	130	om_cn_sp	sapc_om1_sp1
192.168.218.8	/29	Private	eVIP router link for OAM traffic	131	om_cn_sp	sapc_om1_sp2
192.168.217.0	/27	Private	eVIP router link for LDAP traffic	140	sig_data_1_sp	sapc_sig2_sp1
192.168.217.32	/27	Private	eVIP router link for LDAP traffic	141	sig_data_1_sp	sapc_sig2_sp2
192.168.219.0	/27	Private	eVIP router link for replication traffic	150	sig_data_2_sp	sapc_sig3_sp1
192.168.219.32	/27	Private	eVIP router link for replication traffic	151	sig_data_2_sp	sapc_sig3_sp2
192.168.220.0	/27	Private	eVIP router link for signaling traffic 2 (Rx)	122	sig_cn_2_sp	sapc_sig4_sp1
192.168.220.32	/27	Private	eVIP router link for signaling traffic 2 (Rx)	123	sig_cn_2_sp	sapc_sig4_sp2
192.168.100.0	/24	Private	System Management Network	138	N/A	sapc_mgmt_sp
sapc_om2_sp_net	/29	Public	Hypervisor management network	137	om_cn_sp	sapc_om2_sp
			VRRP IP for hypervisor management			%{sapc_om2_sp_gw}
			CMX26 IP for hypervisor management			%{sapc_om2_sp_cmx26_addr} with net suffix (CIDR)
			CMX28 IP for hypervisor management			%{sapc_om2_sp_cmx28_addr} with net suffix (CIDR)
	N/A	N/A	VR ID for hypervisor management	N/A		%{sapc_om2_sp_vrid}
sapc_sig_cn_1_vip	/32	Public	VIP signaling address	N/A	sig_cn_1_sp	%{sapc_sig_cn_1_vip} with net suffix (CIDR)
sapc_sig_cn_2_vip	/32	Public	VIP signaling 2 (Rx) address	N/A	sig_cn_2_sp	%{sapc_sig_cn_2_vip} with net suffix (CIDR)
sapc_om_cn_vip1	/32	Public	VIP OAM address	N/A	om_cn_sp	%{sapc_om_cn_vip1} with net suffix (CIDR)



Network Address	Mask	Type	Usage	VLAN ID	Virtual Router	VLAN Name/Tag
sapc_om_cn_vip2	/32	Public	VIP provisioning address	N/A	om_cn_sp	%{sapc_om_cn_vip2} with net suffix (CIDR)
sapc_sig_data_1_vip	/32	Public	VIP LDAP address	N/A	sig_data_1_sp	%{sapc_sig_data_1_vip} with net suffix (CIDR)
sapc_sig_data_2_vip	/32	Public	VIP replication address	N/A	sig_data_2_sp	%{sapc_sig_data_2_vip} with net suffix (CIDR)
sig_cn_1_pr_net	N/A	Private	Uplink VLAN connected to external network for signaling traffic	sig_cn_1_pr_id	sig_cn_1_sp	%{sig_cn_1_pr_id}
	N/A		Uplink OSPF area for signaling traffic ⁽³⁾			%{sig_cn_1_pr_ospf}
	/29		Uplink CMX26 IP for signaling traffic			%{sig_cn_1_pr_addr1} with net suffix (CIDR)
			Uplink CMX28 IP for signaling traffic			%{sig_cn_1_pr_addr2} with net suffix (CIDR)
			Uplink gateway 1 for signaling traffic ⁽⁴⁾			%{sig_cn_1_pr_gw1}
			Uplink gateway 2 for signaling traffic			%{sig_cn_1_pr_gw2}
sig_cn_2_pr_net	N/A	Private	Uplink VLAN connected to external network for signaling 2 traffic	sig_cn_2_pr_id	sig_cn_2_sp	%{sig_cn_2_pr_id}
	N/A		Uplink OSPF area for signaling 2 traffic ⁽³⁾			%{sig_cn_2_pr_ospf}
	/29		Uplink CMX26 IP for signaling 2 traffic			%{sig_cn_2_pr_addr1} with net suffix (CIDR)
			Uplink CMX28 IP for signaling 2 traffic			%{sig_cn_2_pr_addr2} with net suffix (CIDR)
			Uplink gateway 1 for signaling 2 traffic ⁽⁴⁾			%{sig_cn_2_pr_gw1}
			Uplink gateway 2 for signaling 2 traffic ⁽⁴⁾			%{sig_cn_2_pr_gw2}



Network Address	Mask	Type	Usage	VLAN ID	Virtual Router	VLAN Name/Tag
om_cn_pr_net	N/A	Private	Uplink VLAN connected to external network for OAM traffic	om_cn_pr_id	sig_cn_sp	%{om_cn_pr_id}
	N/A		Uplink OSPF area for OAM traffic ⁽³⁾			%{om_cn_pr_ospf}
	/29		Uplink CMX26 IP for OAM traffic			%{om_cn_pr_addr1} with net suffix (CIDR)
			Uplink CMX28 IP for OAM traffic			%{om_cn_pr_addr2} with net suffix (CIDR)
			Uplink gateway 1 for OAM traffic ⁽⁴⁾			%{om_cn_pr_gw1}
			Uplink gateway 2 for OAM traffic ⁽⁴⁾			%{om_cn_pr_gw2}
sig_data_1_pr_net	N/A	Private	Uplink VLAN connected to external network for LDAP traffic	sig_data_1_pr_id	sig_data_1_sp	%{sig_data_1_pr_id}
	N/A		Uplink OSPF area for LDAP traffic ⁽³⁾			%{sig_data_1_pr_ospf}
	/29		Uplink CMX26 IP for LDAP traffic			%{sig_data_1_pr_addr1} with net suffix (CIDR)
			Uplink CMX28 IP for LDAP traffic			%{sig_data_1_pr_addr2} with net suffix (CIDR)
			Uplink gateway 1 for LDAP traffic ⁽⁴⁾			%{sig_data_1_pr_gw1}
			Uplink gateway 2 for LDAP traffic ⁽⁴⁾			%{sig_data_1_pr_gw2}
sig_data_2_pr_net	N/A	Private	Uplink VLAN connected to external network for replication traffic	sig_data_2_pr_id	sig_data_2_sp	%{sig_data_2_pr_id}
	/29		Uplink CMX26 IP for replication traffic			%{sig_data_2_pr_addr1} with net suffix (CIDR)
			Uplink CMX28 IP for replication traffic			%{sig_data_2_pr_addr2} with net suffix (CIDR)
			Uplink gateway 1 for replication traffic			%{sig_data_2_pr_gw1}
			Uplink gateway 2 for replication traffic			%{sig_data_2_pr_gw2}

(1) For a GeoRed deployment, this subnet belongs to the customer, since the interfaces to which this subnet addresses are assigned and the Site Routers (SRs) are in the same Autonomous System (AS), so these routes are learned by the SRs through OSPF and, therefore seen from them.

(2) For a GeoRed deployment, this subnet must be filtered out on the SRs to avoid their announcement to the customer backbone.

(3) This parameter is specific and mandatory only for a GeoRed deployment.

(4) This parameter is specific and mandatory only for a Standalone deployment. BFD enabled is also mandatory on the SRs side to ensure a fast failover recovery.



Table 5 IP Allocation of Internal Networks for SAPC

IP Address	Node	Interface	Comment
169.254.69.0/24	Network	N/A	VLAN sapc_boot_sp Booting & Scaling network
.1	SC-1	eth2	
.2	SC-2	eth2	
.n	PL-n	bond1	
.242	SC-1 SC-2	eth2:2	Boot MIP address
.200 - .232			Temporary IP address pool for scaled blades
.253	CMX 0-26	vlan1.4001	ARP target on CMX 0-26
.254	CMX 0-28	vlan1.4001	ARP target on CMX 0-28
172.16.100.0/24	Network		VLAN sapc_int_sp Cluster Internal network
.1	SC-1	bond0	
.2	SC-2	bond0	
.n	PL-n	bond0	
.243	SC-1 SC-2	bond0:1	NFS MIP address
244	One of the PL nodes	bond0:1	SS7 CPM MIP address
.253	CMX 0-26	vlan1.4003	ARP target on CMX 0-26
.254	CMX 0-28	vlan1.4003	ARP target on CMX 0-28

Table 6 OSPF Stub Areas

Network	Gateways	VLAN	OSPF Area	Comments
192.168.218.0/29	CMX 0-26: 192.168.21 8.1	130	0.1.1.1	O&M Traffic
	CMX 0-28: 192.168.21 8.2			
192.168.218.8/29	CMX 0-26: 192.168.21 8.9	131	0.1.1.1	O&M Traffic
	CMX 0-28: 192.168.21 8.10			
192.168.216.0/27	CMX 0-26: 192.168.21 6.1	120	0.0.1.1	Signaling Traffic
	CMX 0-28: 192.168.21 6.2			
192.168.216.32/27	CMX 0-26: 192.168.21 6.33	121	0.0.1.1	Signaling Traffic
	CMX 0-28: 192.168.21 6.34			



Network	Gateways	VLAN	OSPF Area	Comments
192.168.217.0/27	CMX 0-26: 192.168.21 7.1	140	0.0.1.2	LDAP Traffic
	CMX 0-28: 192.168.21 7.2			
192.168.217.32/27	CMX 0-26: 192.168.21 7.33	141	0.0.1.2	LDAP Traffic
	CMX 0-28: 192.168.21 7.34			
192.168.219.0/27	CMX 0-26: 192.168.21 9.1	150	0.0.1.3	Replication Traffic
	CMX 0-28: 192.168.21 9.2			
192.168.219.32/27	CMX 0-26: 192.168.21 9.33	151	0.0.1.3	Replication Traffic
	CMX 0-28: 192.168.21 9.34			
192.168.220.0/27	CMX 0-26: 192.168.22 0.1	122	0.0.1.4	Signaling Rx Traffic
	CMX 0-28: 192.168.22 0.2			
192.168.220.32/27	CMX 0-26: 192.168.22 0.33	123	0.0.1.4	Signaling Rx Traffic
	CMX 0-28: 192.168.22 0.34			

3.2.1 BSP 8100 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 7 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.