

# CSCF VNF Network Connectivity Overview

Call Session Control Function

DESCRIPTION

**Copyright**

© Ericsson AB 2014–2018. 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

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>CSCF VNF Logical Network Reference Setup</b>	<b>3</b>
2.1	Logical Network Reference Setup	3
2.2	IP Routing	5
2.3	CSCF ALB Configuration	5
2.4	Logical Network Operation and Maintenance	7
2.5	Logical Network Signaling	9
2.6	Logical Network Charging	12
2.7	Logical Network Internal	14
2.8	Logical Network Setup in Multiple CSCF VNF Instance Deployment	15
<b>3</b>	<b>Example Configurations</b>	<b>21</b>
3.1	Static Routing with BFD Configuration	21
3.2	Static Routing without BFD Configuration	23
3.3	Dynamic Routing Design	27
3.4	OpenStack Deployment	29
3.5	Equal-Cost Multipath Considerations	42





# 1 Introduction

This document gives Solution Architects guidance on how to deploy the Call Session Control Function (CSCF) Virtual Network Function (VNF) in a cloud environment. The document provides a logical description of the CSCF VNF networking requirements. The final section gives examples of cloud networking infrastructure configurations required to fulfill the networking requirements of the CSCF VNF.

The document describes how to configure the cloud network infrastructure from a CSCF VNF perspective. This document does not specify the exact commands to execute, or Application Programming Interface (API) calls to make, but rather describes the configuration on a logical level.

It is assumed that the cloud framework, including hardware and relevant software components, is already installed. It is also assumed that the user of this document has a deep understanding of the cloud infrastructure on which the CSCF VNF is to be deployed.

It is assumed that the reader of this document has a deep understanding of the CSCF, and the document [CSCF Technical Description](#) has been read and fully understood. For detailed information of each CSCF interface/integration-point, refer to the relevant Interwork Description.

It is outside the scope of this document to describe how to configure external router and other routers on the customer site. However, there is a general recommendation on how external router can be configured in the document, without specifying any details. It is also outside the scope of this document to describe any firewall configuration.

This document does not cover dimensioning or scaling aspects of a CSCF VNF deployment.

For more information on scaling, refer to [CSCF Scaling Management](#).





## 2 CSCF VNF Logical Network Reference Setup

The CSCF VNF is realized by using several logical networks, where each logical network has its own purpose. This document proposes a reference logical network setup, which is realized by the virtual networks that are listed later in this document. The reason for using different logical networks is to enable logic separation between different functions owing to, for example, security reasons.

It is not required that the CSCF VNF is deployed using the reference logical network setup that is described in this document. The logical network setup can be altered depending on deployment-specific requirements. Any logical network setup other than the CSCF reference logical network setup is not elaborated further in this document.

How to set up the CSCF VNF, and how to allocate software components to Virtual Machine (VM) instances is described in [CSCF Software and Pool Allocation Guidelines](#), and is therefore not in the scope of this document.

For more information regarding basic requirements of what is required from a cloud infrastructure, refer to [Virtual CSCF Infrastructure Requirements](#).

### 2.1 Logical Network Reference Setup

The CSCF VNF exposes several network interfaces. These interfaces expose the CSCF functionality, or are used by the CSCF to access network functions, for example Domain Name System (DNS) and Network Time Protocol (NTP). In the reference network setup of the CSCF VNF, one or more of these network interfaces is allocated to a virtual network.

The following logical networks are part of the CSCF reference network setup. This document assumes that the same logical networks exist in an operator network, and that the operator requires that the CSCF VNF is being connected to these existing logical networks:

- Operation and Maintenance Network
- Signaling Network
- Charging Network
- Internal Network
- Confidential network

**Note:** Descriptions of the confidential network are outside the scope of this document. For information on the confidential network, refer to Lawful Interception (LI) documentation.

Which CSCF VNF interfaces are exposed in each network is described later in the document. It is outside the scope of this document to show how other network entities are connected to the listed logical networks.

**Note:** There are no External Network entities connected to the Internal Network. The Internal Network only connects the CSCF VNF instances.

Figure 1 shows an overview of the CSCF VNF, the associated pool allocations (profiles), and the logical network included in the reference logical network setup.

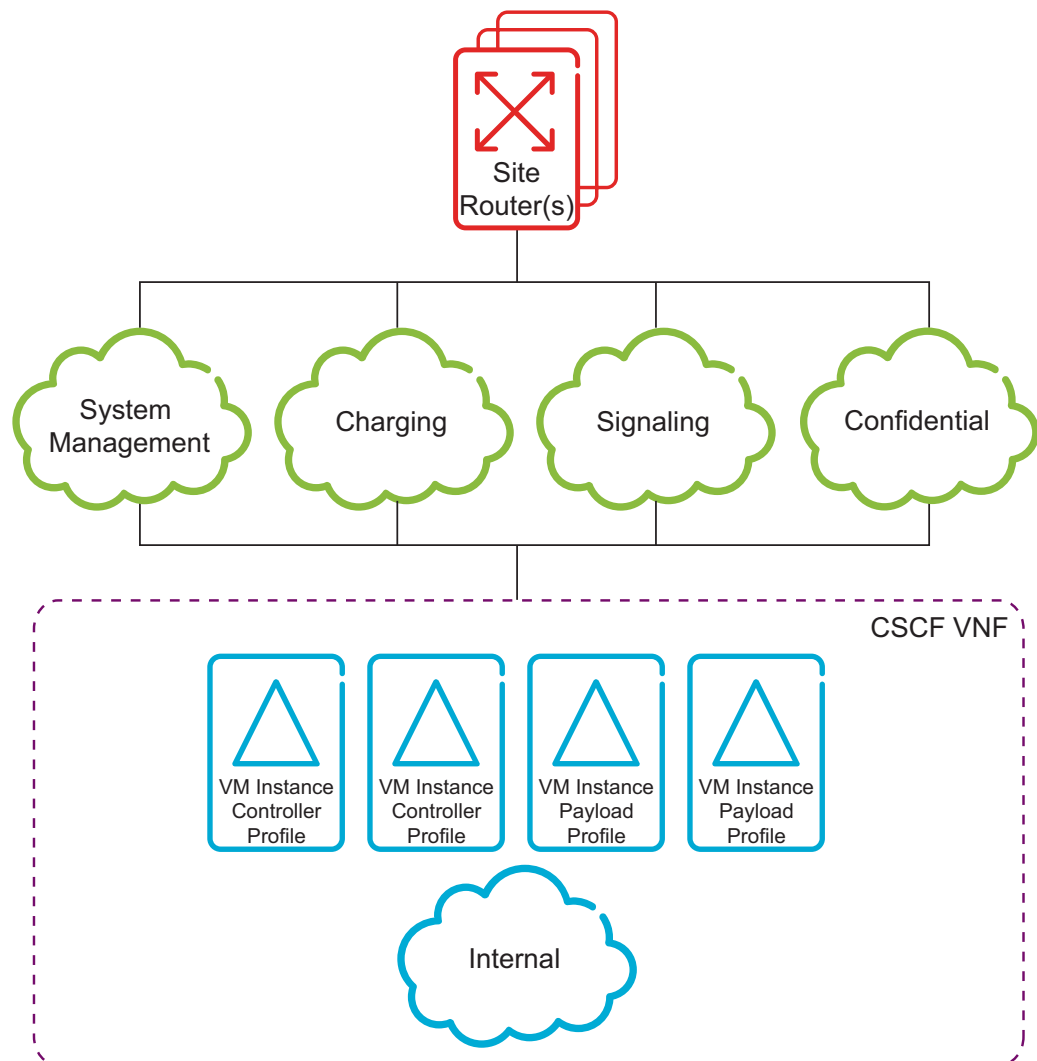


Figure 1 CSCF VNF and Its Logical Network Setup

Each logical network is realized using one or more virtual networks and optionally a Virtual Routing Function as described later in this document. This document does not describe how virtual networks and Virtual Routing Functions are realized by the cloud infrastructure.





As defined in *Virtual CSCF Infrastructure Requirements*, the minimum cloud configuration (2+2) is used to illustrate the CSCF network connectivity. Scale-out can be performed to increase the number of Payload Profile VM instances as described in *CSCF Scaling Management*.

## 2.2 IP Routing

Routing towards the CSCF VNF from the external router to the respective Virtual Routing Function is assumed to use Policy Based Routing (PBR). PBR is a technique used to make routing decisions based on policies (source, destination, port, and so on) set by the network administrator. Usually, it can also be read as static routes in a router.

The IP routing logic in the respective Virtual Routing Function (realized by Virtual Routers, for example, see Figure 3) then forwards the IP packet to the correct CSCF VNF VM instance. The following deployment strategy is used to realize the IP routing logic in the Virtual Routing Function:

### — Static routing in Virtual Routing Function

This means that static routing is configured in the Virtual Routing Function. This results in that the incoming IP packets are forwarded to one of the VM instances that handles the specific Virtual IP address (VIP). To distribute the IP packets between the different VM instances, and to avoid reordering of IP packets inside the CSCF, flow-based Equal-Cost Multipath (ECMP) is required. ECMP in this context means that all IP packets within the same IP flow (TCP session, SCTP stream, and fragmented UDP packets) are received by the same CSCF VM instance.

In the following sections, routing is described assuming that static routing is used.

## 2.3 CSCF ALB Configuration

The CSCF software is distributed across the VMs within a VNF using two software profiles – Controller Profile (OAM functionality) and Payload Profile (Charging, Signaling, Confidential, and Traffic functionality). Across the VMs, network connectivity is configured through several defined Abstract Load Balancers (ALB), with each ALB having a defined eVIP Front End (FE), Load Balancer Element (LBE), and Security Element (SE), see Figure 2.

**Note:** OAM is not defined in an ALB but in an MIP.

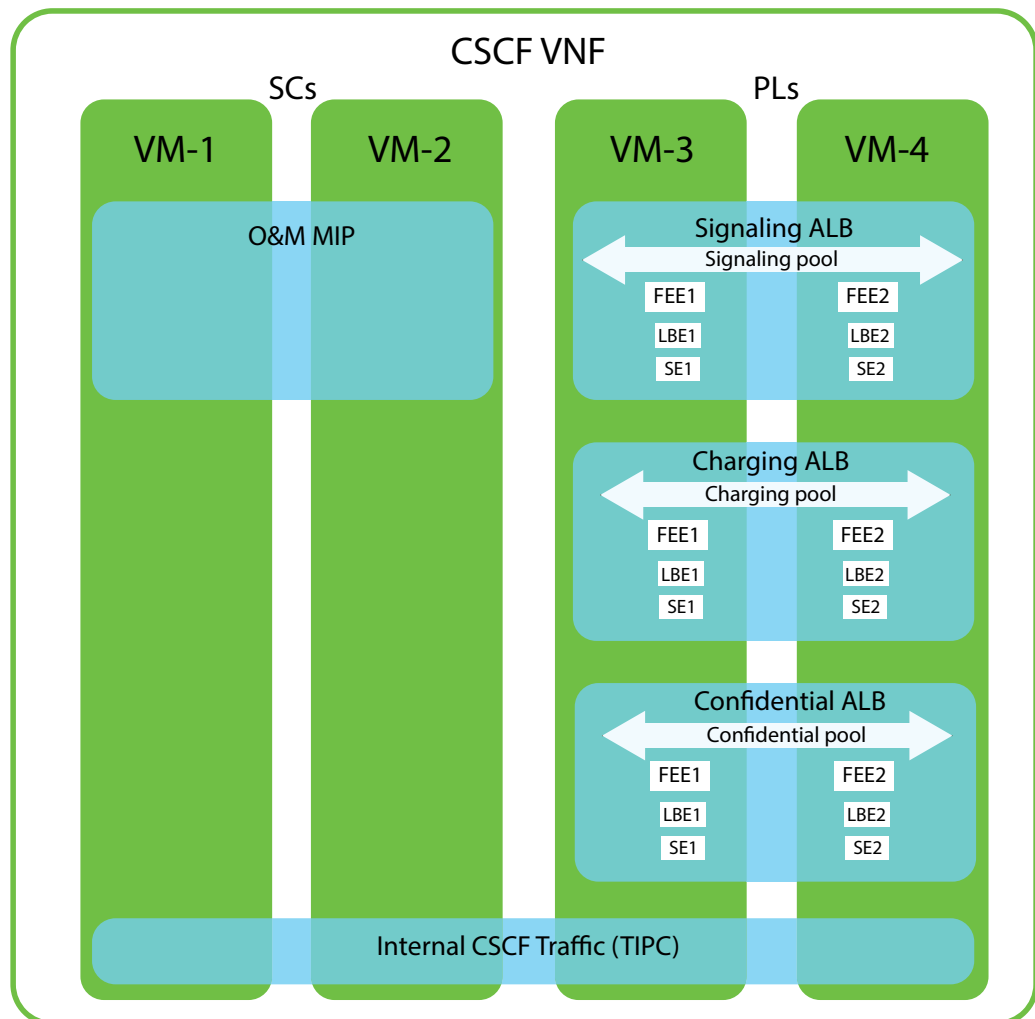


Figure 2 CSCF ALB Configuration

**Note:**

- Specific eVIP FEs are not configured for internal CSCF application traffic across CSCF VMs. Internal application traffic is distributed as defined by eVIP target pools. Refer to [eVIP Management Guide](#) for more information.
- Descriptions of the confidential network are outside the scope of this document. For information on the confidential network, refer to [LI documentation](#).

The connectivity between the set of ALB provided VIP addresses and the External Network entities is established through the FEs. For an ALB that groups single-homed VIP addresses, 4×FEs are defined. The ALBs that group multihomed VIP addresses are equipped with 2×FEs. Because of the nature of the VNF internal life cycle management of the FEs, their position is not fixed. They can appear on any of the available PLs. One PL can host only one FE from an ALB, but can host multiple FEs from different ALBs. To maximize the availability



of the established SCTP association, the FEs of the paired multihomed ALBs (<cscf\_om|cscf\_sig>\_pdl and <cscf\_om|cscf\_sig>\_pdr) are never collocated on a single PL.

All the FEs that belong to an ALB and the adjacent VIP gateway routers are connected to the same VIP FE network. Routing over the VIP FE networks can be accommodated as follows in the preference order:

- Static routing (without single-hop BFD supervision)
- Static routing with single-hop BFD supervision

## 2.4 Logical Network Operation and Maintenance

### 2.4.1 Purpose

The purpose of this logical network is to enable Simple Network Management Protocol (SNMP) communication between the Business Support System (BSS) or Operations Support System (OSS) and the Controller Profile VM instances. This includes the sending of SNMP traps to the OSS and fetching counter-information from the Controller Profile VM instances. The logical network is also used to configure the CSCF VNF and to connect to the Network License Server (NeLS).

The CSCF VNF exposes the following MIP interface on the logical network Operation and Maintenance (OAM):

- CSCF OAM MIP interface

The CSCF VNF exposes the following direct IP interface to all Controller Profile VM instances. Direct IP interface in this context means public addressable IP address:

- Unique public routable IP address to each VM instance with Controller Profile

### 2.4.2 Description

It is assumed that the external router is configured with a set of PBR rules. These rules send IP packets targeted to the MIP address (enumerated in Section 2.4.1 Purpose on page 7) to OAM Virtual Routing Function (OAM-VR). It is also assumed that the public routable IP addresses are part of the Virtual Network OAM-Ext, hence it is not required to configure any explicit PBR rules in the external router for these public IP addresses.

The OAM-VR is required to enable Layer 3 routing to and from the CSCF VNF. The CSCF VNF VM instances of type Controller Profile use static routing so that the OAM-VR routes incoming IP packets towards the CSCF OAM MIP. These IP packets are sent to the Controller Profile VM instances.

As it is required to have a Virtual Routing Function to enable Layer 3 routing, it is also required to have the following two virtual networks to realize Logical Network Operation and Maintenance:

- Virtual Network OAM-Ext – A Virtual Network between external router and OAM-VR.
- Virtual Network OAM – IntMgmt - direct addressing of the VM instances with Controller Profile using public IP addresses.

Figure 3 shows the realization of the logical network setup for operation and maintenance of a 2+2 node system.

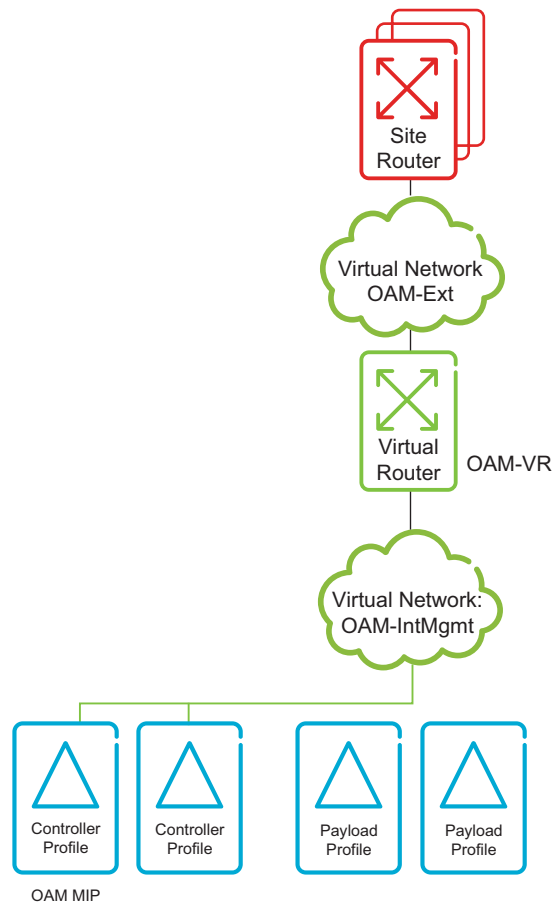


Figure 3 Realization of Logical Network Setup Operation and Maintenance

### 2.4.3

#### Configuration Requirements for Virtual Network OAM-Ext

The following configuration requirements apply to this network:

- Externally accessible



Must be possible to access this network from, for example, the OSS. That is, the CSCF OAM MIP is published to the OSS through this network.

- IP address range

At least one IP address for each of the endpoints is required – external router and OAM-VR.

- Dynamic Host Configuration Protocol (DHCP) Service

DHCP is disabled on this network.

#### 2.4.4 Configuration Requirements for Virtual Network OAM-IntMgmt

The following configuration requirements apply to this network:

- IP address range

IP address range to include at least three endpoints – OAM-VR and two VM instances with Controller Profile.

- DHCP Service

DHCP is disabled on this network.

#### 2.4.5 Configuration Requirements for Virtual Routing Function OAM-VR

The following configuration requirement exists for this virtual routing function:

- Static Routing Rule

PBR rules must be defined that enable routing of IP packets from the CSCF VNF correctly. These PBR rules are CSCF VNF instance-specific and must adhere to the relevant network plan.

## 2.5 Logical Network Signaling

### 2.5.1 Purpose

The purpose of the Logical Network is to enable Session Initiation Protocol (SIP) communication between the CSCF and other Internet Protocol Multimedia Subsystem (IMS) network entities. This network also enables Diameter-based communication between the CSCF, PCRF, and Subscriber Location Function (SLF), or Home Subscriber Server (HSS).

The CSCF VNF exposes the following VIP interface on Logical Network Signaling:

- Interrogating Call Session Control Function (I-CSCF) SIP VIP interface

- Serving Call Session Control Function (S-CSCF) SIP VIP interface
- Emergency Call Session Control Function (E-CSCF) SIP VIP interface
- Break-in Control Function (BCF) SIP VIP interface
- Emergency Access Transfer Function (EATF) SIP VIP interface
- Serving Call Session Control Function (S-CSCF) Diameter SLF/HSS VIP interface
- E-CSCF HTTP VIP interface

## 2.5.2 Description

It is assumed that the external router is configured with a set of PBR rules. These rules send IP packets addressed to the VIP addresses enumerated in Section 2.5.1 Purpose on page 9 to the Virtual Routing Function Signaling (Sig-VR).

SIG-VR is required to enable Layer 3 routing to and from the CSCF VNF. The VM instances of type Payload Profile use static routing such that the SIG-VR routes incoming IP packets towards the CSCF VIP interfaces, and that these IP packets are sent to the Payload Profile VM instances.

It is required to have a Virtual Routing Function to enable Layer 3 routing, it also implies that Logical Network Signaling is realized by the following two Virtual Networks:

- Virtual Network Sig-Ext – A virtual network between external router and SIG-VR.
- Virtual Network Sig-IntVIP – A virtual network between SIG-VR and CSCF VNF. CSCF Signaling VIP addresses on these VM instances are configured using static routing with or without BFD.

Figure 4 shows the realization of the logical network setup for signaling of a 2+2 node system.

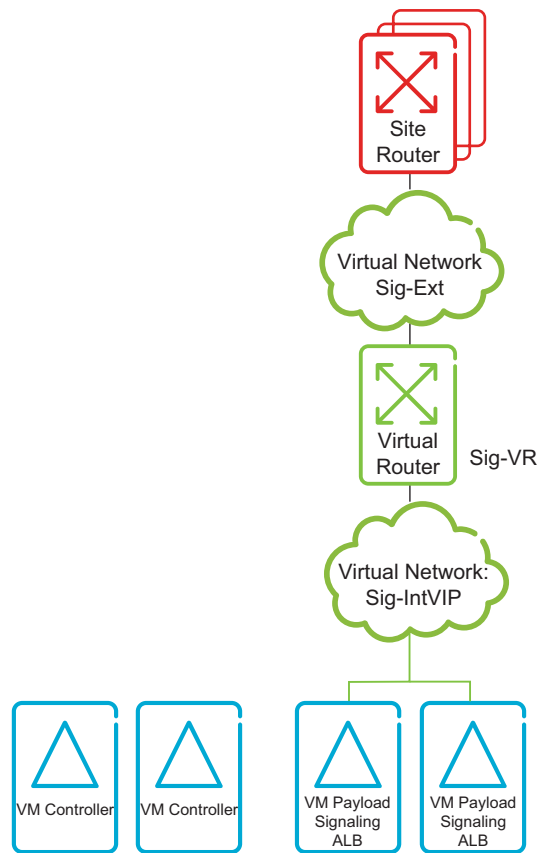


Figure 4 Realization of Logical Network Setup Signaling

### 2.5.3 Configuration Requirements for Virtual Network Sig-Ext

The following configuration requirements apply to this network:

- Externally Accessible

Must be possible to access this network from other IMS network entities such as HSS.

- IP address range

At least one IP address for each of the endpoints is required – external router and SIG-VR.

- DHCP Service

DHCP is disabled on this network.



## 2.5.4 Configuration Requirements for Virtual Network Sig-IntVIP

The following configuration requirements apply to this network:

- IP address range

At least one IP address for each of the endpoints is required – Virtual Routing Function Signaling ALB having Payload Profile installed.

- DHCP Service

DHCP is disabled on this network.

## 2.5.5 Configuration Requirements for Virtual Routing Function Sig-VR

The following configuration requirement exists for this Virtual Routing function:

- Static Routing without BFD
- Static Routing with BFD support

PBR rules must be defined that enables routing of IP packets from the CSCF VNF correctly. These PBR rules are CSCF VNF instance-specific and must adhere to relevant network plan.

# 2.6 Logical Network Charging

## 2.6.1 Purpose

The purpose of this network is to enable Diameter-based communication between the CSCF and Charging Collection Function.

The CSCF VNF exposes the following VIP interface on Logical Network Charging:

- S-CSCF Offline Charging VIP interface
- S-CSCF Online Charging VIP interface
- E-CSCF Offline Charging VIP interface

## 2.6.2 Description

It is assumed that the external router is configured with a set of PBR rules. These rules send IP packets targeted to the VIP addresses enumerated in Section 2.6.1 Purpose on page 12) to Virtual Routing Function Charging (CHA-VR).

CHA-VR is required to enable Layer 3 routing to and from the CSCF VNF. The CSCF VNF VM instances of type Payload Profile are configured using static routing





to communicate with CHA-VR so that incoming IP packets are sent to the VM instances of type Payload Profile.

As it is required to have a Virtual Routing Function to enable Layer 3 routing, it also implies that Logical Network Charging is realized by the following two Virtual Networks:

- Virtual Network Cha-Ext – A Virtual Network between external router and CHA-VR
- Virtual Network Cha-IntVIP – A Virtual Network between CHA-VR and CSCF VNF. VM instances CSCF Signaling VIP addresses are configured using static routing/BFD.

Figure 5 shows the realization of the logical network setup for charging.

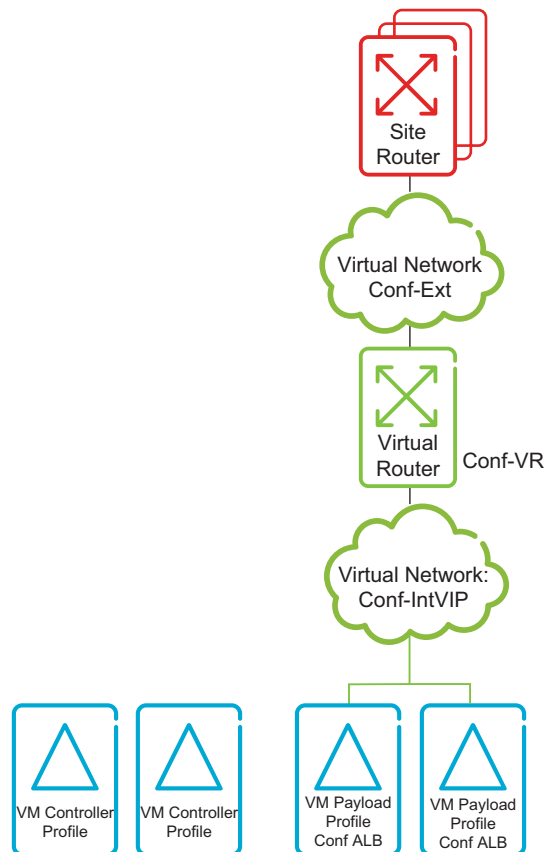


Figure 5 Realization of Logical Network Setup Charging

### 2.6.3 Configuration Requirements for Virtual Network Cha-Ext

The following configuration requirements apply to this network:

- Externally Accessible



Must be possible to access this network from Charging Collection Function and the opposite way.

- IP address range

At least one IP address for each of the endpoints is required – external router and CHA-VR.

- DHCP Service

DHCP is disabled on this network.

## 2.6.4 Configuration Requirements for Virtual Network Cha-IntVIP

The following configuration requirements apply to this network:

- IP address range

IP address range to include at least three endpoints – CHA-VR and at least two VM instances with Payload Profile.

- DHCP Service

DHCP is disabled on this network.

## 2.6.5 Configuration Requirements for Virtual Routing Function Cha-VR

The following configuration requirement exists for this Virtual Routing function:

- Static Routing without BFD
- Static Routing with BFD support

PBR rules must be defined that enables routing of IP packets from the CSCF VNF correctly. These PBR rules are CSCF VNF instance-specific and must adhere to the relevant network plan.

## 2.7 Logical Network Internal

### 2.7.1 Purpose

The purpose of this network is to enable communication between the VM instances that form CSCF VNF. Internal communication, among others, includes communication based on the protocols Transparent Inter-Process Communication (TIPC), Dynamic Host Configuration Protocol (DHCP), Bootstrap Protocol (BOOTP), Trivial File Transfer Protocol (TFTP), and Network File System (NFS).



## 2.7.2 Description

As the purpose of this Logical Network is to enable intra-CSCF VNF communication, Logical Network Internal does not have any external IP connectivity.

**Note:** The Logical Network Internal is unique per CSCF VNF instance. That is, if it is required to deploy two CSCF VNF instances then it is required to create two Logical Network Internal instances.

The communication between VM instances is done by using Layer 2 routing. The result: no Virtual Routing function required and Logical Network Internal can be realized by one Virtual Network (Virtual Network Internal).

Figure 6 shows the realization of the Logical Network Internal setup.

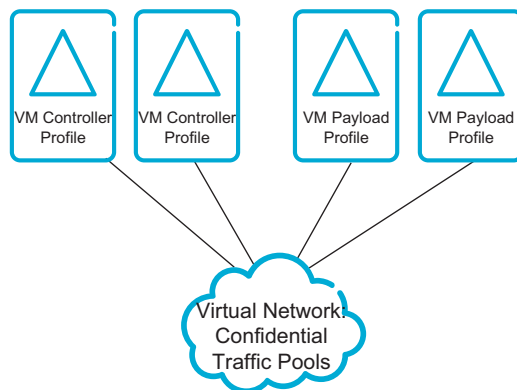


Figure 6 Realization of Logical Network Internal Setup

## 2.7.3 Configuration Requirements for Virtual Network Internal

The following configuration requirements apply to this network:

- IP address range

IP address range to include all VM instances that forms CSCF VNF. IP range must be the same as in `cluster.conf` file.

- DHCP Service

DHCP is disabled on this network. VM instances receive their IP addresses from `cluster.conf` file.

## 2.8 Logical Network Setup in Multiple CSCF VNF Instance Deployment

It is possible to deploy the CSCF VNF multiple times in the same cloud infrastructure, resulting in multiple CSCF VNF instances. Having multiple CSCF

VNF instances deployed in the same cloud infrastructure has some networking implications that must be noted.

It is required that Logical Network Internal and its underlying Virtual Network Internal are unique per CSCF VNF instance. If each CSCF VNF instance is not paired with a unique internal network instance, CSCF VNF instances will malfunction.

For the other Logical Networks, it is more on-site specific networking requirements from the operator and security requirements that apply. It is possible to create dedicated network instances (Virtual Networks and Virtual Routing Functions) per CSCF VNF instance. It is also possible to reuse Virtual Network instances – except for Virtual Network Internal. Another variant is to reuse Virtual Routing Functions and create CSCF VNF instance-specific Virtual Networks.

Create CSCF VNF instance-specific Virtual Networks and Virtual Routing Function. The reason for doing this is to separate the CSCF VNF instances, networking-wise, for security reasons. In this way, there is no logical IP connectivity between the CSCF VNF instances. However, depending on how CSCF VNF instances are deployed, it is possibly not a physical separation between the two instances.

Figure 7 shows CSCF VNF and its logical network setup in a deployment of multiple CSCF VNF instances and when full separation is required.

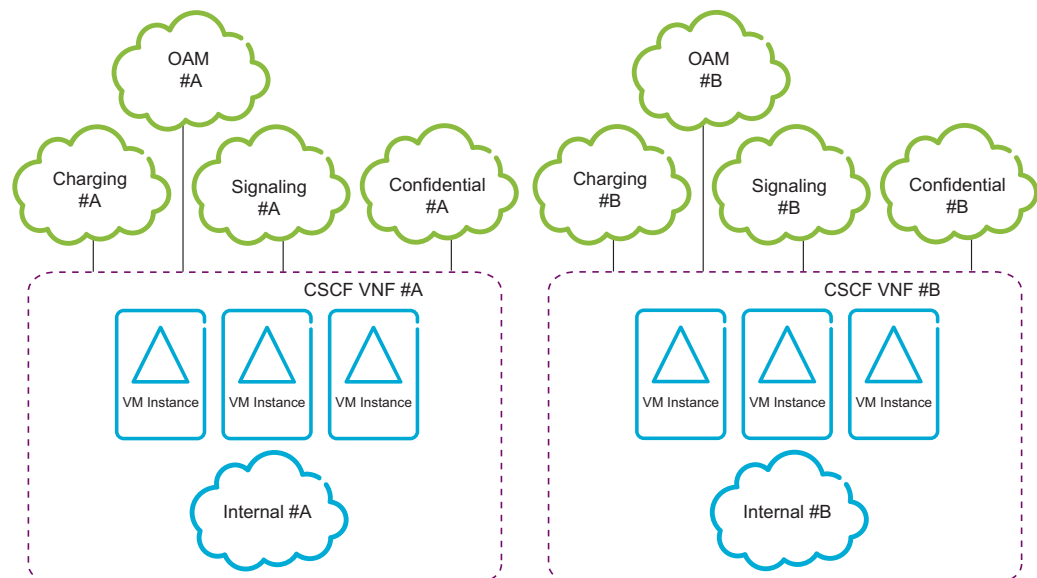


Figure 7 CSCF VNF and Logical Network Setup for Multiple CSCF VNF Instance Deployment When Full Separation Is Required

Figure 8 shows logical network setup signaling combined with deployment of multiple CSCF VNF instances when full separation is required.

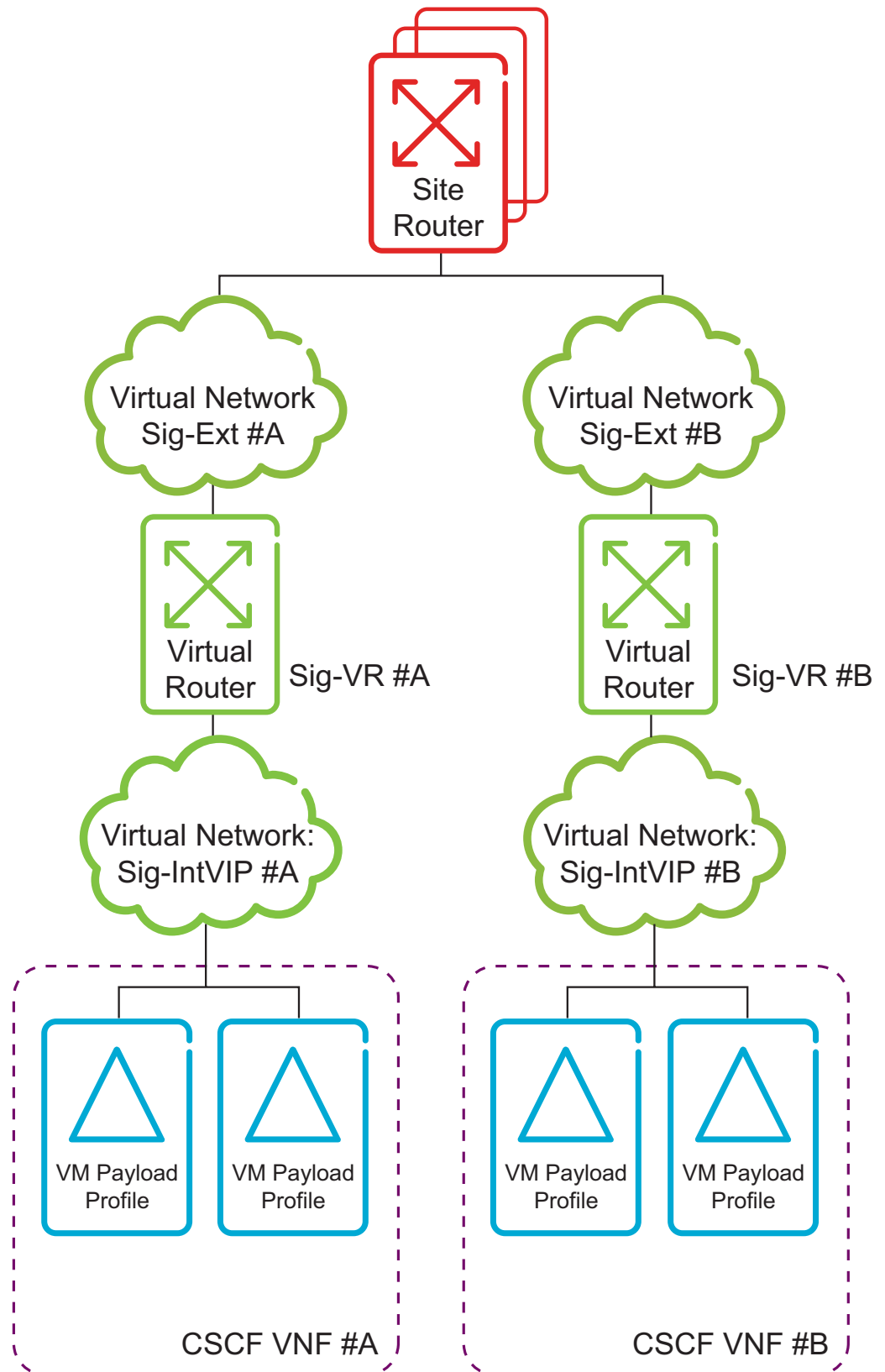


Figure 8 Logical Network Setup Signaling Combined with Deployment of Multiple CSCF VNF Instances When Full Separation Is Required

For the other Logical Networks Operation and Maintenance, Charging, and Confidential, the same pattern as for Signaling applies.

The drawback of these recommendations is that CSCF VNF instances require more Virtual Networks instances. If it is not required to separate the CSCF VNF instances from each other, reuse the network entities between the CSCF VNF instances. However, it is required to have CSCF VNF instance unique Virtual Networks for internal communication. The other networking entities are reused between CSCF VNF entities.

Figure 9 shows CSCF VNF and its logical network setup for multiple CSCF VNF instance deployment and when full separation is not required.

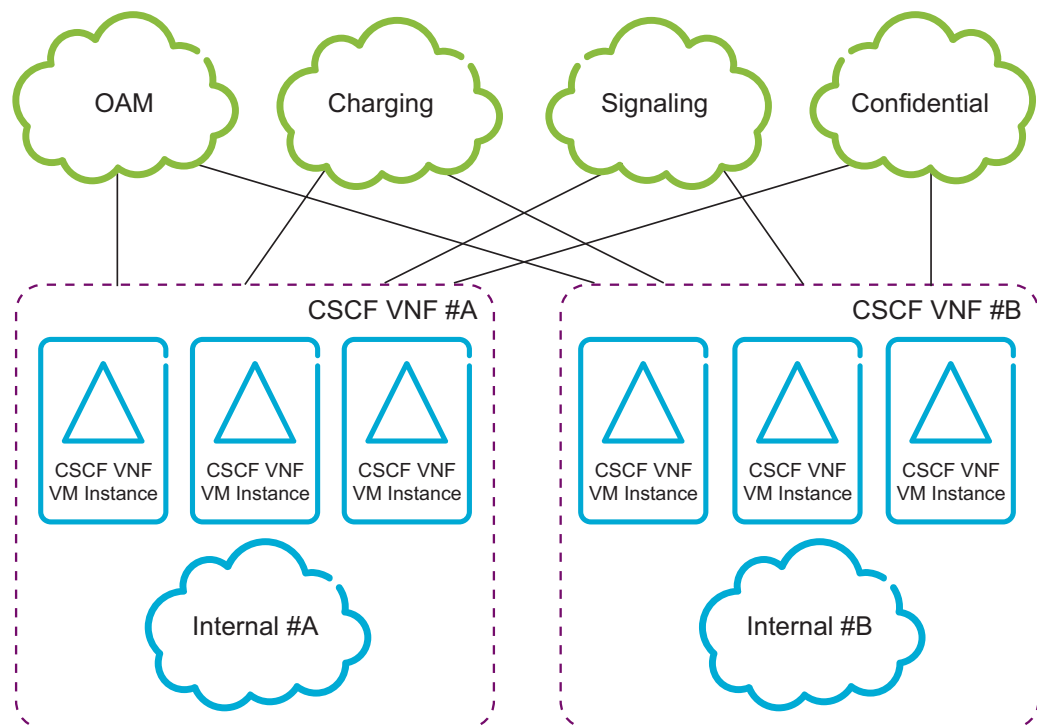


Figure 9 CSCF VNF and Its Logical Network Setup in Case of Multiple CSCF VNF Instance Deployment and When Full Separation Is Not Required

Figure 10 shows logical network setup signaling combined with deployment of multiple CSCF VNF instances when full separation is not required.

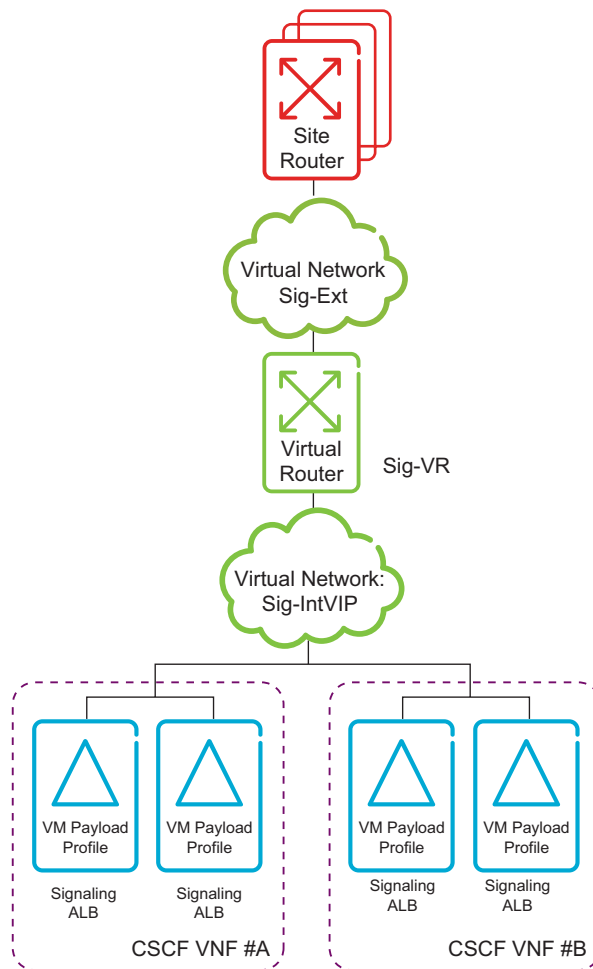


Figure 10 Logical Network Setup Signaling Combined with Deployment of Multiple CSCF VNF Instances When Full Separation Is Not Required

For the other Logical Networks Operation and Maintenance, Charging, and Confidential, the same pattern as for Signaling applies.







## 3 Example Configurations

This section describes example Cloud Networking Infrastructure configurations and deployments.

### 3.1 Static Routing with BFD Configuration

This section gives an example static routing with BFD configuration setup for CSCF VNF, that is when static routing with BFD is enabled in Virtual Routing Function. The actual values used for these parameters can vary depending on the deployment.

In this document, it is assumed that there are two VM instances per VIP address serving as VIP endpoints. Each of these VM instances internally has a VIP FE per VIP address and each VIP FE holds its own static routing with BFD configuration. If there are more than two VM instances per VIP address, the configuration must be adjusted accordingly.

#### 3.1.1 Sig-IntVIP Static Routing with BFD Configuration

This section gives an example Static Routing with BFD configuration for Sig-IntVIP network, as shown in Table 1 and Table 2.

Table 1 Static Routing with BFD Parameters for CSCF VNF Sig FE 3

Static Routing with BFD Parameter	Value
Local Address	192.168.216.3/24
Remote Gateway	192.168.216.1
bfd.RequiredMinEchoRXInterval	0
bfd.DesiredMinTxInterval	300
bfd.RequiredMinRxInterval	300
bfd.DetectMult	3

Table 2 Static Routing with BFD Parameters for CSCF VNF Sig FE 4

Static Routing with BFD Parameter	Value
Local Address	192.168.216.4/24
Remote Gateway	192.168.216.1
bfd.RequiredMinEchoRXInterval	0
bfd.DesiredMinTxInterval	300

Static Routing with BFD Parameter	Value
bfd.RequiredMinRxInterval	300
bfd.DetectMult	3

### 3.1.2 Cha-IntVIP Static Routing with BFD Configuration

This section gives an example Static Routing with BFD configuration for Cha-IntVIP network, as shown in Table 3 and Table 4.

Table 3 Static Routing with BFD Parameters for CSCF VNF Cha FE 3

Static Routing with BFD Parameter	Value
Local Address	192.168.217.3/24
Remote Gateway	192.168.217.1
bfd.RequiredMinEchoRXInterval	0
bfd.DesiredMinTxInterval	300
bfd.RequiredMinRxInterval	300
bfd.DetectMult	3

Table 4 Static Routing with BFD Parameters for CSCF VNF Cha FE 4

Static Routing with BFD Parameter	Value
Local Address	192.168.217.4/24
Remote Gateway	192.168.217.1
bfd.RequiredMinEchoRXInterval	0
bfd.DesiredMinTxInterval	300
bfd.RequiredMinRxInterval	300
bfd.DetectMult	3

### 3.1.3 Static Routing with BFD Configuration SCTP Multi-Homing

The following figure shows the CSCF VNF Virtual IP Access, static routing design for multihomed VIP addresses with BFD enabled.

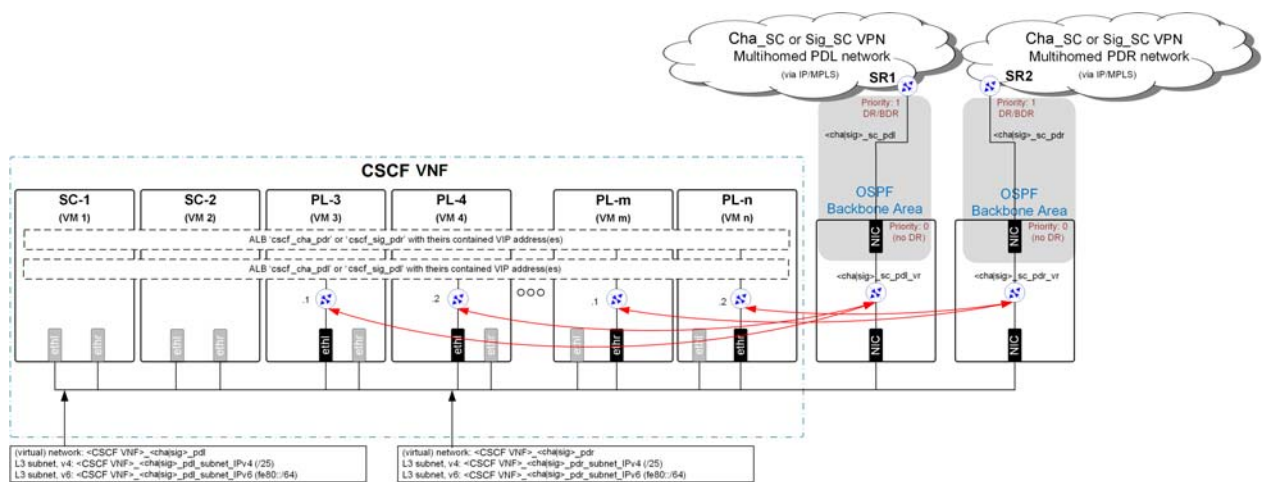


Figure 11 CSCF VNF Virtual IP Access – BFD-Enabled Static Routing Design, Multihomed

The connected PLs embedded routing instances, the FEs are split into the following two groups that consist of two routing instances respectively:

— Group 1, PDL

- The `<cha|sig>_sc_pdl_vr` router is statically configured as default gateway in the FEs of the `cscf_<cha|sig>_pdl` ALB.
- The FEs of the `cscf_<cha|sig>_pdl` ALB are statically configured as possible equal cost next hops towards the provided VIPs in the `<cha|sig>_sc_pdl_vr` router.
- Every statically configured route is protected with single-hop BFD session.

— Group 2, PDR

- The `<cha|sig>_sc_pdr_vr` router is statically configured as default gateway in the FEs of the `cscf_<cha|sig>_pdr` ALB.
- The FEs of the `cscf_<cha|sig>_pdr` ALB are statically configured as possible equal cost next hops towards the provided VIPs in the `<cha|sig>_sc_pdr_vr` router.
- Every statically configured route is protected with single-hop BFD session.

The static routes towards the VIP addresses are imported into separate OSPF routing domains by the `<cha|sig>_sc_pdl_vr` and the `<cha|sig>_sc_pdr_vr` OSPF processes.

## 3.2 Static Routing without BFD Configuration

This section gives an example static routing without BFD configuration setup for CSCF VNF, that is when static routing without BFD is enabled in Virtual Routing



Function. The actual values used for these parameters can vary depending on the deployment.

In this document, it is assumed that there are two VM instances per VIP address serving as VIP endpoints. Each of these VM instances internally has a VIP FE per VIP address and each VIP FE holds its own static routing without BFD configuration. If there are more than two VM instances per VIP address, the configuration must be adjusted accordingly.

### 3.2.1 Sig-IntVIP Static Routing without BFD Configuration

This section gives an example Static Routing without BFD configuration for Sig-IntVIP network, as shown in Table 5 and Table 6.

Table 5 Static Routing without BFD Parameters for CSCF VNF Sig FE 3

Static Routing without BFD Parameter	Value
Local Address	192.168.216.3/24
Remote Gateway	192.168.216.252

Table 6 Static Routing without BFD Parameters for CSCF VNF Sig FE 4

Static Routing without BFD Parameter	Value
Local Address	192.168.216.4/24
Remote Gateway	192.168.216.252

### 3.2.2 Cha-IntVIP Static Routing without BFD Configuration

This section gives an example Static Routing without BFD configuration for Cha-IntVIP network, as shown in Table 7 and Table 8.

Table 7 Static Routing without BFD Parameters for CSCF VNF Cha FE 3

Static Routing without BFD Parameter	Value
Local Address	192.168.217.3/24
Remote Gateway	192.168.217.252



Table 8 Static Routing without BFD Parameters for CSCF VNF Cha FE 4

Static Routing without BFD Parameter	Value
Local Address	192.168.217.4/24
Remote Gateway	192.168.217.252

### 3.2.3 Static Routing without BFD Configuration SCTP Multi-Homing

The following figure shows the CSCF VNF Virtual IP Access, static routing without BFD design for multihomed VIP addresses.

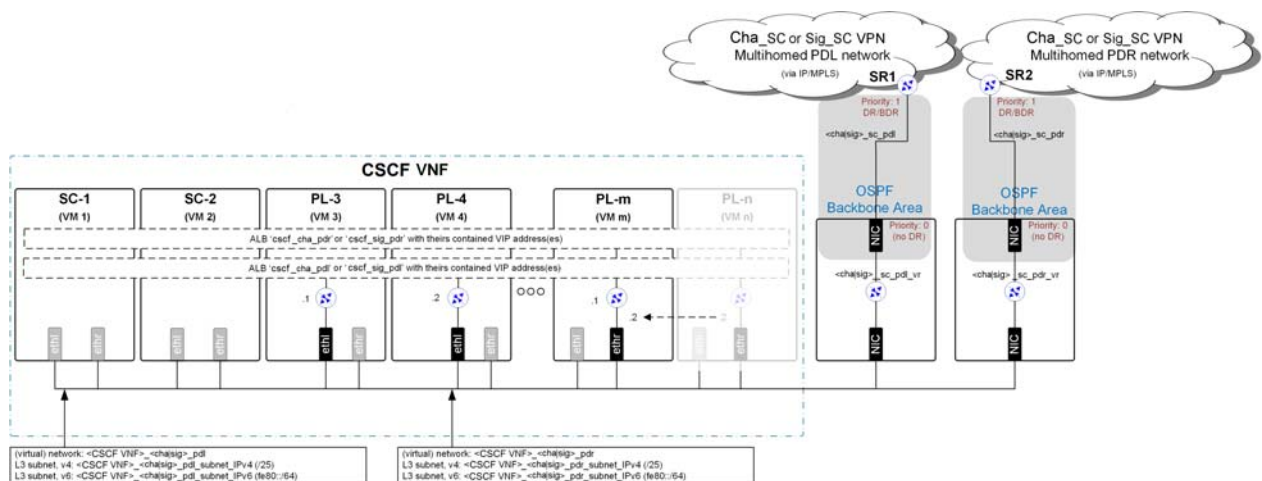


Figure 12 CSCF VNF Virtual IP Access – Static Routing Design, Multihomed VIP Addresses

The fundamental behavior is the same as in the network design for single-homed VIP addresses. However, there are some differences as follows:

#### — Receive direction

- All the FEs are statically configured as possible equal cost next hops towards the `cscf_<cha|sig>_pdl` ALB provided VIPs in the `<cha|sig>_sc_pdl` VIP gateway router.

Similarly, all the FEs are statically configured as possible equal cost next hops towards the `cscf_<cha|sig>_pdr` ALB provided VIPs in the `<cha|sig>_sc_pdr` VIP gateway router.

- If a PL that is hosting an FE is scaled in and there is no free PL exist in the VNF that could host the configured but not instantiated FE, its external interface address is taken over by a still running FE element.

In the figure, consider the case when there are 4 PLs available, and PL-n is scaled in. In this case, the external interface address of the hosted FE is automatically taken over by a still running FE instance that is belonging to the same ALB; in the example, by the FE that is hosted on PL-m.

- With the proper configuration, the VNF guarantees that at least one FE remains for both the `cscf_<cha|sig>_pdl` and the `cscf_<cha|sig>_pdr` ALBs, as a last resort.
- Because of this mechanism, the configured next hop addresses of the VIP routes cannot disappear. Therefore, their availability does not need to be supervised with BFD; all the statically configured next hop addresses towards a VIP can permanently remain in the ECMP group of the VIP gateway.

#### — Sending direction

- The single piece of default gateway address (per INET flavor) that can be configured in the FEs is provided by the adjacent VIP gateway router as follows:
  - For the FEs in the `cscf_<cha|sig>_pdl` ALB, the default route is provided through the `<cha|sig>_sc_pdl` VIP gateway router.
  - For the FEs in the `cscf_<cha|sig>_pdr` ALB, the default route is provided through the `<cha|sig>_sc_pdr` VIP gateway router.

The static routes towards the VIP addresses are imported into the separate OSPF routing domains by the `<cha|sig>_sc_pdl` and `<cha|sig>_sc_pdr` OSPF processes.

### SCTP Multi-Homing, Double-Failure Scenario

A double-failure scenario needs to be considered when there is only one PL remaining in the system. See the use case depicted in the following figure:

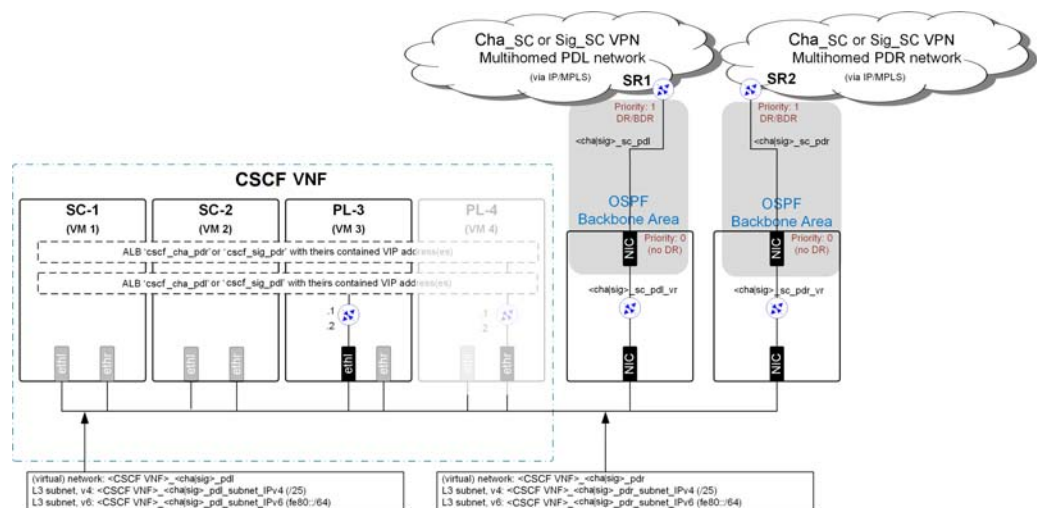


Figure 13 Double-failure Scenario Use Case

Let us assume that the VNF contains two PLs only, and these are hosting two FEs that are belonging to the `cscf_<cha|sig>_pdl` and the `cscf_<cha|sig>_pdr` ALBs. The external interface addresses of the not instantiated FE entities are



stacked, because of the limited number of available PLs. Assume that PL-4 becomes unavailable. In that situation, the VIP external connectivity over the PDR network is broken. The higher-level SCTP protocol embedded mechanism detects the path failure, resulting in an active path reselection over the still established SCTP associations.

### 3.3 Dynamic Routing Design

The reference dynamic routing design is used to solve the constraint that virtual OSPF links cannot be configured in the FEs. Hence, the VIP gateway routers must be connected to the OSPF backbone, owing to that every OSPF area must be connected to the backbone.

Preferably, OSPF must be combined with BFD to achieve faster forwarding path failure detection.

#### 3.3.1 Dynamic Routing for Single-Homed VIP Addresses

Figure 14 shows the CSCF VNF Virtual IP Access, dynamic routing design for single-homed VIP addresses.

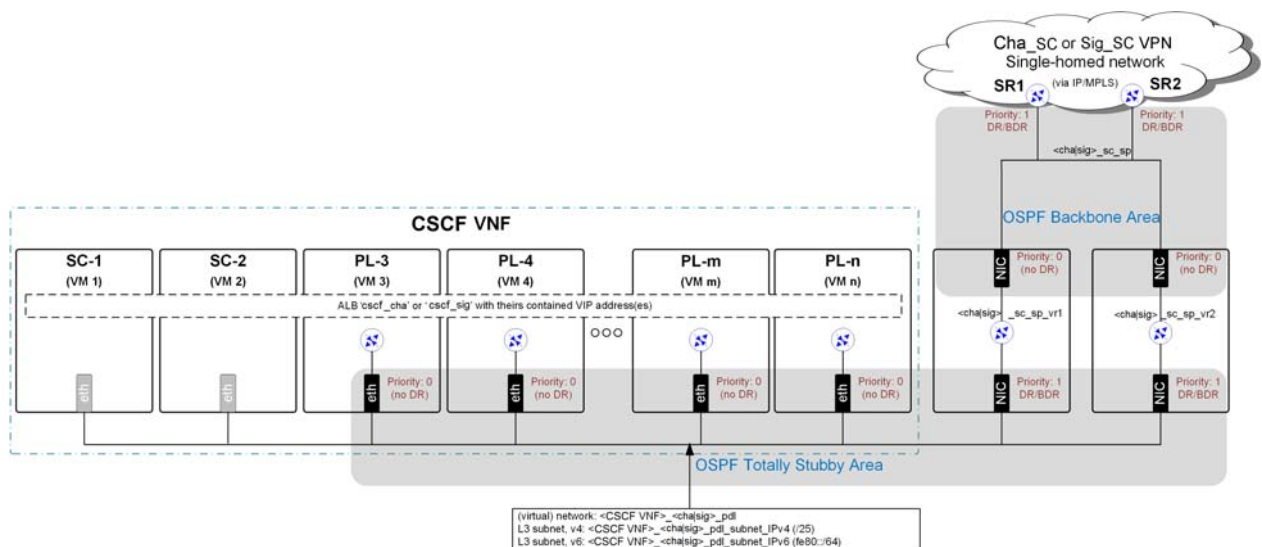


Figure 14 CSCF VNF Virtual IP Access – Dynamic Routing Design, Single-Homed

The <sig|cha>\_sc\_sp\_vr1 and the <sig|cha>\_sc\_sp\_vr2 routing instances are Area Border Routers (ABRs) in the following areas:

— OSPF Totally Stubby Area

- To minimize the load on CSCF VNF routing instances by hiding the OSPF topological changes from them as much as possible, ensure the following:

- The priority of the OSPF interfaces of the PLs embedded routing instances is set to 0. With this setting, they are never selected as DR or BDR inside the area.
- The OSPF area, between the PLs embedded and the soft router instances, is defined as a Totally Stubby Area (area <X.Y.Z.W> stub no-summary). With this setting, the following occur:
  - Only type 1 and type 2 Link-State Advertisements (LSAs) are exchanged inside the area. The size of the link state database of the PLs embedded routing instances can be minimized.
  - All routing out of the area relies on the redundant default routes that injected by the ABRs.
- The VIP addresses that are collected in the `cscf_<sig|cha>` ALB, as connected /32 (IPv4) and /128 (IPv6) stubs, are injected into OSPF by the CSCF VNF routing instances with LSA Type 1 (Router LSA).
- Backbone
  - To minimize the load on the soft routers upon OSPF topological changes in the backbone area, the priority of the backbone interfaces is set to 0. With this setting, they are never selected as DR or BDR inside the backbone area.
  - All routing out of the IMS Central Module (Site) relies on the default routes that are injected into OSPF by the Site Routers (default-information originate).

### 3.3.2 Dynamic Routing for Multihomed VIP Addresses

Figure 15 shows the CSCF VNF Virtual IP Access, dynamic routing design for multihomed VIP addresses.

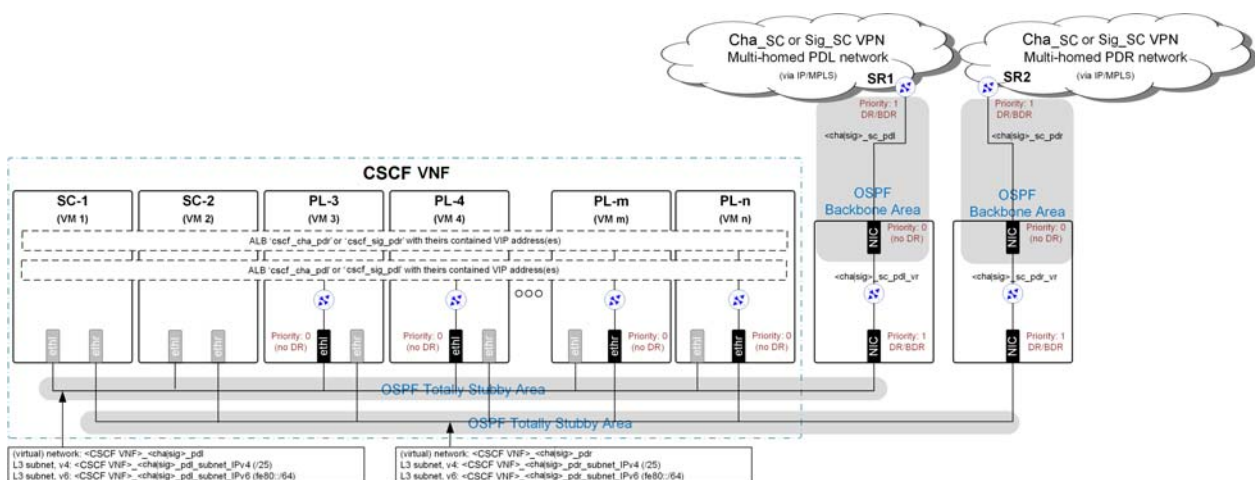


Figure 15 CSCF VNF Virtual IP Access – Dynamic Routing Design, Multihomed





The routing does not differ fundamentally from the single-homed scenario. The only difference in this scenario is the following VIP addresses are injected into different routing domains as connected /32 (IPv4) and /128 (IPv6) stubs:

- The VIP addresses that are collected in the `cscf_<cha|sig>_pd1` ALBs
- The VIP addresses that are collected in the `cscf_<cha|sig>_pdr` ALBs

## 3.4 OpenStack Deployment

This section describes how to configure the different networks in OpenStack context. That is, when CSCF VNF is deployed in an OpenStack cloud, it can be deployed in the Ericsson Cloud System cloud or some other OpenStack based cloud.

**Note:** In the following sections, it is assumed that only one CSCF VNF instance is deployed in the cloud. That is, the names/identifiers are not denoted with instance identifiers in this document. If multiple CSCF VNF instances are to be deployed into the same cloud, it is recommended to prefix all names/identifiers with the CSCF VNF instance name, for example, Karlstad-City-OAM-Ext.

### 3.4.1 Example Data Used

In the following sections, the provided example configuration data is based on the CSCF VNF configuration as shown in Table 9.

Table 9 Configuration Values Used in the Example

CSCF VNF Parameter	Value
System Management net	10.50.41.48/29
CSCF OAM MIP	10.50.41.50
System Management SC-1	10.50.41.51
System Management SC-2	10.50.41.52
I-CSCF SIP VIP	10.50.41.202
S-CSCF SIP VIP	10.50.41.203
S-CSCF HSS VIP	10.50.41.204
S-CSCF Offline Charging VIP	10.50.41.205
S-CSCF Online Charging VIP	10.50.41.206
E-CSCF SIP VIP	10.50.41.208
OAM-VR IP (Ext)	172.16.5.6
External router OAM GW	172.16.5.5
Signaling eVIP FEE-3 IP	192.168.216.3



CSCF VNF Parameter	Value
Signaling eVIP FEE-4 IP	192.168.216.4
Sig-VR IP (Int)	192.168.216.1
Sig-VR IP (Ext)	172.16.5.2
External router Sig GW	172.16.5.1
Charging eVIP FEE-3 IP	192.168.217.3
Charging eVIP FEE-4 IP	192.168.217.4
Cha-VR IP (Int)	192.168.246.1
Cha-VR IP (Ext)	172.16.5.26
Site Router Cha GW	172.16.5.25
Internal Net (cluster.conf)	169.254.100.0/24
Confidential eVIP FEE-3 IP <sup>(1)</sup>	192.168.219.x
Confidential eVIP FEE-4 IP <sup>(1)</sup>	192.168.219.x

(1) Descriptions of the confidential network are outside the scope of this document. For information on the confidential network, refer to LI documentation.

### 3.4.2

#### Configuration of Logical Network Operation and Maintenance

Figure 16 shows an overview of the OpenStack/Neutron building blocks that are used to build Logical Network O&M.

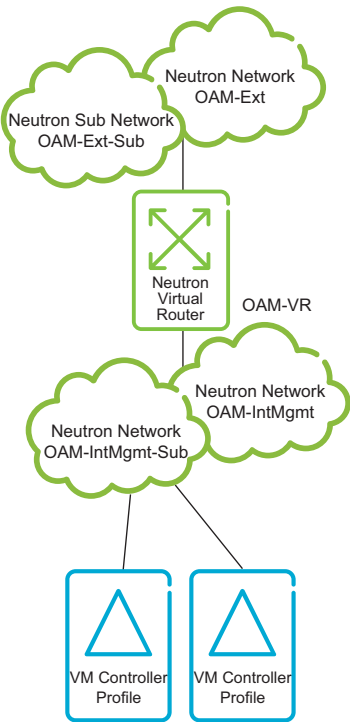


Figure 16 Logical Network Setup Operational and Maintenance Built by Neutron Components

3.4.2.1

Configuration of Virtual Network OAM-Ext

The following configuration settings are recommended for OAM-Ext network in OpenStack context.

Table 10 Recommended Values for Neutron Net-Create Command

OpenStack Parameter	Recommended Value
Name	OAM-Ext
prefix	As required
shared	FALSE
tenant_id	As required
provider:network_type	Vlan
provider:physical_network	As required
provider:segmentation_id	As required
router:external	TRUE

Table 11 Recommended Values for Neutron Subnet-Create Command

OpenStack Parameter	Recommended Value
Name	OAM-Ext-Sub



OpenStack Parameter	Recommended Value
Network	OAM-Ext
CIDR	As required – for example 172.16.5.4/30
prefix	As required
tenant_id	As required
gateway	As required – for example 172.16.5.5/32
allocation-pool	As required – for example start=172.16.5.6 end=172.16.5.7
host-route	Not used
dns-nameserver	Not used
disable-dhcp	Used (no parameter value)
ip-version	As required

### 3.4.2.2 Configuration of Virtual Network OAM-IntMgmt

The following configuration settings are recommended for OAM-IntMgmt network in OpenStack context.

Table 12 Recommended Values for Neutron Net-Create Command

OpenStack Parameter	Recommended Value
Name	OAM-IntMgmt
prefix	As required
shared	FALSE
tenant_id	As required
provider:network_type	Not used
provider:physical_network	Not used
provider:segmentation_id	Not used
router:external	TRUE

Table 13 Recommended Values for Neutron Subnet-Create Command

OpenStack Parameter	Recommended Value
Name	OAM-IntMgmt-Sub
Network	OAM-IntMgmt
CIDR	As required – for example 192.168.0.0/29



OpenStack Parameter	Recommended Value
prefix	As required
tenant_id	As required
allocation-pool	As required – for example start=192.168.0.1 end=192.168.0.3
host-route	Not used
dns-nameserver	Not used
disable-dhcp	Used (no parameter value)
ip-version	As required

### 3.4.2.3 Configuration of Virtual Router OAM-VR

The following configuration settings are recommended for OAM-VR network in OpenStack context.

Table 14 Recommended Values for Neutron Router-CREATE Command

OpenStack Parameter	Recommended Value
Name	OAM-VR

Table 15 Recommended Values for Neutron Router-Interface-Add Command

OpenStack Parameter	Recommended Value
router-id	OAM-VR
interface	OAM-Ext

Table 16 Recommended Values for Neutron Router-Interface-Add Command

OpenStack Parameter	Recommended Value
router-id	OAM-VR
interface	OAM-IntMgmt

Table 17 Recommended Values for Neutron Router-Gateway-Set Command

OpenStack Parameter	Recommended Value
router-id	OAM-VR
external-network-id	OAM-Ext

### 3.4.3 Configuration of Logical Network Signaling

Figure 17 shows an overview of the OpenStack building blocks that are used to build Logical Network Signaling.

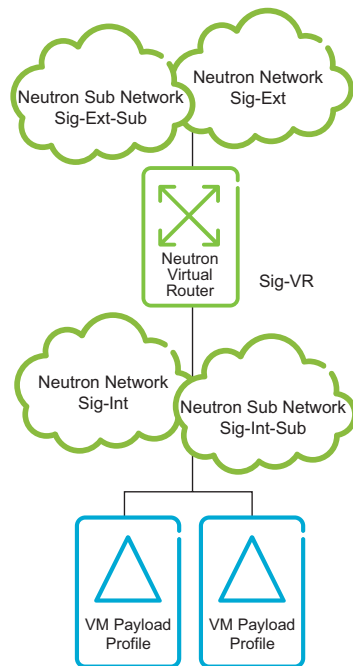


Figure 17 Logical Network Setup Signaling Built by Neutron Components

### 3.4.3.1 Configuration of Virtual Network Sig-Ext

The following configuration settings are recommended for Sig-Ext network in OpenStack context.

Table 18 Recommended Values for Neutron Net-Create Command

OpenStack Parameter	Recommended Value
Name	Sig-Ext
prefix	As required
shared	FALSE
tenant_id	As required
provider:network_type	Vlan
provider:physical_network	As required
provider:segmentation_id	As required
router:external	TRUE

Table 19 Recommended Values for Neutron Subnet-Create Command

OpenStack Parameter	Recommended Value
Name	Sig-Ext-Sub
Network	Sig-Ext



OpenStack Parameter	Recommended Value
CIDR	As required – for example 172.16.5.2/30
prefix	As required
tenant_id	As required
gateway	As required – for example 172.16.5.1/32
allocation-pool	As required – for example start=172.16.5.1 end=172.16.5.2
host-route	Not used
dns-nameserver	Not used
disable-dhcp	Used (no parameter value)
ip-version	As required

### 3.4.3.2

#### Configuration of Virtual Network Sig-IntVIP

The following configuration settings are recommended for Sig-IntVIP network in OpenStack context.

Table 20 Recommended Values for Neutron Net-Create Command

OpenStack Parameter	Recommended Value
Name	Sig-IntVIP
prefix	As required
shared	FALSE
tenant_id	As required
provider:network_type	Not used
provider:physical_network	Not used
provider:segmentation_id	Not used
router:external	TRUE

Table 21 Recommended Values for Neutron Subnet-Create Command

OpenStack Parameter	Recommended Value
Name	Sig-IntVIP-Sub
Network	Sig-IntVIP
CIDR	As required – for example 192.168.216.0/29
prefix	As required

OpenStack Parameter	Recommended Value
tenant_id	As required
allocation-pool	As required – for example start=192.168.216.3 end=192.168.216.11
host-route	Not used
dns-nameserver	Not used
disable-dhcp	Used (no parameter value)
ip-version	As required

### 3.4.3.3 Configuration of Virtual Router Sig-VR

The following configuration settings are recommended for Sig-VR in OpenStack context.

Table 22 Recommended Values for Neutron Router-Create Command

OpenStack Parameter	Recommended Value
Name	Sig-VR

Table 23 Recommended Values for Neutron Router-Interface-Add Command

OpenStack Parameter	Recommended Value
router-id	Sig-VR
interface	Sig-Ext

Table 24 Recommended Values for Neutron Router-Interface-Add Command

OpenStack Parameter	Recommended Value
router-id	Sig-VR
interface	Sig-IntVIP

Table 25 Recommended Values for Neutron Router-Gateway-Set Command

OpenStack Parameter	Recommended Value
router-id	Sig-VR
external-network-id	Sig-Ext

Table 26 Recommended Values for Neutron Staticroute-Create Command

OpenStack Parameter	Recommended Value
ID	Sig-VR
destination <sup>(1)</sup>	10.50.41.201/32





OpenStack Parameter	Recommended Value
nexthop	192.168.216.3
destination	10.50.41.201/32
nexthop	192.168.216.11
Destination	10.50.41.202/32
nexthop	192.168.216.3
destination	10.50.41.202/32
nexthop	192.168.216.11
destination	10.50.41.203/32
nexthop	192.168.216.3
destination	10.50.41.203/32
nexthop	192.168.216.11
destination	10.50.41.208/32
nexthop	192.168.216.3
destination	10.50.41.208/32
nexthop	192.168.216.11

(1) Nexthop and destination are configured in pairs.

### 3.4.4

### Configuration of Logical Network Charging

Figure 18 shows an overview of the OpenStack building blocks that are used to build Logical Network Charging.

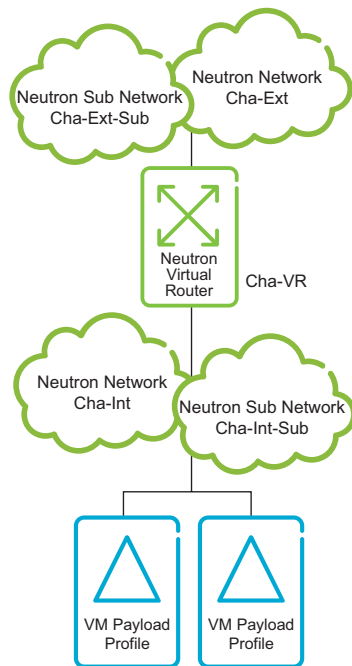


Figure 18 Logical Network Setup Charging Built by Neutron Components

### 3.4.4.1 Configuration of Virtual Network Cha-Ext

The following configuration settings are recommended for Cha-Ext network in OpenStack context.

Table 27 Recommended Values for Neutron Net-Create Command

OpenStack Parameter	Recommended Value
Name	Cha-Ext
prefix	As required
shared	FALSE
tenant_id	As required
provider:network_type	Vlan
provider:physical_network	As required
provider:segmentation_id	As required
router:external	TRUE

Table 28 Recommended Values for Neutron Subnet-Create Command

OpenStack Parameter	Recommended Value
Name	Cha-Ext-Sub
Network	Cha-Ext



OpenStack Parameter	Recommended Value
CIDR	As required – for example 172.16.5.24/30
prefix	As required
tenant_id	As required
gateway	As required – for example 172.16.5.25/32
allocation-pool	As required – for example start=172.16.5.25 end=172.16.5.26
host-route	Not used
dns-nameserver	Not used
disable-dhcp	Used (no parameter value)
ip-version	As required

### 3.4.4.2

#### Configuration of Virtual Network Cha-IntVIP

The following configuration settings are recommended for Cha-IntVIP network in OpenStack context.

Table 29 Recommended Values for Neutron Net-Create Command

OpenStack Parameter	Recommended Value
Name	Cha-IntVIP
prefix	As required
shared	FALSE
tenant_id	As required
provider:network_type	Not used
provider:physical_network	Not used
provider:segmentation_id	Not used
router:external	TRUE

Table 30 Recommended Values for Neutron Subnet-Create Command

OpenStack Parameter	Recommended Value
Name	Cha-IntVIP-Sub
Network	Cha-IntVIP
CIDR	As required – for example 192.168.246.0/29
prefix	As required

OpenStack Parameter	Recommended Value
tenant_id	As required
allocation-pool	As required – for example start=192.168.246.3 end=192.168.246.11
host-route	Not used
dns-nameserver	Not used
disable-dhcp	Used (no parameter value)
ip-version	As required

### 3.4.4.3 Configuration of Virtual Router Cha-VR

The following configuration settings are recommended for Cha-VR in OpenStack context.

Table 31 Recommended Values for Neutron Router-Creat Command

OpenStack Parameter	Recommended Value
Name	Cha-VR

Table 32 Recommended Values for Neutron Router-Interface-Add Command

OpenStack Parameter	Recommended Value
router-id	Cha-VR
interface	Cha-Ext

Table 33 Recommended Values for Neutron Router-Interface-Add Command

OpenStack Parameter	Recommended Value
router-id	Cha-VR
interface	Cha-IntVIP

Table 34 Recommended Values for Neutron Router-Gateway-Set Command

OpenStack Parameter	Recommended Value
router-id	Cha-VR
external-network-id	Cha-Ext

Table 35 Recommended Values for Neutron Staticroute-Creat Command

OpenStack Parameter	Recommended Value
ID	Cha-VR
destination <sup>(1)</sup>	10.50.41.205/32

OpenStack Parameter	Recommended Value
nexthop	192.168.246.3
destination	10.50.41.205/32
nexthop	192.168.246.11
Destination	10.50.41.206/32
nexthop	192.168.246.3
destination	10.50.41.206/32
nexthop	192.168.246.11

(1) Nexthop and destination are configured in pairs.

### 3.4.5 Configuration of Logical Network Internal

Figure 19 shows an overview of the OpenStack building blocks that are used to build Logical Network Internal.

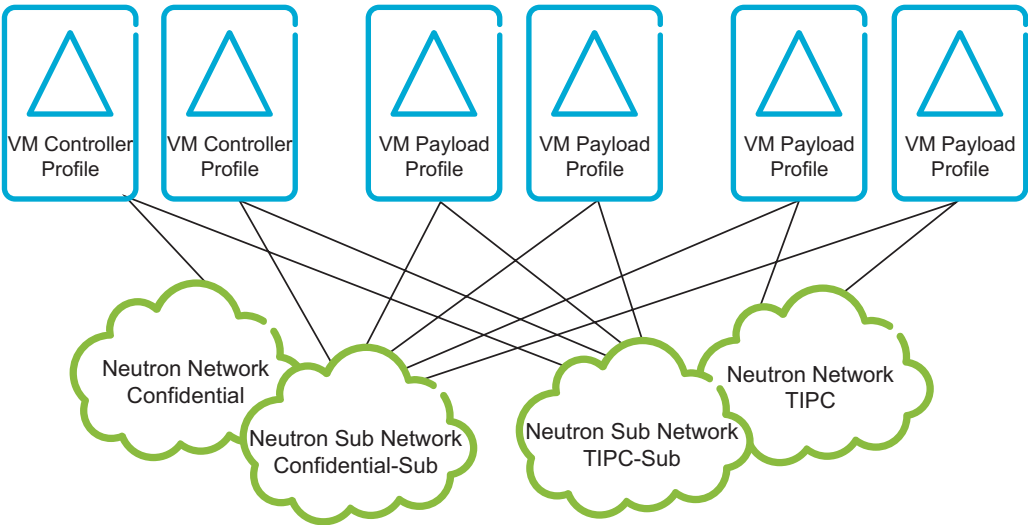


Figure 19 Logical Network Setup Internal Built by Neutron Components

#### 3.4.5.1 Configuration of Virtual Network Internal

The following configuration settings are recommended for Internal network in OpenStack context.

Table 36 Recommended Values for Neutron Net-Create Command

OpenStack Parameter	Recommended Value
Name	Internal
prefix	As required
shared	FALSE



OpenStack Parameter	Recommended Value
tenant_id	As required
provider:network_type	Vlan
provider:physical_network	As required
provider:segmentation_id	As required
router:external	TRUE

Table 37 Recommended Values for Neutron Subnet-Create Command

OpenStack Parameter	Recommended Value
Name	Internal-Sub
Network	Internal
CIDR	As required – for example 169.254.100.0/24
prefix	As required
tenant_id	As required
gateway	Not used
allocation-pool	As required – for example start=169.254.100.1 end=169.254.100.254
host-route	Not used
dns-nameserver	Not used
disable-dhcp	Used (no parameter value)
ip-version	As required

## 3.5 Equal-Cost Multipath Considerations

The CSCF VNF requires that flow-based ECMP is applied for TCP sessions, SCTP streams, and for fragmented UDP packets. This is needed as CSCF VNF requires that all IP packets from a TCP packet flow or SCTP packet flow or fragmented UDP packet flow are received on the same CSCF VNF instance (all packets within the flow are sent to the same CSCF VNF instance).

It is assumed in this document, that all networking routing entities support flow-based Equal-Cost Multipath for TCP, as this is a de facto standard for the TCP. The following subsections give some examples of the network configuration when it is not possible to use flow-based ECMP.

**Note:** This is not required for UDP packets that are not fragmented.



### 3.5.1 Avoid Fragmented UDP Packets through Using TCP

In the CSCF VNF implementation, the eVIP FE implementation reassembles fragmented UDP packets before passing it on to CSCF application logic. As the eVIP FE runs on multiple VM instances, it is required that all UDP fragments are received by the same VM instance.

If it is not possible to achieve flow-based Equal-Cost Multipath for fragmented UDP packets, it is required to use TCP instead of UDP. This implies that any SIP communication to and from the CSCF VNF that can result in IP fragmentation, must use TCP. The DNS server and other network entities must be configured for TCP. It is also required to change CSCF configuration: set `cscfSendRequestUdpOnly` to `false`.

Do not use the DF (Do not Fragment) flag in the IP header to avoid fragmentation. The CSCF VNF is able to receive IP packets of the path MTU size (typically 1500 bytes) and then fragment the IP packets according to an internal MTU size of about 1452 bytes. If the received packet MTU size is larger than internal MTU size of 1452 bytes and the DF bit is set, the CSCF discards the IP packet.

Use TCP if the SIP message size is above 1300 bytes. This is also indicated in [RFC3261](#).

### 3.5.2 Avoid Fragmented SCTP Packets through Using TCP

The problem for fragmented UDP packets as mentioned in section Section 3.5.1 Avoid Fragmented UDP Packets through Using TCP on page 43, also applies to SCTP for the same reason. If it is not possible to use flow-based ECMP for SCTP stream, it is required to use TCP instead of SCTP. This implies that communication between the CSCF VNF and SLF/HSS must use TCP.

**Note:** The SLF or HSS, or both, possibly must be reconfigured for TCP.

### 3.5.3 Configure Network Routing in a Active/Standby Pattern

An alternative way to solve the fragmentation, is to define one of the CSCF Signaling VMs as primary destination for all IP packets. The other VM instance of the same type is then defined as secondary destination. If there are three instances of this type, define the third instance as tertiary destination. Primary, secondary, and optionally tertiary destinations are in this context defined as PBR in the external router.

The drawback of this type of solution is that, whenever a fault happens (for example an unexpected termination of the VM instance which is the primary destination), it results in the loss of all TCP connections (for example Diameter connections to SLF/HSS). Then the connections must be reestablished and this takes some time. That is why this setup is not the default configuration.