ETSI GR NFV-IFA 022 V3.1.1 (2018-04)

Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on Management and Connectivity for Multi-Site Services

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/NFV-IFA022

Keywords
interface, management, NFV, orchestration, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
oneM2M logo is protected for the benefit of its Members.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 7
Foreword 7
Modal verbs terminology 7
1 Scope 8
2 References 8
2.1 Normative references 8
2.2 Informative references 8
3 Definitions and abbreviations 10
3.1 Definitions 10
3.2 Abbreviations 10
4 Overview 11
4.1 Introduction 11
5 Use Cases 12
5.1 Introduction 12
5.2 Use Case 1: Network Service for E2E Enterprise virtual Customer Premises Equipment (vCPE) 12
5.2.1 Introduction 12
5.2.2 Trigger 14
5.2.3 Actors and roles 14
5.2.4 Pre-conditions 15
5.2.5 Post-conditions 15
5.2.6 Operational Flows 15
5.2.7 Other Considerations 20
5.2.7.1 Network Service Instance Description 20
5.2.7.2 Infrastructure Description 20
5.2.7.3 Mapping of Service Instance Model to Supporting Infrastructure 21
5.2.7.4 Management Architecture and Activities 22
5.2.8 Analysis 23
5.3 Use Case 2: Network Service for E2E Enterprise vCPE across two WANs 26
5.3.1 Introduction 26
5.3.2 Trigger 28
5.3.3 Actors and roles 28
5.3.4 Pre-conditions 28
5.3.5 Post-conditions 28
5.3.6 Operational Flows 29
5.3.7 Other Considerations (e.g. Performance) 29
5.3.8 Analysis 29
5.4 Use Case 3: NS Expansion to other NFVI-PoPs over WAN 31
5.4.1 Introduction 31
5.4.2 Trigger 32
5.4.3 Actors and roles 32
5.4.4 Pre-conditions 33
5.4.5 Post-conditions 33
5.4.6 Operational Flows 33
5.4.7 Other Considerations (e.g. Performance) 34
5.4.8 Analysis 34
5.5 Use case 4: Network Service Virtual Link aggregation 34
5.5.1 Introduction 34
5.5.2 Trigger 35
5.5.3 Actors and roles 35
5.5.4 Pre-conditions 36
5.5.5 Post-conditions 36
5.5.6 Operational Flows 36
5.5.7 Other Considerations (e.g. Performance) 36
5.5.8 Analysis 37

5.6 Use case 5: Checking multi-site connectivity....38
5.6.1 Introduction....38
5.6.2 Trigger....39
5.6.3 Actors and roles....39
5.6.4 Pre-conditions....39
5.6.5 Post-conditions....39
5.6.6 Operational Flows....40
5.6.7 Other Considerations (e.g. Performance)....40
5.6.8 Analysis....40
5.7 Use case 6: Multi-site Virtual Link redundancy....41
5.7.1 Introduction....41
5.7.2 Trigger....42
5.7.3 Actors and roles....42
5.7.4 Pre-conditions....43
5.7.5 Post-conditions....43
5.7.6 Operational Flows....43
5.7.7 Other Considerations (e.g. Performance)....43
5.7.8 Analysis....44
5.8 Use case 7: Multi-site Virtual Link healing....45
5.8.1 Introduction....45
5.8.2 Trigger....47
5.8.3 Actors and roles....47
5.8.4 Pre-conditions....47
5.8.5 Post-conditions....48
5.8.6 Operational Flows....48
5.8.7 Other Considerations (e.g. Performance)....49
5.8.8 Analysis....49
5.9 Use case 8: Multi-site VNF deployment....50
5.9.1 Introduction....50
5.9.2 Trigger....52
5.9.3 Actors and roles....52
5.9.4 Pre-conditions....53
5.9.5 Post-conditions....53
5.9.6 Operational Flows....53
5.9.7 Other Considerations (e.g. Performance)....55
5.9.8 Analysis....55
5.10 Use case 9: Addressing multi-site deployment requirements in NSDs....56
5.10.1 Introduction....56
5.10.2 Trigger....56
5.10.3 Actors and roles....57
5.10.4 Pre-conditions....57
5.10.5 Post-conditions....57
5.10.6 Operational Flows....57
5.10.7 Other Considerations (e.g. Performance)....57
5.10.8 Analysis....57
5.11 Use Case 10: User Equipment (UE) Location Triggered Network Service Migration Across NFVI PoPs....60
5.11.1 Introduction....60
5.11.2 Triggers....61
5.11.3 Actors and roles....62
5.11.4 Pre-conditions....62
5.11.5 Post-conditions....63
5.11.6 Operational Flows....63
5.11.7 Other Considerations (e.g. Performance)....64
5.11.8 Analysis....64
5.12 Use case 11: Modification to the WAN Connectivity Resource of a Multi-site NS....65
5.12.1 Introduction....65
5.12.2 Trigger....65
5.12.3 Actors and roles....65
5.12.4 Pre-conditions....66
5.12.5 Post-conditions....66
5.12.6 Operational Flows....66
5.12.7 Other Considerations (e.g. Performance)....67

5.12.8 Analysis 67
5.13 Use Case 12: Network Service for virtual Radio Access Network (vRAN) 67
5.13.1 Introduction 67
5.13.2 Trigger 69
5.13.3 Actors and roles 69
5.13.4 Pre-conditions 70
5.13.5 Post-conditions 70
5.13.6 Operational Flows 70
5.13.7 Other Considerations (e.g. Performance) 72
5.13.8 Analysis 72
5.14 Use case 13: Use of WAN connectivity by compute-only NFVI-PoP deployments 73
5.14.1 Introduction 73
5.14.2 Trigger 74
5.14.3 Actors and roles 75
5.14.4 Pre-conditions 75
5.14.5 Post-conditions 75
5.14.6 Operational Flows 76
5.14.7 Other Considerations (e.g. Performance) 76
5.14.8 Analysis 77
6 Analysis 78
6.1 Use Case analysis with a focus on the NFV-MANO functions 78
6.2 Analysis about WIM role 79
6.2.1 Existing concept of WIM and Network Controller 79
6.2.2 Analysis about connectivity service decomposition 79
6.2.3 Analysis about WIM role in multi-site connectivity 80
6.3 Potential architecture options 81
6.3.1 Introduction 81
6.3.2 Architecture option #A: WIM integration as specialized VIM 81
6.3.3 Architecture option #B: Managing WIM functionality of OSS/BSS with Os-Ma-nfvo reference points 83
6.4 Information modelling analysis 85
6.4.1 General 85
6.4.2 Gap analysis and extensions to NSD and VNFD 85
6.4.2.1 Current connectivity model in the NSD (IFA 014) 85
6.4.2.2 Affinity/anti-affinity constraints 86
6.4.2.2.1 Description 86
6.4.2.2.2 Identified gaps and/or extensions 88
6.4.2.3 NS VL service availability features 88
6.4.2.3.1 Description 88
6.4.2.3.2 Identified gaps and/or extensions 89
6.4.3 Gap analysis and extensions to NS runtime information 89
6.4.3.1 Current connectivity model in the NS runtime information (ETSI GS NFV-IFA 013) 89
6.4.3.2 NS VL runtime view 90
6.4.3.2.1 Description 90
6.4.3.2.2 Identified gaps and/or extensions 93
6.4.4 Gap analysis and extensions to VNF runtime information 93
6.4.4.1 Current connectivity model in the VNF runtime information (ETSI GS NFV-IFA 007) 93
6.4.4.2 VNF VL runtime view 94
6.4.4.2.1 Description 94
6.4.4.2.2 Identified gaps and/or extensions 95
6.4.5 Gap analysis and extensions to virtualised network resource runtime information 96
6.4.5.1 Current connectivity model related to virtual network and NFVI-PoP connectivity (ETSI GS NFV-IFA 005) 96
6.4.5.2 Virtual network runtime deployment view 97
6.4.5.2.1 Description 97
6.4.5.2.2 Identified gaps and/or extensions 99
6.4.5.3 NFVI-PoP and WAN connectivity views 99
6.4.5.3.1 Description 99
6.4.5.3.2 Identified gaps and/or extensions 100
7 Recommendations 100

7.1 Overview 100
7.2 General recommendations 100
7.3 Functional recommendations 101
7.4 Reference points and/or interfaces 103
7.4.1 Reference point between OSS/BSS and NFVO (Os-Ma-nfvo) 103
7.4.2 Reference point between NFVO and VNFM (Or-Vnfm) 103
7.4.3 Reference point between NFVO and VIM (Or-Vi) 104
7.4.4 Reference point between NFVO and WIM 105
7.5 Descriptors and other information/data model artefacts 105
7.6 Recommendations related to Security 107

8 Conclusion 108

Annex A: A collection of variants of multi-site NS deployment 109

A.1 Introduction 109

A.2 L2 WAN connectivity 109
A.2.1 Case 1: Extending a VLAN network across WAN 109
A.2.1.1 Overview 109
A.2.1.2 Properties of virtual network resources 110
A.2.1.3 Operational flow 111
A.2.1.4 Considerations 112
A.2.1.4.1 Distributed control and centralized control in VLAN ID assignment 112
A.2.1.4.2 Supporting L3 connectivity services 112
A.2.2 Case 2: EVPN connection with Inter-AS among NFVI-PoPs 112
A.2.2.1 Overview 112
A.2.2.2 Properties of virtual network resources 113
A.2.2.3 Operational flow 114

A.3 L3 WAN connectivity 116
A.3.1 Case 1: VXLAN connection over L3 WAN connectivity between NFVI-PoPs 116
A.3.1.1 Overview 116
A.3.1.2 Properties of virtual network resources 117
A.3.1.3 Operational flow 118

Annex B: Gap analysis between WIM and Network Controller 120

B.1 Introduction 120

B.2 Recap on Analysis of SDN across multiple VIMs 120

B.3 SDN Architecture for Transport Networks 120

B.4 Interoperability test and demonstration by ONF/ OIF in 2016 121

B.5 ETSI-NFV PoC#42 Mapping ETSI-NFV onto Multi-Vendor, Multi-Domain Transport SDN 122

B.6 Analysis 122

Annex C: Security and Regulatory Concerns 124

C.1 Risk analysis and assessment 124

Annex D: Authors & contributors 126

History 128

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document provides a report on the functional architecture necessary to provision and manage multi-site network services. To this end, a set of multi-site use cases are described, analysed and used to produce a set of recommendations for normative work.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS NFV 001: "Network Functions Virtualisation (NFV); Use Cases".

[i.2] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.3] ETSI GS NFV-EVE 005: "Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework".

[i.4] ETSI GS NFV-INF 005 (V1.1.1): "Network Functions Virtualisation (NFV); Infrastructure; Network Domain".

[i.5] ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.6] ETSI GS NFV-IFA 010: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Functional requirements specification".

[i.7] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[i.8] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.9] ETSI GS NFV-IFA 008: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[i.10] ETSI GS NFV-IFA 011: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; VNF Descriptor and Packaging Specification".

[i.11] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Os-Ma-Nfvo reference point - Interface and Information Model Specification".

[i.12] ETSI GS NFV-IFA 014: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Network Service Templates Specification".

[i.13] ETSI GR NFV-IFA 015: "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Report on NFV Information Model".

[i.14] IETF RFC 4364: "BGP/MPLS IP Virtual Private Networks (VPNs)".

[i.15] IETF RFC 4448: "Encapsulation Methods for Transport of Ethernet over MPLS Networks".

[i.16] IETF RFC 4761: "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling".

[i.17] IETF RFC 4762: "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling".

[i.18] IETF RFC 7080: "Virtual Private LAN Service (VPLS) Interoperability with Provider Backbone Bridges".

[i.19] IETF RFC 7348: "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks".

[i.20] IETF RFC 7432: "BGP MPLS-Based Ethernet VPN".

[i.21] IETF RFC 7637: "NVGRE: Network Virtualization Using Generic Routing Encapsulation".

[i.22] IETF RFC 4090: "Fast Reroute Extensions to RSVP-TE for LSP Tunnels".

[i.23] ETSI GS NFV-REL 001: "Network Functions Virtualisation (NFV); Resiliency Requirements".

[i.24] ONF TR-512: "Core Information Model".

[i.25] ONF TR-527: "Functional Requirements for Transport API".

[i.26] ONF TAPI: "Transport API (TAPI) 2.0 Overview".

[i.27] 3GPP TS 38.401: "NG-RAN; Architecture description (Release 15)".

[i.28] ETSI TS 123 401: "LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401)".

[i.29] 3GPP TS 23.501: "System Architecture for the 5G System".

[i.30] Broadband Forum TR-345: "Broadband Network Gateway and Network Function Virtualization", Issue: 1, October 2016.

[i.31] Broadband Forum TR-359: "A Framework for Virtualization", Issue: 1, October 2016.

[i.32] ONUG: "ONUG Software-Defined WAN Use Case", October, 2014.

[i.33] ONF TR-522: "SDN Architecture for Transport Networks".

[i.34] ETSI GS NFV-SEC 004 (V1.1.1): "Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications".

[i.35] ETSI GS NFV-SEC 006 (V1.1.1): "Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns".

[i.36] ETSI GS NFV-SEC 010 (V1.1.1): "Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements".

[i.37] ETSI GS NFV-SEC 012 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

[i.38] IEEE STD 802.1ad: "Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges", 2005.

[i.39] ANSI/IEEE Standard 802.1Q: "IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks", 1998.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV 003 [i.2] and the following apply:

site: A Network Point of Presence (N-PoP), as defined in ETSI GS NFV 003 [i.2].

multi-site network service: network service whose constituent Network Functions/NSs are deployed in more than one site

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.2] and the following apply:

AS	Autonomous System
ASBR	Autonomous System Border Router
BGP	Border Gateway Protocol
CE	Customer Edge
CU	Centralized Unit
DU	Distributed Unit
e-BGP	external BGP
EvCPE	Enterprise vCPE
EVPN	Ethernet VPN
GRE	Generic Routing Encapsulation
LAN	Local Area Network
LSP	Label-Switched Path
MP-BGP	Multiprotocol BGP
MPLS	Multiprotocol Label Switching
MPLS-OAM	MPLS Operations, Administration and Maintenance
NS	Network Service
NVGRE	Network Virtualisation using Generic Routing Encapsulation
NVO	Network Virtualisation Overlay
OSPF	Open Shortest Path First
PE	Provider Edge
RAN	Radio Access Network
RD	Route Distinguisher
RSVP-TE	ReSource reserVation Protocol Traffic Engineering
ToR	Top of Rack
UE	User Equipment
vAPL	virtual Appliance
vBNG	virtual Broadband Network Gateway
vCDN	virtual Content Delivery Network
vCPE	virtual Customer Premises Equipment
vCU	virtualised CU
VID	VLAN Identifier
VNI	VXLAN Network Identifier
vRAN	virtual Radio Access Network
VPN	Virtual Private Network
VPLS	Virtual Private LAN Service
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual Extensible LAN

4 Overview

4.1 Introduction

In the near future it is anticipated that there will be Network Services (NS) deployed such that connectivity among the service components, e.g. VNF, VNFC, PNF, will be necessary across wide area networks (WAN), or access networks (collectively called WANs here), both legacy and SDN-enabled. In these services, the endpoints and network functions will reside in two or more locations, which may be customer premises, N-PoPs or NFVI-PoPs.

The method by which these services are to be supported is left largely undefined in the release 1 and 2 NFV ISG documents. Documents from release 1 provide only high-level descriptions for how WAN connectivity might be supported. Clause 5.4.3 of [i.5] introduces the concept of the WIM, "a specialized VIM is a WAN Infrastructure Manager (WIM), typically used to establish connectivity between PNF endpoints in different NFVI-PoPs". Clause 5.6 of [i.5] references a figure, 5.2, which is included below as Figure 4.1-1. It shows a "hybrid network environment example illustrating the goal of NFV to have fully programmatic open interfaces for service and Resource Orchestration within and across NFVI-PoPs". Clause 5.6 further describes establishing end-2-end connectivity across virtualised networks in the PoPs and the WAN, under the control of the VIMs and the PoP VIMs and WAN WIMs.

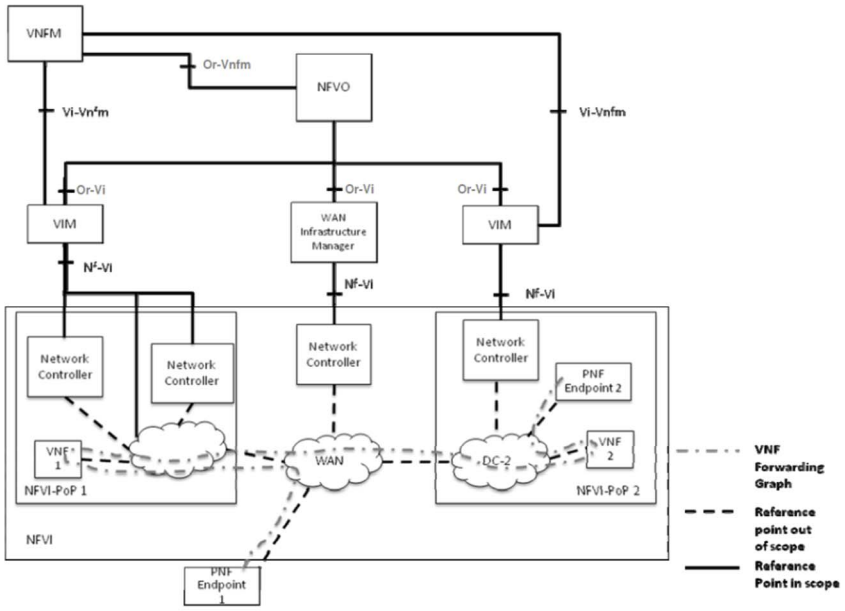

Figure 4.1-1: Release 1 Concept of WIM Role for Services over WAN (from [i.5])

This intent of the present document is to:

1) examine and analyse, through use cases, the issues surrounding support for network services distributed among multiple sites and across multiple networks and domains; and

2) based on use cases and analysis, define a set of recommendations regarding how best to support these services.

This is a deep analysis, so that that there is a clear understanding of how, where and when network service descriptions, and specifically the links between NF (and VNFC), are translated to the underlying infrastructure to establish connectivity. The scope of the recommendations includes clarifying the role of the WIM and how it integrates and communicates with MANO functional blocks, as well as possible updates to existing MANO functional block roles and reference points.

5 Use Cases

5.1 Introduction

The purpose of the use cases introduced in the present document is twofold: first, to examine and analyse the issues and capabilities related to supporting network services distributed among multiple sites; and second, to analyse how the connectivity between NF (and VNFC) can be mapped to the underlying infrastructure. The use cases cover different aspects of multi-site connectivity management, including fulfilment and assurance aspects.

The list of use cases introduced is as follows:

- Related to fulfilment processes:
  - Use Case 1: Network Service for E2E Enterprise vCPE.
  - Use Case 2: Network Service for E2E Enterprise vCPE across two WANs.
  - Use Case 3: NS Expansion to other NFVI-PoPs over WAN.
  - Use Case 4: Network Service Virtual Link aggregation.
  - Use Case 5: checking multi-site connectivity.
  - Use Case 8: multi-site VNF deployment.
  - Use Case 9: Addressing multi-site deployment requirements in NSDs.
  - Use Case 12: Network Service for vRAN.
  - Use Case 13: Use of WAN connectivity by compute-only NFVI-PoP deployments.
- Related to assurance processes:
  - Use Case 6: multi-site Virtual Link redundancy.
  - Use Case 7: multi-site Virtual Link healing.
  - Use Case 10: UE (user equipment) Location Triggered Network Service Migration Across NFVI-PoPs.
  - Use Case 11: Modification to the WAN Connectivity Resource of a Multi-site NS.

For each one of the use cases the following items are provided: an introduction, use case description (actors, triggers, pre-conditions, post-conditions, operation flows), other considerations, and analysis.

5.2 Use Case 1: Network Service for E2E Enterprise virtual Customer Premises Equipment (vCPE)

5.2.1 Introduction

This use case is discussed in the context of the Enterprise vCPE (EvCPE) network service orchestration. As shown in Figure 5.2.1-1, the overall model focuses on two NFVI-PoPs located at two different sites connected over a shared WAN infrastructure (e.g. IP/ Multiprotocol Label Switching (MPLS), optical network, etc.).

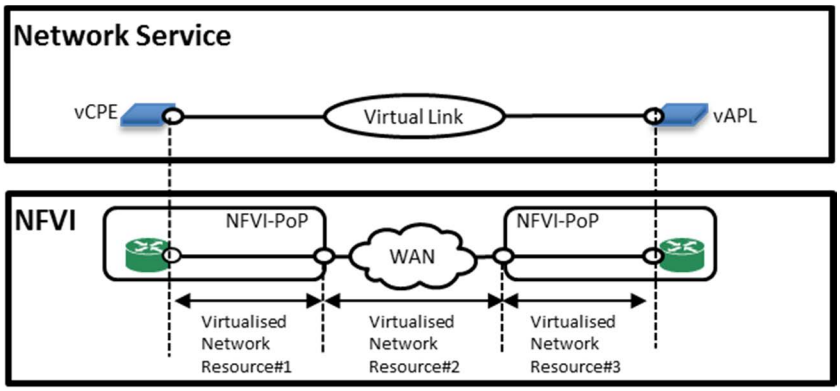

Figure 5.2.1-1: Connectivity overview for enabling Network Service

A network service (NS) consisting of two VNFs is instantiated as shown in Figure 5.2.1-1. Each VNF comes from one of two groups of VNFs, namely vCPE and Virtual Appliance (vAPL). Each group is installed in a different site, and the VNFs of the NS are connected across the WAN infrastructure.

NOTE: vCPE, or virtual CPE, represents a set of VNFs providing the functionality of an enterprise CPE. vAPL represents a set of virtualised appliances of any type that may be combined with the previous ones form a meaningful NS.

The virtualised network resources for Site#1, for WAN, and for Site#2 are referred to as virtualised network resource#1, #2 and #3, respectively. The virtualised network resources assigned to the vCPE and vAPL VNFs are terminated at virtual network ports which are attached to the WAN infrastructure. As a result, a unified Virtual Link is created by combining the virtualised network resource#1, #2 and #3.

Base operational flows for deploying NSs across the two sites are examined. VNFs are deployed in each of two sites, Site#1 and Site#2 and network connectivity is configured between those sites. The VNF deployments at each site and the network connectivity between the two sites should be coordinated in such a way as to deliver a unified service. The VNFs at each site will be connected across the WAN. The connectivity of VNFs over the WAN can be performed:

a) through gateways at each site that translate/map between the in-site and WAN virtual networks; or

b) as an overlay network using tunnelling protocols (see clause 5.2.4.2.1 in ETSI GS NFV-EVE 005 [i.3]). Examples of tunnelling protocols typically used in data centres include VXLAN and Network Virtualisation using Generic Routing Encapsulation (NVGRE). Tunnelling protocols offer the ability to stack/aggregate different customer private networks across a provider network.

Two base operational flows, namely BF#1.1 and BF#1.2, corresponds to connectivity approach a), and one base operational flow, namely BF#1.3 corresponds to connectivity approach b). These are described below.

Figure 5.2.1-2 provides a more detailed view of the use case. The architectural model is derived from Figure 5.2 in [i.5]. It shows a multi-site model managed by a single Service Provider. The figure also shows the related architectural components (e.g. WIM, Network Controller, NFVO, etc.) and reference points, which are further referred in the present use case.

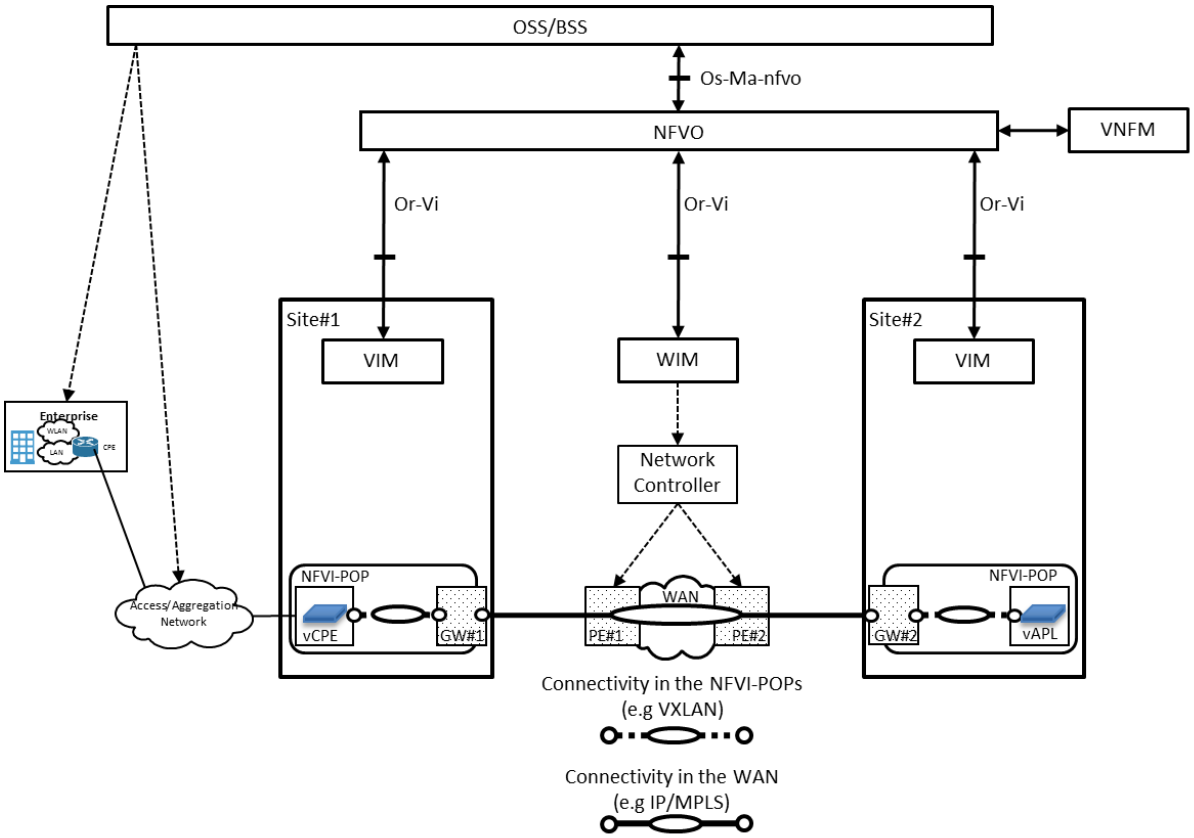

Figure 5.2.1-2: High-level view of the EvCPE service across WAN

5.2.2 Trigger

Table 5.2.2-1 describes the use case trigger.

Table 5.2.2-1: Network Service for E2E Enterprise vCPE trigger base flow #1

Trigger	Description
BF#1.1, BF#1.2 and BF#1.3	The OSS requests the NFVO to instantiate a NS with a VNF in Site#1 and another in Site#2, with these VNFs connected by a virtual link.

5.2.3 Actors and roles

Table 5.2.3-1 describes the use case actors and roles.

Table 5.2.3-1: Network Service for E2E Enterprise vCPE actors and roles

#	Actor	Description
1	OSS/BSS	
2	NFVO	
3	VIM	
4	Network Controller	
5	WIM	

5.2.4 Pre-conditions

Table 5.2.4-1 describes the pre-conditions.

Table 5.2.4-1: Network Service for E2E Enterprise vCPE Pre-conditions

#	Pre-condition	Description
1	The network between the enterprise site and Site#1 shown in Figure 5.2.1-2 works properly according to the SLA.	
2	The infrastructure of the NFVI-PoP at Site#1 and Site#2 and the network infrastructure of the WAN are also physically connected.	

5.2.5 Post-conditions

Table 5.2.5-1 describes the post-conditions for base flow #1 (i.e. BF#1.1, BF#1.2 and BF#1.3).

Table 5.2.5-1: Network Service for Enterprise vCPE post-conditions for base flow #1

#	Post-condition	Description
1	An EvCPE service is installed with VNF is two sites. The vCPE is in one site and the vAPL is in another site. The virtual link between the VNF is supported across a WAN.	

5.2.6 Operational Flows

Table 5.2.6-1 and Table 5.2.6-2 describe the base flow #1.1 (BF#1.1) and the base flow #1.2 (BF#1.2), respectively for the approach of translating/mapping in between in-site and WAN virtual networks (see clause 5.2.1).

The BF#1.1 shows the approach of translating/ mapping between in-site and in-WAN virtual networks based on information provided by WIMs. The BF#1.2 shows the approach of translating/mapping between in-site and in-WAN virtual networks based on information provided by VIMs.

Table 5.2.6-1: Network Service for E2E Enterprise vCPE base flow #1.1

#	Flow	Description
1	OSS/BSS -> NFVO	Requests to instantiate a NS across Site#1 and Site#2. Optionally OSS/BSS can specify the site where its constituent VNFs should be allocated as local constraints. *Interface - Os-Ma-nfvo*
2	NFVO	Starts an instantiation process for the vCPE and vAPL VNFs with the VNFM(s). The NFVO checks the capability (e.g. MPLS and QoS support) and capacity which are provided by the NFVI-PoP at site#1, the NFVI-PoP at site#2 and the WAN. Then the NFVO decides the location where to instantiate the vCPE and vAPL VNFs and decides to setup network connectivity between two sites across the WAN through gateways at each site translating/mapping in between in-site and WAN virtual networks.
3	NFVO ->WIM	Requests to allocate virtualised resource#2 between NFVI-PoPs at Site#1 and at Site#2 with a designated bandwidth. *Interface - Or-Vi*
4	WIM -> Network Controller	Requests to create network connectivity between PE#1 and PE#2 with the designated bandwidth between Site#1 and Site#2. *Interface - e.g. NBI for Network controllers*
5	Network Controller	Creates the network connectivity between PE#1 and PE#2 with the designated bandwidth. The IP/MPLS path configurations are, for example, installed into gateways, PE#1, PE#2 and other provider routers in the WAN infrastructure. There are multiple options where the end points for the VNFs are installed, as discussed in ETSI GS NFV-INF 005 [i.4] (e.g. vSwitch, NIC, Top of Rack (ToR), vRouter, etc.).
6	Network Controller -> WIM	Returns the response to the network creation request. In this context, the information for connecting to the WAN (e.g. IP address, VXLAN ID, and MPLS-VPN Route Distinguisher (RD) are returned.
7	WIM -> NFVO	Returns the response to the virtualised resource allocation request between NFVI-PoPs at Site#1 and at Site#2. In this context, the resource identifier, which is used for identifying the virtualised resource at the WIM, and information for connecting to the WAN (e.g. IP address and VXLAN ID, and MPLS-VPN RD) are returned. *Interface - Or-Vi*
8	NFVO -> VIM at Site#1	Requests to allocate the virtualised resource#1 connecting to the WAN. The NFVO sends information for connecting to the network connectivity over the WAN which are obtained in step 7. See note. *Interface - Or-Vi*
9	VIM at Site#1	Allocates the virtualised resource for connecting to the WAN at Site#1. See note.
10	VIM at Site#1 -> NFVO	Returns the response for allocating the virtualised resource for connecting to the WAN. The VIM returns resource identifier which is used for identifying virtualised resource at the VIM. See note. *Interface - Or-Vi*
11	NFVO -> VIM at Site#2	Requests to allocate the virtualised resource#3 connecting to the WAN. The NFVO sends information for connecting to the network connectivity over the WAN which are obtained in step 7. See note. *Interface - Or-Vi*
12	VIM at Site#2	Allocates the virtualised resource connecting to WAN. See note.
13	VIM at Site#2 -> NFVO	Returns the response to the request for allocating the virtualised resource for connecting to the WAN. The VIM returns resource identifier which is used for identifying virtualised resource at the VIM. See note. *Interface - Or-Vi*
14	NFVO	Completes the instantiation process for the vCPE and vAPL with the VNFM(s).
15	NFVO -> OSS/BSS	Returns the results of NS instantiation request.
NOTE: The set of steps 8, 9 and 10 and set of steps 11, 12, 13 can be executed sequentially or in parallel. That is, the procedure to establish connectivity at Site#1 can be executed in parallel to the procedure to establish connectivity at Site#2.		

Table 5.2.6-2: Network Service for E2E Enterprise vCPE base flow #1.2

#	Flow	Description
1	OSS/BSS -> NFVO	Requests to instantiate a NS across Site#1 and Site#2. Optionally OSS/BSS can specify the site where its constituent VNFs should be allocated as local constraints. *Interface - Os-Ma-Nfvo*
2	NFVO	Starts an instantiation process for the vCPE and vAPL VNFs with the VNFM(s). The NFVO checks the capability (e.g. MPLS and QoS support) and capacity which are provided by the NFVI-PoP at site#1, the NFVI-PoP at site#2 and the WAN. Then the NFVO decides the location where to instantiate the vCPE and vAPL VNFs and decides to setup network connectivity between two sites across the WAN through gateways at each site translating/mapping in between in-site and WAN virtual networks.
3	NFVO ->WIM	Requests to allocate virtualised network resource#2 between NFVI-PoPs at Site#1 and at Site#2 with a designated bandwidth. *Interface - Or-Vi*
4	WIM -> Network Controller	Requests to create network connectivity between PE#1 and PE#2 with the designated bandwidth between Site#1 and Site#2. *Interface - e.g. NBI for Network controllers*
5	Network Controller	Creates the network connectivity between PE#1 and PE#2 with the designated bandwidth. The IP/MPLS path configurations are, for example, installed into gateways, PE#1, PE#2 and other provider routers in the WAN infrastructure.
6	Network Controller -> WIM	Returns the response to the network creation request. In this context, the information for connecting to the WAN (e.g. IP address) are returned.
7	WIM -> NFVO	Returns the response to the virtualised resource allocation request between NFVI-PoPs at Site#1 and at Site#2. In this context, the resource identifier, which is used for identifying the virtualised network resource at the WIM and the information for connecting to the WAN are returned. *Interface - Or-Vi*
8	NFVO -> VIM at Site#1	Requests to allocate the virtualised resource#1 at Site#1. See note 1. *Interface - Or-Vi*
9	VIM at Site#1	Allocates the virtualised resource#1. See note 1.
10	VIM at Site#1 -> NFVO	Returns the response for allocating the virtualised resource for connecting to the WAN. The VIM returns resource identifier which is used for identifying virtualised resource#1 and the information for connecting to the NFVI-PoP at Site#1 (e.g. IP address, VXLAN ID, and MPLS-VPN RD). See note 1. *Interface - Or-Vi*
11	NFVO -> VIM at Site#2	Requests to allocate the virtualised resource#3 at Site#2. See note 1. *Interface - Or-Vi*
12	VIM at Site#2	Allocates the virtualised resource#3. See note 1.
13	VIM at Site#2 -> NFVO	Returns the response for allocating the virtualised resource for connecting to the WAN. The VIM returns resource identifier which is used for identifying virtualised resource#3 and the information for connecting to the NFVI-PoP at Site#2 (e.g. IP address, VXLAN ID, and MPLS-VPN RD). See note 1. *Interface - Or-Vi*
14	NFVO ->WIM	Requests to update the virtualised network resource#2 at the WAN. The NFVO sends the information for connecting to the endpoints of the site#1 and site#2 for the interconnection between the two sites which is obtained in step 10 and 13. See note 2. *Interface - Or-Vi*
15	WIM -> Network Controller	Request to configure the provider edge (PE) node#1 and PE node#2 at WAN. See note 2. *Interface - e.g. NBI for Network controllers*
16	Network Controller	Configures the PE node#1 and PE node#2 at WAN. See note 2.
17	Network Controller -> WIM	Returns the response for configuring the PE node#1 and PE node#2 at WAN. See note 2.
18	WIM -> NFVO	Returns the response for updating the virtualised network resource#2. See note 2.

#	Flow	Description
19	NFVO -> VIM at Site#1	Requests to update the virtualised network resource#1 connecting to the WAN. The NFVO sends the information for connecting to the endpoint of the site#2 for the interconnection between the two sites which is obtained in step 13. See note 2. *Interface - Or-Vi*
20	VIM at Site#1	Configures the virtualised network resource#1. See note 2.
21	VIM at Site#1 -> NFVO	Returns the response for updating the virtualised network resource#1. See note 2. *Interface - Or-Vi*
22	NFVO -> VIM at Site#2	Requests to update the virtualised network resource#3 connecting to the WAN. The NFVO sends the information for connecting to the endpoint of the site#1 for the interconnection between the two sites which is obtained in step 10. See note 2. *Interface - Or-Vi*
23	VIM at Site#2	Configures the virtualised network resource#3. See note 2.
24	VIM at Site#2 -> NFVO	Returns the response for updating the virtualised network resource#3. See note 2. *Interface - Or-Vi*
25	NFVO	Completes the instantiation process for the vCPE and vAPL with the VNFM(s).
26	NFVO -> OSS/BSS	Returns the results of NS instantiation request.
NOTE 1: The set of steps 8, 9 and 10 and set of steps 11, 12, 13 can be executed sequentially or in parallel. That is, the procedure to establish connectivity at Site#1 can be executed in parallel to the procedure to establish connectivity at Site#2. NOTE 2: The set of steps from 14 to 18, set of steps from 19 to 21 and set of steps from 22 to 24 can be executed sequentially or in parallel. That is, the procedures to configure the virtualised network resource#1, virtualised network resource#2 and the virtualised network resource#3 can be executed in parallel.		

Table 5.2.6-3 describes the base flow #1.3 (BF#1.3) for the approach of tunnelling in-site virtual networks in WAN virtual networks (see clause 5.2.1). The flow includes all necessary steps on setting up the connectivity assuming the case that only physical connectivity has been established (see pre-condition #2 in Table 5.2.4-1).

Table 5.2.6-3: Network Service for E2E Enterprise vCPE base flow #1.3

#	Flow	Description
1	OSS/BSS -> NFVO	Requests to instantiate a NS across Site#1 and Site#2. Optionally OSS/BSS can specify the site where its constituent VNFs should be allocated as local constraints. *Interface - Os-Ma-nfvo*
2	NFVO	Starts an instantiation process for the vCPE and vAPL VNFs with the VNFM(s). The NFVO checks the capability (e.g. MPLS and QoS support) and capacity which are provided by the NFVI-PoP at site#1, the NFVI-PoP at site#2 and the WAN. Then the NFVO decides the location where to instantiate the vCPE and vAPL VNFs and decides to establish an interconnection between the two sites as an overlay network using tunnelling protocols. In this case, the NFVO coordinates the resources commonly used between the two sites (e.g. VXLAN Network Identifier for VXLAN, Tenant Network ID for NVGRE, VLAN ID in the C-Tag of IEEE 802.1ad [i.38], etc.). This coordination process can involve interaction with VIMs on the two sites to check the availability of the common resources, get information about them, and reserve them. *Interface - Or-Vi*
3	NFVO ->WIM	Requests to allocate virtualised resource#2 between NFVI-PoPs at Site#1 and at Site#2 with a designated bandwidth. *Interface - Or-Vi*
4	WIM -> Network Controller	Requests to create network connectivity between PE#1 and PE#2 with the designated bandwidth between Site#1 and Site#2. *Interface - e.g. NBI for Network controllers*
5	Network Controller	Creates the network connectivity between PE#1 and PE#2 with the designated bandwidth. The IP/MPLS path configurations are, for example, installed into gateways, PE#1, PE#2 and other provider routers in the WAN infrastructure. There are multiple options where the end points for the VNFs are installed, as discussed in ETSI GS NFV-INF 005 [i.4] (e.g. vSwitch, NIC, ToR, vRouter, etc.).

#	Flow	Description
6	Network Controller -> WIM	Returns the response to the network creation request. In this context, the information for connecting to the WAN (e.g. IP address, VLAN ID in the S-Tag of IEEE 802.1ad [i.38], and MPLS-VPN RD) are returned.
7	WIM -> NFVO	Returns the response to the virtualised resource allocation request between NFVI-PoPs at Site#1 and at Site#2. In this context, the resource identifier, which is used for identifying the virtualised resource at the WIM, and information for connecting to the WAN (e.g. IP address, VLAN ID in the S-Tag of IEEE 802.1ad [i.38], and MPLS-VPN RD) are returned. *Interface - Or-Vi*
8	NFVO -> VIM at Site#1	Requests to allocate the virtualised resource#1 for the interconnection between the two sites. The NFVO sends information on the common resources for the interconnection between the two sites which are obtained in step 2. The NFVO also sends information for connecting to the network connectivity over the WAN which are obtained in step 7. See note 1. *Interface - Or-Vi*
9	VIM at Site#1	Allocates the virtualised resource#1 based on the information provided in step 8. See note 1.
10	VIM at Site#1 -> NFVO	Returns the response to the request for allocating the virtualised resource#1 for the interconnection between the two sites. The VIM returns the information for connecting to the endpoint at the Site#1 (e.g. the address of Virtual Extensible LAN (VXLAN) Tunnel End Point (VTEP) for VXLAN or the router supporting NVGRE). See note 1. *Interface - Or-Vi*
11	NFVO -> VIM at Site#2	Requests to allocate the virtualised resource#3 for the interconnection between the two sites. The NFVO sends information on the common resources for the interconnection between the two sites which are obtained in step 2. The NFVO also sends information for connecting to the network connectivity over the WAN which are obtained in step 7. See note 1. *Interface - Or-Vi*
12	VIM at Site#2	Allocates the virtualised resource#3 based on the information provided in step 11. See note 1.
13	VIM at Site#2 -> NFVO	Returns the response to the request for allocating the virtualised resource#3 for the interconnection between the two sites. The VIM returns the information for connecting to the endpoint at the Site#2 (e.g. the address of VTEP for VXLAN or the router supporting NVGRE) is returned. See note 1. *Interface - Or-Vi*
14	NFVO -> VIM at Site#1	NFVO requests to configure the virtualised resource#1 connecting to the WAN. The NFVO sends the information for connecting to the endpoint of the site#2 for the interconnection between the two sites which is obtained in step 13. See note 2. *Interface - Or-Vi*
15	VIM at Site#1	Configures the virtualised resource#1. See note 2.
16	VIM at Site#1 -> NFVO	Returns the response to the request for configuring the virtualised resource#1. See note 2. *Interface - Or-Vi*
17	NFVO -> VIM at Site#2	NFVO requests to configure the virtualised resource#3 connecting to the WAN. The NFVO sends the information for connecting to the endpoint of the site#1 for the interconnection between the two sites which is obtained in step 10. See note 2. *Interface - Or-Vi*
18	VIM at Site#2	Configures the virtualised resource#3. See note 2.
19	VIM at Site#2 -> NFVO	Returns the response to the request for configuring the virtualised resource#3. See note 2. *Interface - Or-Vi*
20	NFVO	Completes the instantiation process for the vCPE and vAPL with the VNFM(s).
21	NFVO -> OSS/BSS	Returns the results of NS instantiation request.

NOTE 1: The set of steps 8, 9 and 10 and set of steps 11, 12, 13 can be executed sequentially or in parallel. That is, the procedure to establish connectivity at Site#1 can be executed in parallel to the procedure to establish connectivity at Site#2.

NOTE 2: The set of steps 14, 15 and 16 and set of steps 17, 18, 19 can be executed sequentially or in parallel. That is, the procedure to configure the virtualised resource at Site#1 can be executed in parallel to the procedure to configure the virtualised resource at Site#2.

5.2.7 Other Considerations

5.2.7.1 Network Service Instance Description

According to the NFV release 2 IFA specifications, there are two ways to control the placement of the VNFs, namely "affinity or anti-affinity group" and "location constraints". The affinity or anti-affinity group describes the affinity or anti-affinity relationship applicable between the VNF instances in the NSD [i.12]. The NFVO needs to select appropriate locations for the VNFs to meet the affinity or anti-affinity group. In addition, the NFVO has to take into account of requirements for the Virtual Links, e. g. latency, bandwidth, availability, when selecting the locations. The location constraints describe the site where the VNF is instantiated as part of the NS instantiation [i.11]. This clause focuses on using the affinity or anti-affinity group to place the VNFs to different sites. Moreover, the way to utilize the "location constraints" for VNF placement to different sites will be described in more details in clause 5.2.7.4.

Figure 5.2.7.1-1 shows parameters of the NSD related to this use case. In Figure 5.2.7.1-1, an affinity or anti-affinity group is defined and applied to the VNF Profiles for vCPE and vAPL. Since the "affinityOrAntiAffinity" and the "scope" attribute of the affinity or anti-affinity group are set to "anti-affinity" and "NFVI-POP", respectively (see rows in red in Table "AffinityOrAntiAffinityGroup"), the NFVO allocates the vCPE and vAPL in different NFVI-PoPs. The NSD also specifies requirements of the Virtual Link which connects vCPE and vAPL (see rows in green in Table "VirtualLinkDf", "connectivityType", and "VirtualLinkProfile"). Therefore, the NFVO finds connectivity between those two NFVI-PoPs which satisfies the requirements.

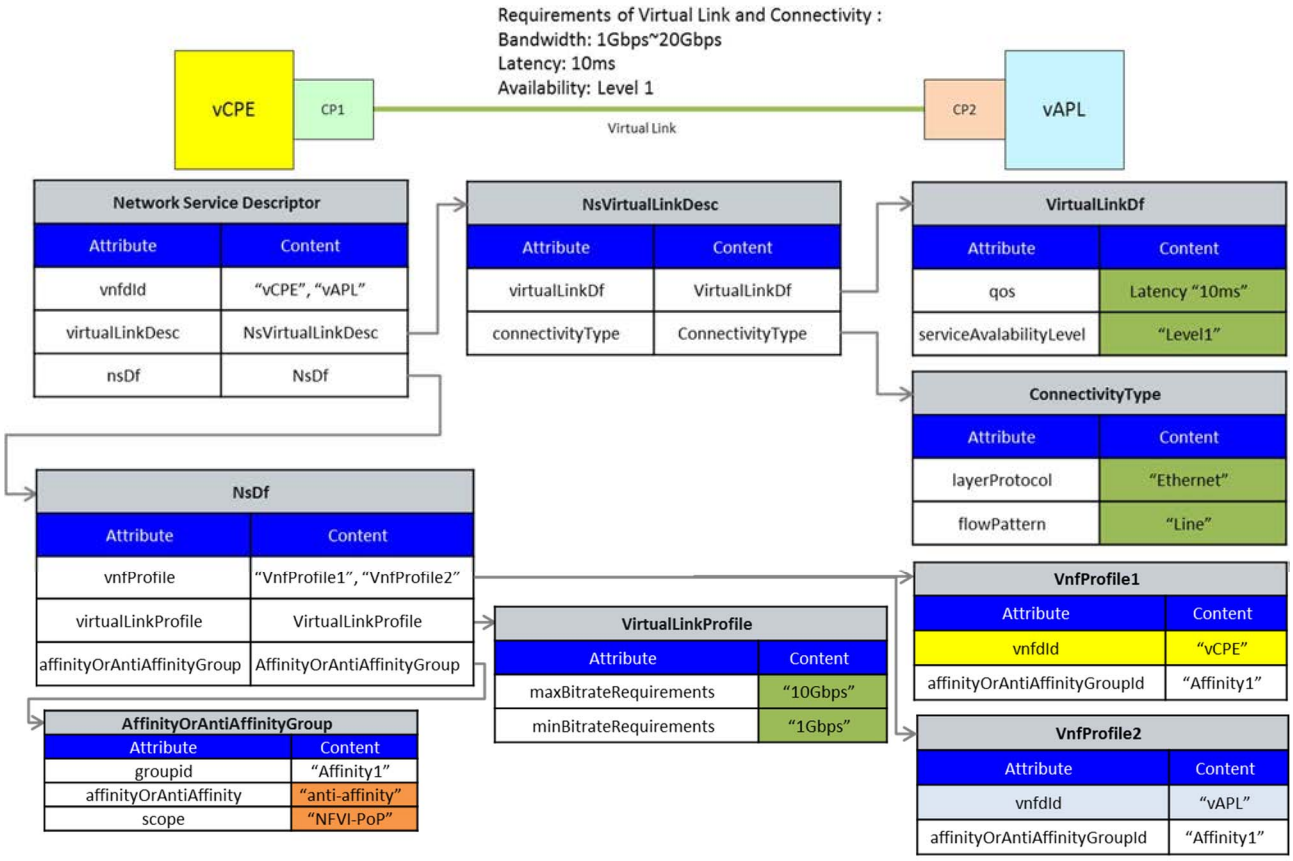

Figure 5.2.7.1-1: Parameters of NSD related to an E2E EvCPE service across WAN

5.2.7.2 Infrastructure Description

As an example Figure 5.2.7.2-1 shows the underlying networks for the case of the MPLS related to this use case. However, the other network architecture does not preclude for this use case.

For the branch site connection case shown in Figure 5.2.7.2-1 a), the Customer Edge (CE) router is equivalent to GW#1 and GW#2 depicted in Figure 5.2.1-2. The Site#1 and Site#2 are connected to the IP-VPN as a customer site. The Virtual Private Network (VPN) routing information of the NFVI-POP are exchanged between the CE and PE routers, and also propagated to other customer sites. For the Inter Autonomous System (AS) connection case shown in Figure 5.2.7.2-1 b), the PE router is equivalent to GW#1 and GW#2 depicted in Figure 5.2.1-2. The Site#1 and Site#2 are identified by the AS number and are administrated by independent AS. These PE routers, which are configured as Autonomous System Border Router (ASBR), exchange the VPN routing information with each other as they are connected to other sites.

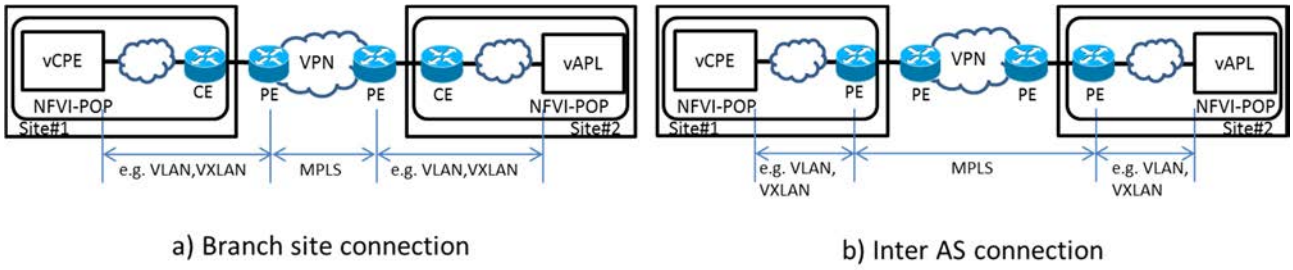

Figure 5.2.7.2-1: Underlying network for the case of MPLS related to an E2E EvCPE service across WAN

5.2.7.3 Mapping of Service Instance Model to Supporting Infrastructure

Figure 5.2.7.3-1 shows the mapping of the service instance model to the infrastructure related to this use case. For the case of BF#1.1 and BF#1.2, the Virtual Link is directly mapped to the underlying network. On the other hand, for the case of BF#1.3, an overlay network is created over the underlying network and the Virtual Links are mapped onto the overlay network. For the case of BF#1.3, the WAN connectivity can be shared with other Virtual Links.

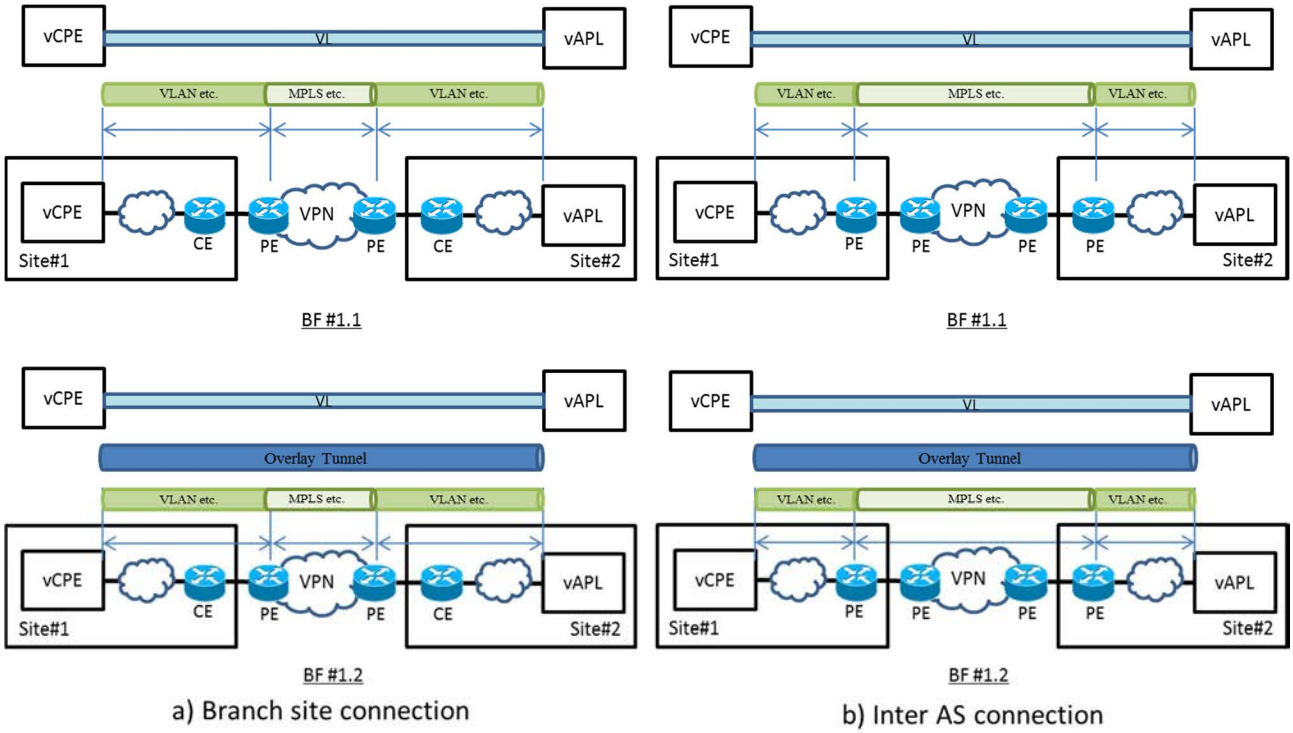

Figure 5.2.7.3-1: Mapping of service instance Model to infrastructure related to an E2E EvCPE service across WAN

5.2.7.4 Management Architecture and Activities

This clause represents a collection of management flows related to a sequence of a NS Instantiation. The diagram shown in Figure 5.2.7.4-1 provides a sequence diagram for instantiating a connectivity service between two sites. All the flows in this clause are informative, representing the base flow #1.1 in the description of the use case 1.

Figure 5.2.7.4-2 shows a mapping of service instance Model to infrastructure related to an E2E EvCPE service across WAN. Some attributes to be discussed are introduced.

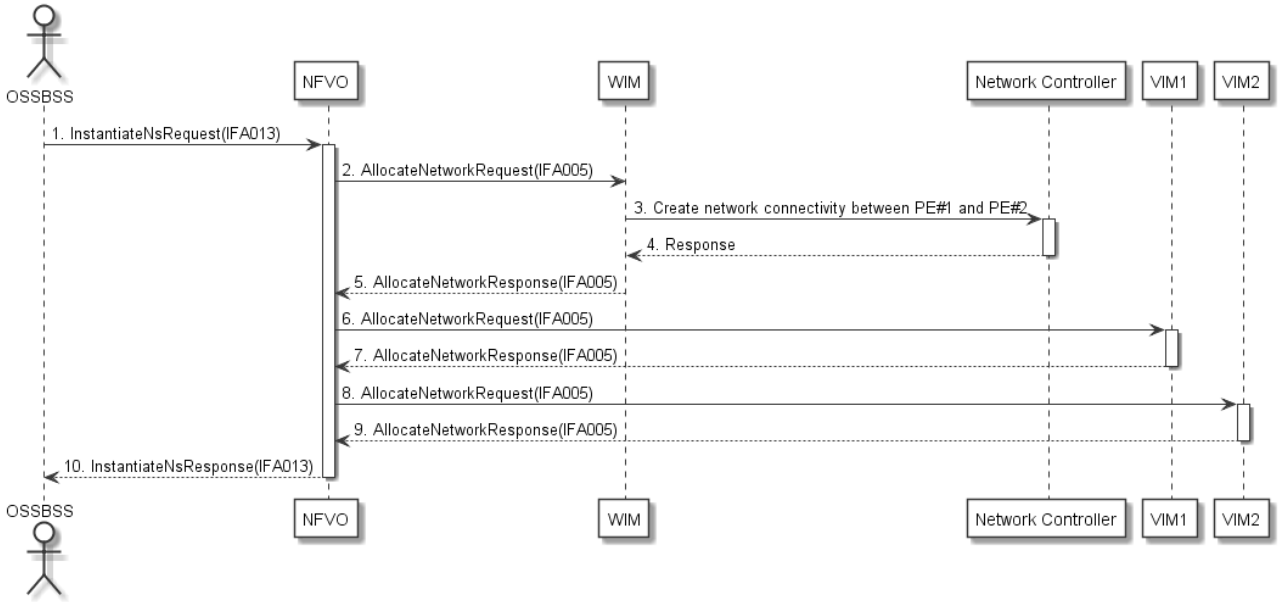

Figure 5.2.7.4-1: Instantiate a connectivity service

In step 1, two parameters, nsInstanceId and locationConstraints are given through Os-Ma-nfvo reference point. The nsInstanceId [i.10] is an identifier of an instance of the NS that has been created. The locationConstraints [i.10] shows the location for the vCPE and vAPL to be instantiated. Site#1 and Site#2, for examples, can be used for the parameter. Affinity group or anti-affinity can also be used for this purpose but, for simplicity, the locationConstraints option is taken in this discussion.

In the context of the use case, step 2 is written with the assumption that Or-Vi reference point [i.7] could be applied for this interaction. More options, if needed, should be discussed in the latter overall use case and requirement analysis. In this assumption for step 2, AllocateNetworkRequest, which shows Site#1 and Site#2 needs to be connected, is passed to the WIM. The networkResourceName and typeNetworkData for the virtualisedResource #2 are also given to the WIM. The networkResourceName [i.7] shows a name of the virtualised network resource. "Virtualised resource #2" is, for example, used for this parameter. The typeNetworkData [i.7] includes a piece of network information about the particular virtual network resource to be instantiated. The content, named as VirtualNetworkData, has bandwidth, networkType ("local", "vlan", "vxlan", "gre", "l3-vpn", "mpls", etc.), segmentType, networkQoS and metadata.

In step 3, the WIM, referring to the typeNetworkData, facilitates the establishment of the network connectivity between the Site#1 and Site#2, e.g. by asking the Network Controller.

Network QoS parameters as networkQoS can be passed via Or-Vi reference point. Capacity, latency, cost, for example, can be considered as attributes. The WIM may declare an explicit path to the Network Controller to guarantee the required networkQoS. The WIM can ask the Network Controller to compute the explicit path if the WIM does not have the computation. The Network types can also be declared if the Network Controller manages multiple layered WAN infrastructures.

In step 6 and 8, the networkResourceName and typeNetworkData are also given through Or-Vi reference point. "Virtualised resource #1" and "Virtualised resource #3" are, for example, given to VIM#1 and VIM#2 respectively.

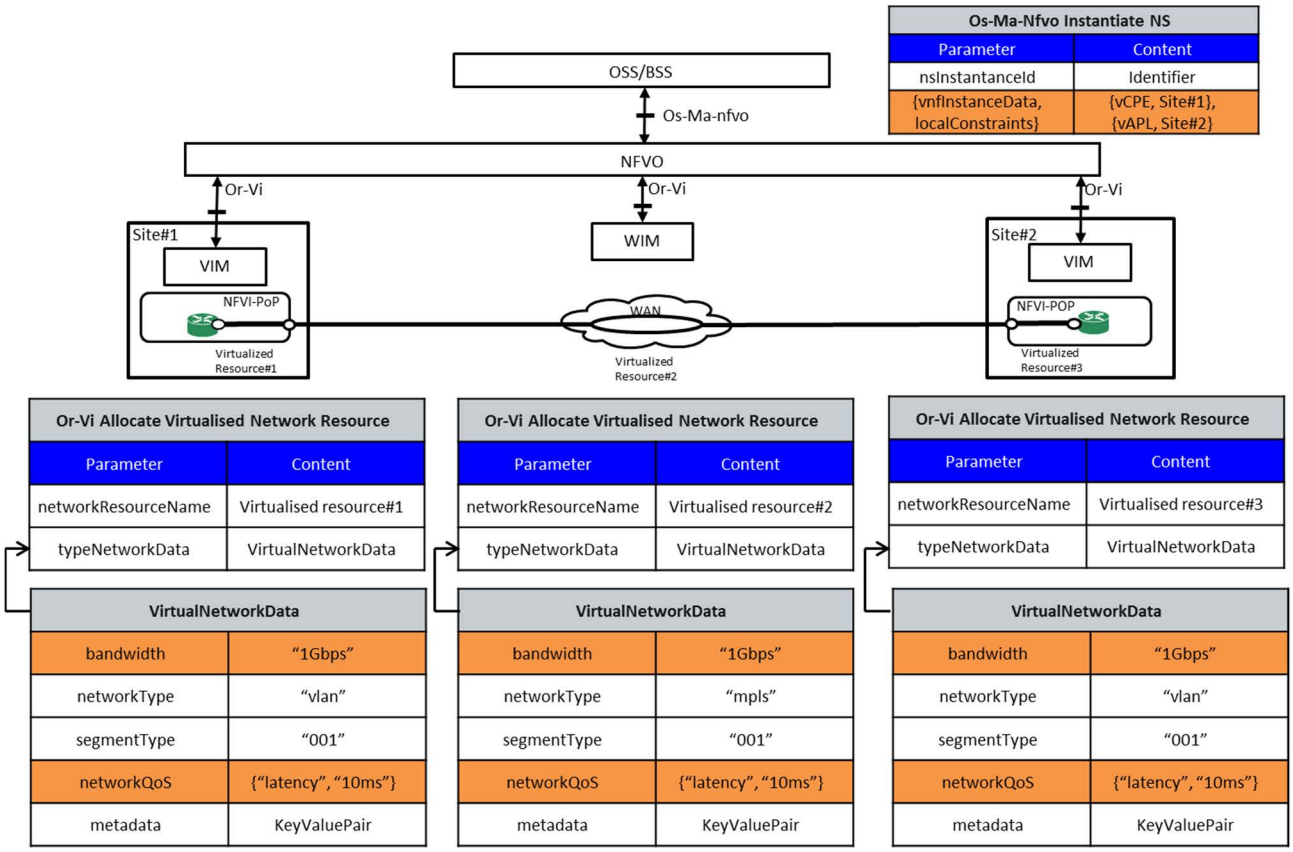

Figure 5.2.7.4-2: Mapping of service instance Model to infrastructure related to an E2E EvCPE service across WAN

5.2.8 Analysis

This clause provides further analysis of Use Case #1 in terms of the connectivity services between different NFVI-PoPs and WAN infrastructure. This analysis will be done with reference to the interfaces defined over the Or-Vi reference point, which form the northbound interface for the VIM. The analysis will highlight the relevant Information Elements and their respective attributes defined over the Or-Vi reference point [i.7] and show how they can be utilized by the WIM in order to ensure connectivity between sites (e.g. central office).

For ensuring connectivity between sites; network connectivity endpoints, virtual network ports, virtual network interfaces and virtual network resources are the essential elements. Figure 5.2.8-1 illustrates the mapping of these elements described in [i.7] in the context of Use Case #1. These elements are described below in the context of providing connectivity between VNFs over a WAN infrastructure.

In this use case, a virtual network resource is characterized by various attributes defined over the VirtualNetwork Information Element [i.7]. For example, it specifies the type of the virtual network. There are multiple options to allocate the virtual network resources (e.g. vlan, vxlan, gre, etc.), which are characterized by the networkResourceTypeId, segment information (e.g. vlan identifier, vxlan indentifier, gre key, etc.), the bandwidth, the network QoS attributes.

On the other hand, a virtual network port is another type of endpoint and characterized by the VirtualNetworkPort Information Element in [i.7]. The attributes of this information element are configured depending on the portType (e.g. L2 or L3 access ports or L1 trunk port), networkId, segmentId (e.g. vlan id, gre key), and the bandwidth (in Mbps) supported by the virtual network port. These attributes are helpful to determine the location of the attachment points to VNFs within the NFVI-PoP. The virtual network port is attached to a virtual network interface, which is a communication endpoint under a compute resource. The virtual network interface is described by the attributes of the VirtualNetworkInterface information element (e.g. networkId, networkPortId, ipAddress, etc.).

Moreover, a network connectivity endpoint is an endpoint attached to an NFVI-PoP administrated by the VIM. As represented by the example, it is considered that the endpoint can be mapped onto a Network Gateway. Such a network gateway can be addressed by an attribute, the networkConnectivityEndpoint of the NfviPop Information Element. This attribute is helpful for other NFVI-PoP or N-PoP to find the location of the network gateway instance.

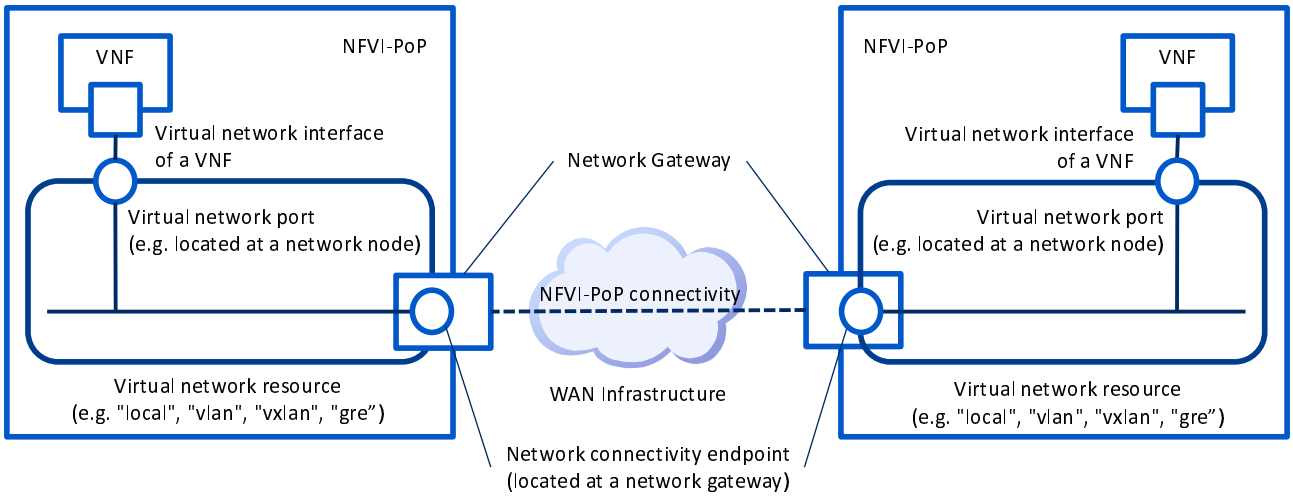

Figure 5.2.8-1: Terminology mappings from IFA 005 context to current document

From the perspective of the infrastructure level, a network gateway of the NFVI-PoP is considered as a customer edge node (CE) [i.14] which connects branch sites. The CE can be considered as an infrastructure node in the infrastructure network domain [i.4], or can also be a virtualised network node. On the other hand, PE nodes are put at the edge of the WAN infrastructure, interfacing to Ex-Nf, a reference point to an external network defined in NFV Infrastructure [i.4].

The connectivity at the WAN infrastructure level, called WAN connectivity, is established between the provider edge nodes. The connectivity may be configured in advance or on-demand. As shown in Figure 5.2.8-2, connectivity between the NFVI-PoPs, configured between the customer edge nodes, needs to be established over the WAN connectivity.

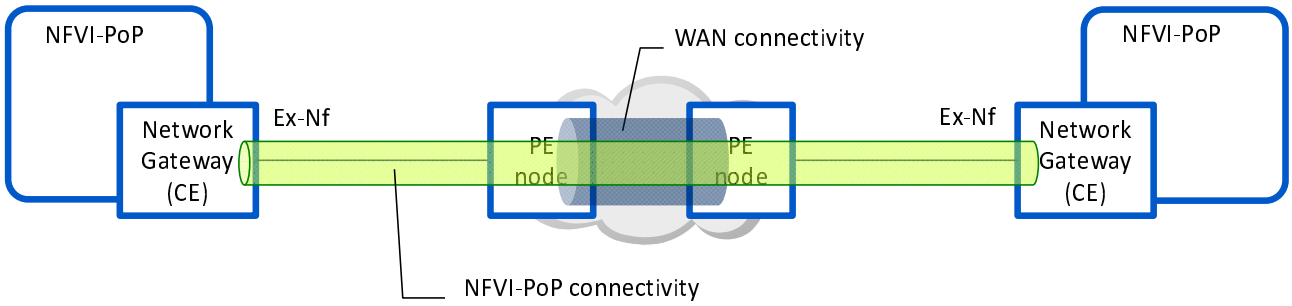

Figure 5.2.8-2: A mapping to the infrastructure

Table 5.2.8-1 shows as examples ways of configuring the WAN and NFVI-connectivity between the NFVI-PoPs. These examples should not be limiting and more examples can be added and analysed, if necessary.

Table 5.2.8-1: Examples for NFVI-PoP connectivity and WAN connectivity

NFVI-PoP connectivity service	WAN Connectivity
Virtual Private LAN Service (VPLS) (layer 2 MPLS VPN) [i.15], [i.16], [i.17]	MPLS (L2-VPN)
VPRN (layer 3 MPLS VPN) [i.14]	MPLS (IP-VPN)
H-VPLS [i.18]	MPLS
Ethernet VPN (EVPN) [i.20]	MPLS
VxLAN [i.19]	IP-Network
NVGRE [i.21]	IP-Network

After the instantiation of the NS, VNFs are connected within the same or different broadcast domain as shown in Figure 5.2.8-3 and Figure 5.2.8-4.

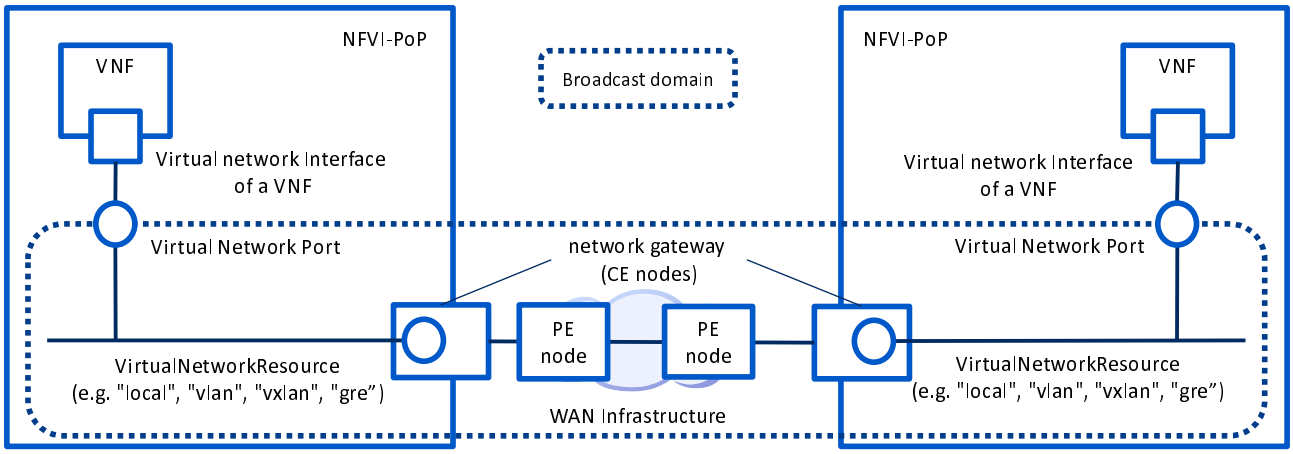

Figure 5.2.8-3: L2 connectivity between NFVI-PoPs

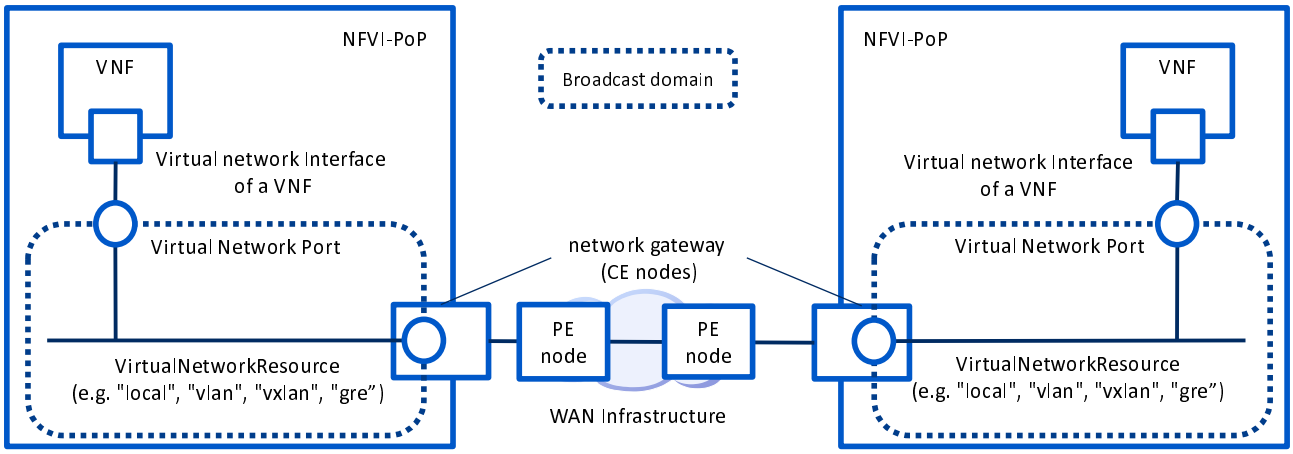

Figure 5.2.8-4: L3 connectivity between NFVI-PoPs

It should be analysed, from a view across all of the use cases, what information elements and attributes to manage the following resources are necessary:

- WAN connectivity
- NFVI-PoP connectivity (configurations for Ex-Nf)
- Configuration of the network gateways to interconnect virtual network resources and NFVI-PoP connectivity

In addition, the base flows in this use case indicate that it is necessary for a VIM/WIM to provide information necessary for connecting to a virtualised network resource the VIM/WIM manages. This information is consumed by other VIMs/WIMs when they connect their virtualised network resources to this one. The flow of information can be as follows:

- WIM to VIM (see steps 7, 8 and 11 of BF#1.1 in Table 5.2.6-1 and steps 7, 8 and 11 of BF#1.3 in Table 5.2.6-3). A VIM uses the information about allocated virtualised network resource on the WAN to configure a virtual network resource within its managed NFVI-PoP to connect to the virtual network resource on the WAN.
- VIM to WIM (see steps 10, 13 and 14 of BF#1.2 in Table 5.2.6-2). A WIM uses the information about the virtualised network resource within the NFVI-PoP connecting to the WAN to configure a virtual network resource within its managed WAN to connect to the virtual network resource within the NFVI-PoP.
- VIM to VIM (see steps 10, 13, 19 and 22 of BF#1.2 in Table 5.2.6-2 and steps 10, 13, 14 and 17 of BF#1.3 in Table 5.2.6-3). A VIM uses the information about other NFVI-PoP endpoints to configure the endpoint of an overlay or inter-AS connection within its managed NFVI-PoP to connect with the peered endpoint within another NFVI-PoP.

This information flow and its data may be technology dependent, and more specific examples are provided in Annex A. The distribution of this information is performed via NFVO as shown in the base flows. Thus, NFVO should be capable of acquiring the relevant information from the source VIM/WIM and then forward the needed information to the appropriate target VIMs/WIMs.

5.3 Use Case 2: Network Service for E2E Enterprise vCPE across two WANs

5.3.1 Introduction

An enterprise vCPE model can be seen as a use case in ETSI GS NFV 001 [i.1], which provides a view of a typical large enterprise comprising headquarters facilities with a centralized corporate IT infrastructure and multiple branches connected to one another and to the enterprise headquarter. The vCPE functions can be deployed at branch sites, service provider's site, and centralized enterprise site. Those sites are interconnected with WAN connectivity service, which traditionally supported by a single infrastructure, or by multiple different network infrastructure (cf ONUG Software-Defined WAN Use Case [i.32]). MPLS, Internet or a pair of them are shown as examples.

Derived from use case 1, this use case discusses how the NFVO maps a Virtual Linkonto an appropriate WAN infrastructure, when multiple WAN infrastructures are available. In the context two virtual links, one for management plane and the other for data plane, are required for a particular NS. For the management plane the requirement is high reliability, while the requirement for the data plane is high capacity. However, the virtual links that have the required characteristics and capacity to satisfy the NS requirements are installed and available in different WAN infrastructures. The MANO should therefore select the Virtual Links that meet best the path criteria for the NS. Therefore this ability of MANO on the selection of the appropriate Virtual Links would enable it to meet criteria such as the connectivity type (e.g. Ethernet, IP-VPN), the performance (the latency, the jitter or the bandwidth), the service availability level, etc.

The following base flow is expected, but not limited:

- BF: NS deployment with two virtual links over different WAN infrastructures:
  - There is a pair of WAN infrastructures, namely WAN#1 or WAN#2, which are connected to each site, namely Site#1 or Site#2. VNFs are deployed at the two sites in the same way as described in Use Case 1, and those are then connected with a pair of Virtual Links belonging to the two WAN infrastructures.
  - The two WAN infrastructures combined fulfil the different requirements of the two Virtual Links such as the connectivity type, the performance, and the service availability level, etc. as required by the NS. The MANO thus selects the appropriate Virtual Links, i.e. the Virtual Link#1 and the Virtual Link#2 from the WAN#1 and the WAN#2, respectively.

Figure 5.3.1-1 shows the connectivity overview for enabling end-to-end the NS across two WAN infrastructures. Two NFVI-PoPs are connected across two WAN infrastructures. Virtualised network resources of Virtual Link#1 and Virtual Link#2 are referred to virtualised network resource#1, #3 and #5 and virtual network resource#2, #4 and #6, respectively. The virtualised network resource #1 and #2, the virtualised network resource #5 and the virtualised network resource #6 are attached to vCPE, vAPL and monitoring, respectively. The virtualised network resource #1 and #5 and the virtualised network resource #2 and #6 are also attached to the virtualised network resource#3 and #4, respectively. As a result, the Virtual Link#1 is installed on the virtualised network resource#1, #3 and #5. And the Virtual Link#2 is installed on the virtualised network resource#2, #4 and #6.

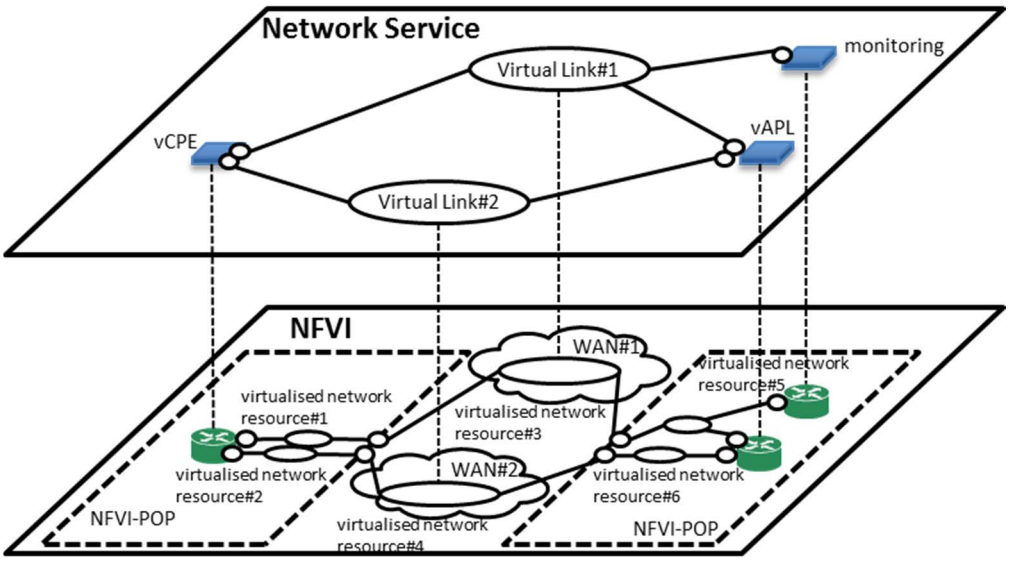

Figure 5.3.1-1: Connectivity overview for enabling End-to-End Network Service across two WANs

Figure 5.3.1-2 provides an architectural view of the use case with respect to the MANO framework. It shows a multi-site model managed by a single Service Provider. The figure also shows the related architectural components (e.g. WIM, Network Controller, NFVO, etc.) and reference points, which are referred to in the present use case. Here the architecture includes a WIM for each WAN. However, this does not preclude an alternative management architecture, where a single WIM may be responsible for both (or more) underlying WANs.

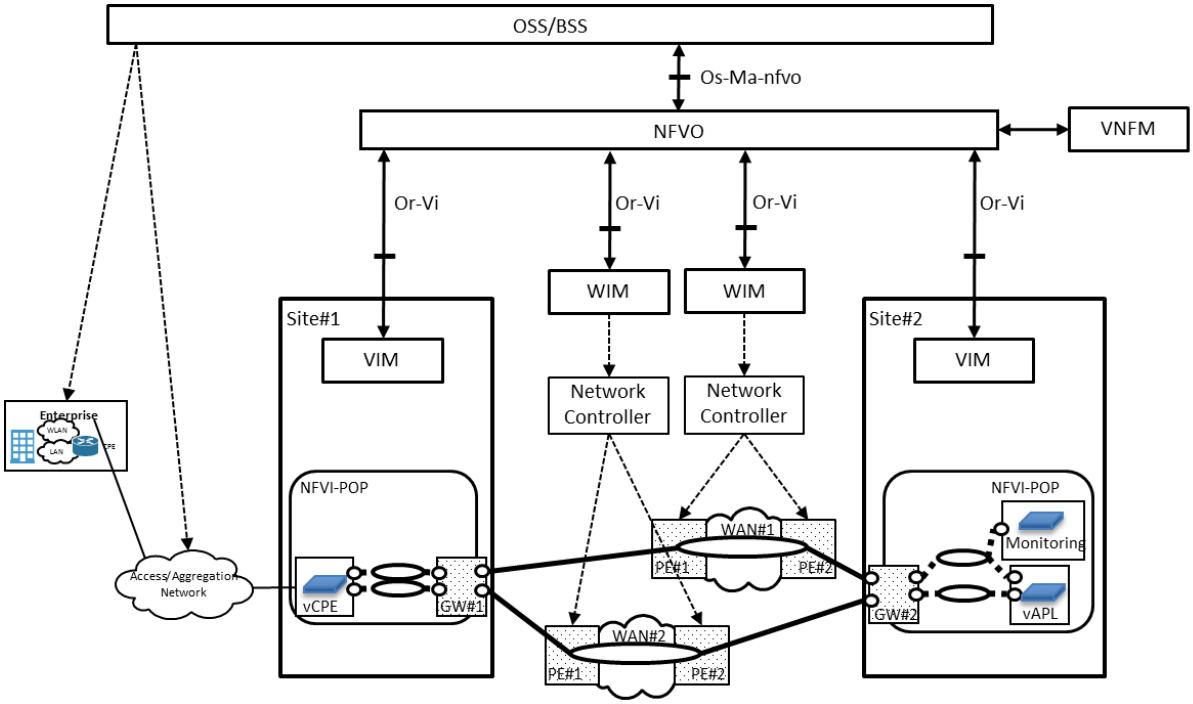

Figure 5.3.1-2: High-level use case for an E2E EvCPE service across two WANs

5.3.2 Trigger

Table 5.3.2-1 describes the use case trigger for base flow.

Table 5.3.2-1: Network Service for E2E Enterprise vCPE across two WANs trigger base flow

Trigger	Description
BF	When the NFVO is requested to instantiate VNFs in the Site#1 and Site#2 from the OSS/BSS.

5.3.3 Actors and roles

Table 5.3.3-1 describes the use case actors and roles.

Table 5.3.3-1: Network Service for E2E Enterprise vCPE across two WANs actors and roles

#	Actor
1	OSS/BSS
2	NFVO
3	VIM
4	Network Controller
5	WIM

5.3.4 Pre-conditions

Table 5.3.4-1 describes the pre-conditions for base flow.

Table 5.3.4-1: Network Service for E2E Enterprise vCPE across two WANs Pre-conditions for base flow

#	Pre-conditions	Comment
1	The network between the enterprise site and Site#1 shown in Figure 5.2.1-2 works properly according to the SLA.	
2	The infrastructure of the NFVI-PoP at Site#1 and Site#2 and that of the WAN#1, WAN#2 are also physically connected.	

5.3.5 Post-conditions

Table 5.3.5-1 describes the post-conditions for base flow.

Table 5.3.5-1: Network Service for E2E Enterprise vCPE across two WANs post-conditions for base flow

#	Post-conditions	Comment
1	E2E EvCPE service is provided across the two sites. The VNF connects two Virtual Links through different WANs.	

5.3.6 Operational Flows

Table 5.3.6-1 describes the base flow.

Table 5.3.6-1: Network Service for E2E Enterprise vCPE across two WANs base flow

#	Actor	Action/Description
1	OSS/BSS -> NFVO	Requests to instantiate a NS across Site#1 and Site#2. Designates WANs to allocate the Virtual Link#1 and #2 respectively by notifying the requirements of the Virtual Links at NSD or input parameters. *Interface - Os-Ma-nfvo*
2	NFVO	Starts an instantiation process for the vCPE and vAPL. NFVO decides allocation of the Virtual Links which meet the requirements shown in step 1 in accordance with the capability and the capacity check of the WAN infrastructure shown in step 2 in Table 5.2.6-1.
3	NFVO, WIM, Network Controller, VIM at Site#1 and VIM at Site#2	The virtualised network resources#1,#3, #5 and the virtual resource#2,#4,#6 are created according to the step 3 to step 15 of "NS for E2E Enterprise vCPE base flow#1" (Table 5.2.6-1), respectively. WIM follow from the step 3 to step 7 but works with WIMs in the WAN#1 and WAN#2.
4	NFVO	Completes the instantiation process for the vCPE and vAPL with the VNFM(s). The VNFs across two sites connect to the Virtual Link#1 and #2.
5	NFVO -> OSS/BSS	Returns the results of NS instantiation request.

5.3.7 Other Considerations (e.g. Performance)

No other considerations are derived from the present use case.

5.3.8 Analysis

The objective of this analysis is to describe the instantiation procedures expressed in step 2 of Table 5.3.6-1 and highlight the main operational steps. In order to determine the location to instantiate the VNFs and Virtual Links requested by OSS/BSS, the NFVO needs to parse the relevant NSD file to determine the location of NFVI-PoPs, and check for available network resources. In this regard the relevant attributes, parameters and contents that are required during different steps of the instantiation process are analysed below.

Network Service Descriptor (NSD) Parsing

The OSS/BSS invokes an "InstantiateNsRequest" on the NFVO to start the instantiation procedure. This request includes the parameter "flavourId", which is linked to the target NSD and refers to NS Deployment Flavour (NsDf) IE which has been on-boarded in advance. The request also includes "locationConstraints" that defines the location constraints for the target VNFs to be instantiated as a part of the target NS. In the context of use case 2, the Virtual Links are required to be deployed in the different WAN infrastructures but the constraints for the Virtual Links have not been specified in the current IFA specifications yet.

Determination of Location of NFVI-PoPs

The parameter "locationContraints" in "instantiateNsRequest" defines constraints on the basis of which NFVI-PoPs are selected for deploying the VNFs as requested by OSS/BSS. The NFVO invokes "NfviPopNetworkInformationRequest" to the VIMs in order to retrieve NfviPop information element. This information element consists of the attribute "geographicalLocationInfo", which provides the information about the geographic location (e.g. geographic coordinates or address of the building, etc.) of the NFVI resources that the VIM manages. Another attribute of "networkConnectivityEndpoint" provides the information about network connectivity endpoints. However, the content of "networkConnectivityEndpoint" attribute has not been specified yet in the specification of the Or-Vi reference point [i.7]. It is expected that the "networkConnectivityEndpoint" attribute provides information about the network interface that connects the NFVI-PoP to the WAN infrastructure, and this information is shared with the WIM.

Network Resource Identification between NFVI-PoP

The "NsVirtualLinkDesc" IE in the NS Deployment Flavour (NsDf) IE includes "connectivityType" and "virtualLinkDf" attributes.

The "connectivityType" attribute has the contents of "layerProtocol" and "flowPattern". The "layerProtocol" identifies the protocol that the VL supports (Ethernet, MPLS, ODU2, IPV4, IPV6, Pseudo-Wire, etc.) while "flowPattern" identifies the flow pattern of the connectivity (Line, Tree, Mesh, etc.). With those contents, the NFVO can determine the type of network connectivity that should be instantiated.

The "virtualLinkDf" attribute has the contents of "qos". The "qos" content has "latency", "packetDelayVariation", "packetLossRatio", and "priority" values. With these values of the "qos" content, NFVO selects WAN infrastructure which satisfies the QoS requirements. A situation may arise where the QoS requirements of Virtual Link#1 and Virtual Link#2 are satisfied by WAN#1 and WAN#2 respectively. As discussed above, a new constraint for virtual link is necessary to deploy Virtual Link#1 and Virtual Link#2 in different WAN infrastructures.

Querying for Network Status

The invocation of the "QueryNetworkCapacityRequest" message by the NFVO can be used to retrieve information elements from VIM at Site#1, VIM at Site#2, WIM#1 and WIM#2. The message has a parameter "resourceCriteria", which declares the characteristics of the virtual network for which the operator may want to know the available, total, reserved and/or allocated capacity. The information provided by this parameter can thus be used to retrieve available path, resource, etc., in the VIM at Site#1, VIM at Site#2, WIM#1 and WIM#2.

In use case 2, NFVO should decide how to allocate the virtualised network resources for Virtual Links in different WAN infrastructures. By comparing attributes and contents in the target NSD and the current status of the virtualised network resources managed by VIM at Site#1, VIM at Site#2, WIM#1 and WIM#2, and by checking if the deployment model is defined in the NSD or not, the NFVO requests for resource allocations to the VIMs and the WIMs. In the operational procedure, the operational policies may contain rules that follow criteria for certain aspects. A non-exhaustive list of criteria is listed below:

- Constraints aspects:
  - The NFVO may consider constraints on location of the VNFs and Virtual Links declared by OSS/BSS.
  - The constraints for the Virtual Links should be declared as such whether they can be deployed in the same or different WAN infrastructures.
- WAN capacity aspects:
  - During the selection process of WAN infrastructure, the NFVO generates "resourceCriteria" parameter, which declares capacity computation parameter for selecting the characteristics of the virtual network.
  - Explicit route declaration can be indicated which WAN infrastructure should be used.
  - WIM should have the capability to compute available network resources.
  - Network Controller should have the capability to compute available capacity if WIM does not have the capability.
- WAN connectivity aspects:
  - During the selection process of WAN infrastructure, the NFVO may require information on the type of connectivity servicesupported by the WIMs.
  - The connectivity information of the NFVO should support different types of layer protocols so that "connectivityType" attribute can be specified with multiple options such as Ethernet, MPLS, ODU2, IPV4, IPV6, Pseudo-Wire, etc.
  - In a situation where there is no WAN connectivity between NFVI-PoPs, NFVO needs to request WIM for allocation of a new WAN connectivity.
  - WIM should be able to configure the WAN connectivity.

- NFVI-PoP Connectivity aspects:
  - In a situation where there is no NFVI-PoP connectivity between NFVI-PoPs, NFVO needs to request WIMs and VIMs for allocation of a new NFVI-PoP connectivity.
  - NFVO should be able to collect network interface information connecting to the WAN infrastructure.

5.4 Use Case 3: NS Expansion to other NFVI-PoPs over WAN

5.4.1 Introduction

Derived from the use case 1, this use case discusses how the NFVO expands the NS to the other NFVI-PoPs over WAN for the purpose of scaling the NS. Flexible NS scaling can help save CAPEX and OPEX when traffic rapidly changes because of expected event, e.g. a scheduled event requiring additional service capacity, or unexpected event (e.g. natural disaster) requiring capacity expansion.

For example, it is assumed that two NFVI-PoPs that are located in different sites are connected over the WAN infrastructure, and the NFV-MANO deploys an NS within one of the sites (the first site). When workloads of the NS cross its capacity threshold and there are not enough available resources to scale the NS within the first site, the NS scaling is resolved by expanding the NS to use resources from a second site. In such a case, the NFV-MANO manages the needed NS Virtual Links and requests new network connectivity between the two sites to expand the NS over the two sites. As a result, the workloads can be distributed between the two sites.

The following base flow is expected, but not limited:

- BF: NS expansion to other NFVI-PoPs over the WAN:
  - There are two sites, namely Site#1 and Site#2, which are physically connected over the WAN. An NS which consists of two VNFs, i.e. vCPE and vAPL#1, and a Virtual Link which connects them is deployed in Sites#1. When a trigger event such as the overload of the vAPL#1 is detected, the NFVO adds a new instance of the vAPL called vAPL#2 in Site#2, and updates the Virtual Link to connect the vAPL#2 across the WAN.

Figure 5.4.1-1 shows a connectivity overview after performing the NS expansion to other NFVI-PoPs over the WAN. By performing the NS expansion, two NFVI-PoPs are connected across a WAN infrastructure. The virtualised resource for the WAN is referred as virtualised network resource#3. A virtualised network resource#2 is created to provide network connectivity within the NFVI-PoP of Site#2. The virtualised network resource#1 in the NFVI-PoP of Site#1, which connects the vCPE and the vAPL#1, is extended to connect the WAN. As a result, the Virtual Link is extended covering the virtual network resource#1, #2 and #3.

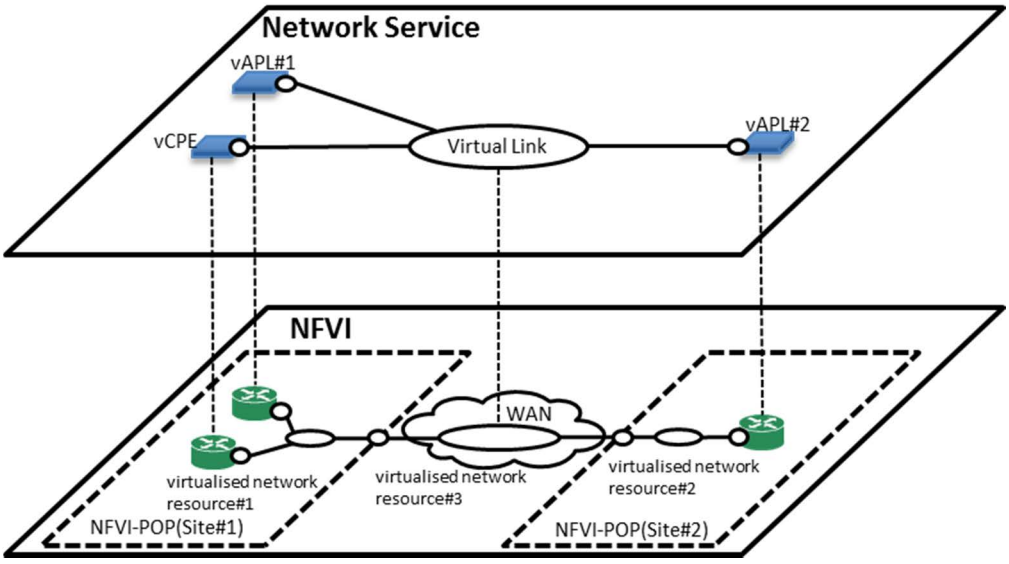

Figure 5.4.1-1: Connectivity overview for enabling NS expansion over WAN

Figure 5.4.1-2 provides an architectural view of the use case. It shows a multi-site model managed by a single Service Provider. The figure also shows the related architectural components (e.g. WIM, Network Controller, NFVO, etc.) and reference points, which are further referred to in the present use case.

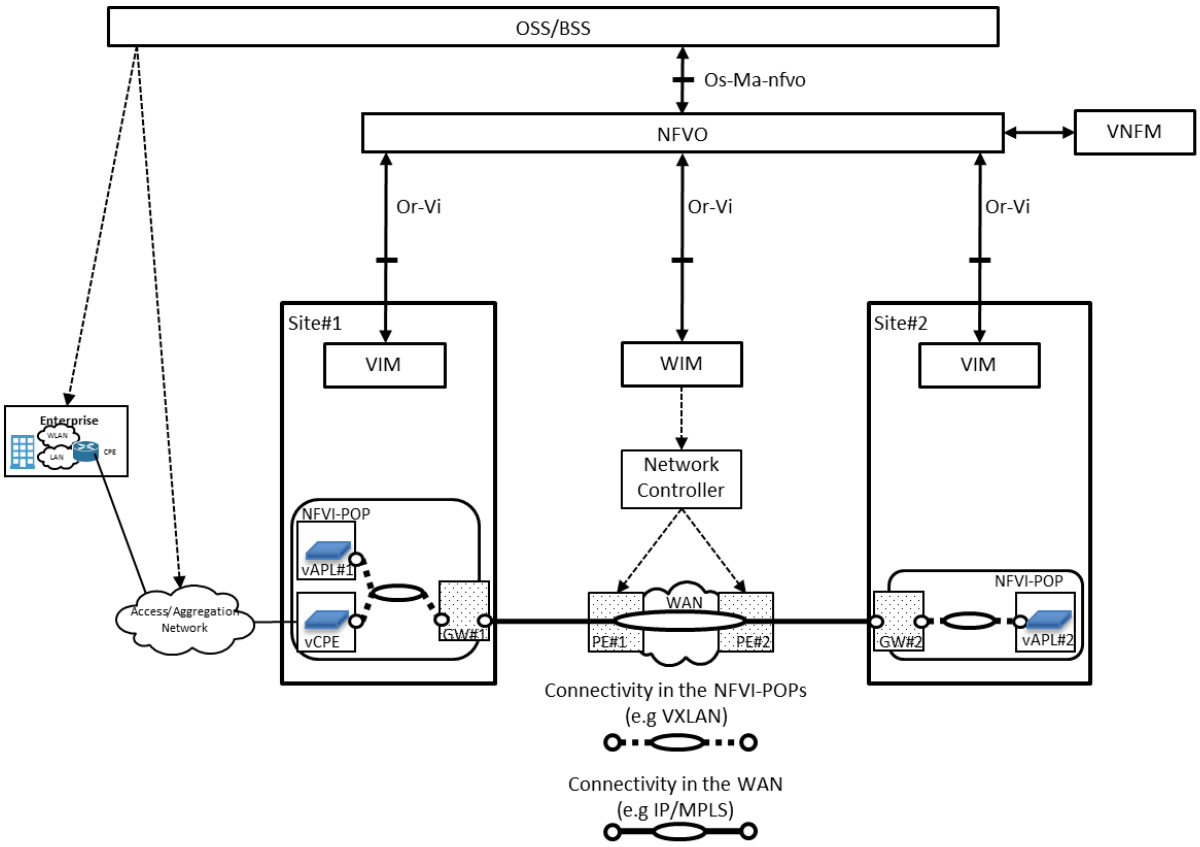

Figure 5.4.1-2: High-level use case for an NS expansion over WAN

5.4.2 Trigger

Table 5.4.2-1 describes the use case trigger for base flow.

Table 5.4.2-1: NS expansion to other NFVI-PoPs over WAN trigger base flow

Trigger	Description
BF	When the NFVO is requested by the OSS/BSS to scale NS to add vAPL#2 due to the OSS/BSS getting a trigger event such as an overload of the vAPL#1.

5.4.3 Actors and roles

Table 5.4.3-1 describes the use case actors and roles.

Table 5.4.3-1: NS expansion to other NFVI-PoPs over WAN actors and roles

#	Actor
1	OSS/BSS
2	NFVO
3	VIM
4	Network Controller
5	WIM

5.4.4 Pre-conditions

Table 5.4.4-1 describes the pre-conditions for base flow.

Table 5.4.4-1: NS expansion to other NFVI-PoPs over WAN Pre-conditions for base flow

#	Pre-conditions	Comment
1	The E2E EvCPE service is provided by the vCPE and the vAPL#1 in Site#1.	The NFVO provides the virtual resource at Site#1 for the E2E EvCPE service by default.

5.4.5 Post-conditions

Table 5.4.5-1 describes the post-conditions for base flow.

Table 5.4.5-1: NS expansion to other NFVI-PoPs over WAN post-conditions for base flow

#	Post-conditions	Comment
1	The E2E EvCPE service is updated across the two sites. The VNFs in the two sites are connected over the Virtual Link through WAN infrastructure.	

5.4.6 Operational Flows

Table 5.4.6-1 describes the base flow.

Table 5.4.6-1: NS expansion to other NFVI-PoPs over WAN base flow

#	Actor	Action/Description
1	OSS/BSS -> NFVO	The OSS/BSS requests to scale the NS to add the vAPL#2. *Interface - Os-Ma-nfvo*
2	NFVO	The NFVO checks the capability whether the Site#1 has enough resources for the vAPL#2. If there are not enough resources at Site#1, the NFVO then checks the capacity of Site#2 for instantiating vAPL#2. If vAPL#2 has the capacity then the NFVO will check the connectivity related capability of WAN between the NFVI-PoP at Site#1, and the NFVI-PoP at Site#2. The NFVO then decides to allocate vAPL#2 to Site#2 and setup a virtualised network resource#3 for network connection between two sites across the WAN. Then the NFVO starts an instantiation process for the vAPL#2 with the VNFM.
3	NFVO, WIM, Network Controller	The virtualised network resources#3 for network connectivity across WAN is created according to step 3 to step 7 of "NS for E2E Enterprise vCPE base flow#1.1" (Table 5.2.6-1).
4	NFVO, VIM at Site#2	The virtualised network resources#2 for connecting to the WAN is created according to the step 11 to step 13 of "NS for E2E Enterprise vCPE base flow#1.1" (Table 5.2.6-1). See note.
5	NFVO -> VIM at Site#1	The NFVO requests to update the virtualised resource#1 for connecting to the WAN. The NFVO sends information for connecting to the network connectivity over the WAN which is obtained in step 3. See note. *Interface - Or-Vi*
6	VIM at Site#1	The VIM at Site#1 updates the virtualised resource#1 for connecting to the WAN. See note.
7	VIM at Site#1 -> NFVO	The VIM as Site#1 returns the response to the request for updating the virtualised resource#1. See note. *Interface - Or-Vi*
8	NFVO	The NFVO completes the instantiation process for the vAPL#2 with the VNFM.
9	NFVO -> OSS/BSS	The NFVO returns the results of the NS scaling request.
NOTE: The step 4 and set of steps 5, 6 and 7 can be executed sequentially or in parallel. That is, the procedure to update connectivity at Site#1 can be executed in parallel to the procedure to create connectivity at Site#2.		

5.4.7 Other Considerations (e.g. Performance)

No other considerations are derived from the present use case.

5.4.8 Analysis

For the expansion of an NS to other NFVI-PoPs over WAN, the NFV-MANO should be able to:

1) Update the connectivity of the NS already deployed within a site to expand the existing NS VL across the WAN.

As the use case depicts, initially, the only available NS Virtual Link was deployed within the boundary of a specific Site (NFVI-PoP), whereas after the expansion, the existing NS Virtual Link expands across the WAN. As introduced in steps 5, 6 and 7 of the operational flow in Table 5.4.6-1, the VIM should support updating the virtualised network for connecting to the WAN.

Requirement Nfvo.NsU.004 of ETSI GS NFV-IFA 010 [i.6] specifies the capability for the NFVO to support updating the existing VL(s)/VNFFG(s) involved in an existing NS. In addition, requirement Nfvo.NsRmpbNfvo.001 of the same referred deliverable [i.6] specifies the support of the capability of the NFVO to issue requests to the VIM in order to allocate, identify, update and release resources needed for the connectivity of NSs. The requirements do not detail within what boundaries/scope such an update of virtualised network resources can be performed, i.e. whether or not such an update concerns only to virtualised network resources within an NFVI-PoP.

The Virtualised Network Resource Management interface produced by the VIM on the Or-Vi reference point towards the NFVO specifies the UpdateNetwork operation (refer to clause 7.4.1.4 of ETSI GS NFV-IFA 005 [i.7]). The operation offers the capability to update different types of virtualised network resources, such as: network, subnet and network ports. The NfviPop information element (refer to clause 8.10.3 of [i.7]) also provides information about the network connectivity endpoints to the NFVI-PoP, which helps building the topology information relative to NFVI-PoP connectivity to other NFVI-PoP. Both, the UpdateNetwork operation as well as the NfviPoP information element are relevant to the present use case. As part of the expansion across the WAN, the existing virtualised network resource(s) within the NFVI-PoP needs to be updated to enable connectivity to the WAN through the appropriate network connectivity endpoint of the NFVI-PoP. Although it is not explicitly detailed in the use case flow, the update to enable connectivity to the WAN might require allocation of new specific virtual network resources such as network ports and network segments. However, neither the UpdateNetwork operation, nor the information elements available in the ETSI GS NFV-IFA 005 [i.7] specify the means on how to realize such a connectivity expansion.

5.5 Use case 4: Network Service Virtual Link aggregation

5.5.1 Introduction

This use case expands on the use case in clause 5.2. It is described on the same assumption that there are two NFVI-PoPs located at two different sites connected over a shared WAN infrastructure (e.g. IP/MPLS, optical network, etc.) as shown in Figure 5.2.1-2.

To improve the usage of WAN connectivity resource, Virtual Links can be aggregated and share common WAN connectivity. That is, when creating a new Virtual Link to interconnect new or existing VNF instances, it is possible to assign the new Virtual Link to an existing virtualised network resource in the WAN used for other existing Virtual Links. This can be achieved as long as:

- the virtualised network resource meets the requirements of the Virtual Link and has enough capacity to accommodate it; and
- the traffic corresponding to the different VLs can be made distinguishable at the each site's edge.

Overlay network and tunnelling protocols typically used in data centres (e.g. VXLAN and NVGRE) are relevant to the present use case. These protocols allow end-to-end consumer private networks to be transported over a single provider network.

Figure 5.5.1-1 shows a connectivity overview of the aggregation of Virtual Links in the WAN. The NS in Figure 5.2.1-1 of use case #1 in clause 5.2 is updated by adding the vCPE2, vAPL2, and a new Virtual Link#2 that connects the vCPE2 and vAPL2. The vCPE2 and vAPL2 are placed in Site#1 and Site#2 respectively. Virtualised resource#4 and virtualised resource#5 are newly allocated on Site#1 and Site#2 respectively and assigned to the new Virtual Link. To aggregate the two Virtual Links into the WAN, virtualised resource#2 at the WAN for the existing Virtual Link#1 is reused for the new Virtual Link#2. As a result, the Virtual Link#2 between vCPE2 and vAPL2 is created by combining the virtualised resource#4, #2 and #5.

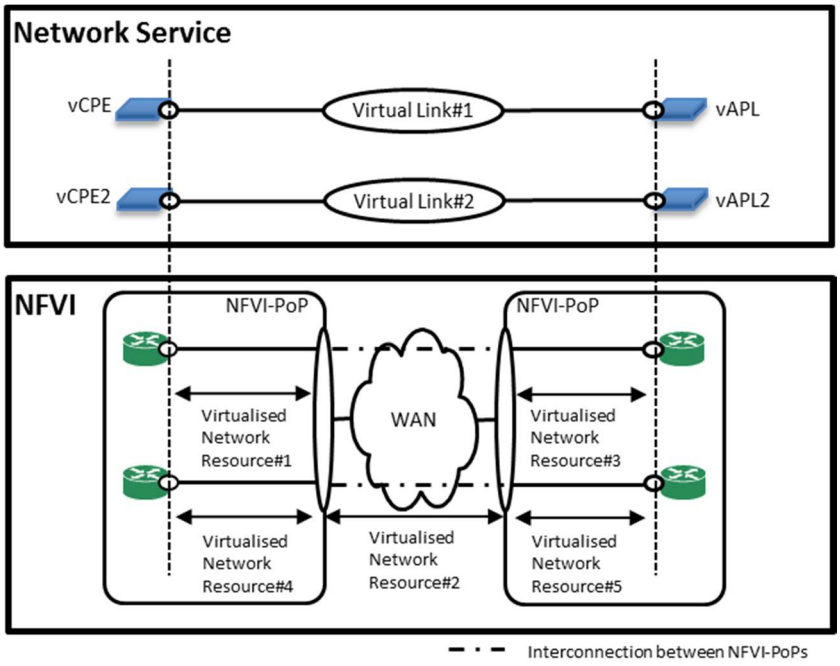

Figure 5.5.1-1: Connectivity overview for aggregating Virtual Links in the WAN enabling End-to-End Network Service

5.5.2 Trigger

Table 5.5.2-1 describes the use case trigger.

Table 5.5.2-1: Network Service Virtual Link aggregation trigger

Trigger	Description
OSS/BSS -> NFVO	When the NFVO is requested to update the NS instance to instantiate and add a new Virtual Link to interconnect new VNFs in the Site#1 and Site#2.

5.5.3 Actors and roles

Table 5.5.3-1 describes the use case actors and roles.

Table 5.5.3-1: Network Service Virtual Link aggregation actors and roles

#	Actor	Description
1	OSS/BSS	
2	NFVO	
3	VIM	

5.5.4 Pre-conditions

Table 5.5.4-1 describes the pre-conditions.

Table 5.5.4-1: Network Service Virtual Link aggregation pre-conditions

#	Pre-condition	Description
1	An E2E EvCPE service is instantiated and works properly according to the SLA.	
2	Virtual Link in the E2E EvCPE service is established over an overlay network between NFVI-PoPs at Site#1 and Site#2.	

5.5.5 Post-conditions

Table 5.5.5-1 describes the post-conditions.

Table 5.5.5-1: Network Service Virtual Link aggregation post-conditions

#	Post-condition	Description
1	The new Virtual Link between newly added VNFs shares the virtualised network resource at the WAN with other existing Virtual Links.	E2E EvCPE service is instantiated and works properly according to the SLA.

5.5.6 Operational Flows

Table 5.5.6-1 describes the operational flow.

Table 5.5.6-1: Network Service Virtual Link aggregation operational flow

#	Flow	Description
1	OSS/BSS -> NFVO	Requests to update the NS across Site#1 and Site#2 to instantiate and add vCPE2 and vAPL2 which require a new Virtual Link. Optionally OSS/BSS can specify the site where its constituent VNFs should be allocated as local constraints. *Interface - Os-Ma-nfvo*
2	NFVO	Starts an instantiation process for the vCPE2 and vAPL2 VNFs with the VNFM(s). The NFVO determines the location where to instantiate the vCPE2 and vAPL2 VNFs taking into account the local constraints, if any.
3	NFVO	NFVO checks existing virtual network resources at the WAN, and selects a virtual network resource at the WAN which can meet the requirements of the new Virtual Link in between vCPE2 and vAPL2 based on the NSD of the NS, its policy, etc. Then, NFVO coordinates the resources commonly used between the two sites (e.g. VXLAN Network Identifier for VXLAN, Tenant Network ID for NVGRE, etc.). This coordination process can involve interaction with VIMs on the two sites to check the availability of the common resources and reserve them. *Interface - Or-Vi*
4	NFVO	NFVO reuses and assigns the selected WAN virtualised network resource for the new Virtual Link to connect the vCPE2 and vAPL2.
5	NFVO -> VIM	Requests allocation of virtualised resouce#4 and virtualised resource#5 to site#1 and site#2 respectively for connecting to the WAN. Then NFVO establishes the connectivity within and between sites for the new Virtual Link. This process follows step 8 to step 18 of Table 5.2.6-2. *Interface - Or-Vi*
6	NFVO	Completes the instantiation process for the vCPE2 and vAPL2 with the VNFM(s).
7	NFVO -> OSS/BSS	Returns the results of NS update request.

5.5.7 Other Considerations (e.g. Performance)

No other considerations are derived from the present use case.

5.5.8 Analysis

- Step 3 of the operational flow in Table 5.5.6-1 shows that the NFVO selects an existing virtualised network resource allocated by the WIM to be used for aggregation of a newly instantiated Virtual Link. This selection would affect not only the resource usage of WAN(s) but also quality of service and availability of the NSs. This is because it could be assumed that the WIM controls QoS of traffic in the WAN on a per virtualised network resource basis. In that case, Virtual Links which have different requirements in QoS should not share the same virtualised network resource at WAN (see also Use Case 2 in clause 5.3). Similarly, to provide redundancy of the network connectivity for the NS, it is useful to allocate Virtual Links to different virtualised network resources at WAN(s) (see also Use Case 6 in clause 5.7). Therefore, NFVO should support flexible control over Virtual Link aggregation (i.e. aggregate the newly instantiated Virtual Link with the existing virtual network resources in the WAN) based on operational policies. Some examples of the information to be considered to build the policies are given below:Tenant-based aggregation decision of Virtual Links into virtualised WAN network resources:

  - Under this policy consideration, the NFVO selects an existing virtualised WAN network resource which has been assigned to a Virtual Link that belongs (has been assigned) to the same tenant.

- Network Service-based or VNF-based aggregation decision of Virtual Links into virtualised WAN network resources:

  - Under this policy consideration, the NFVO selects an existing virtualised WAN network resources that has already been assigned to the same NS(s) and/or VNF(s) or group of NS(s) and/or VNF(s).

- Aggregation decision of Virtual Links into virtualised WAN network resources based on Connectivity Type:

  - Under this policy consideration, the NFVO selects an existing virtualised WAN network resources that has been assigned to other Virtual Links that has (have) the same connectivity type requirements (e.g. layer protocol as "Ethernet" and flow pattern as "Line") as the newly instantiated Virtual Link(s).

NOTE 1: Connectivity Type requirements of a Virtual Link are specified as the connectivityType attribute of the NsVirtualLinkDesc information element in NSD (see clause 6.5.2 in ETSI GS NFV-IFA 014 [i.12]).

- Aggregation decision of Virtual Links into virtualised WAN network resources based on QoS-class of the Virtual Link:

  - Under this policy consideration, the NFVO selects existing virtualised WAN network resources that has been assigned to other Virtual Links that has (have) the same QoS class as the newly instantiated Virtual Link(s).

NOTE 2: QoS parameters of a Virtual Link are specified as the QoS attribute of the VirtualLinkDf information element in the NSD (see clause 6.5.4 in ETSI GS NFV-IFA 014 [i.12]).

- Aggregation decision of Virtual Links into virtualised WAN network resources based on throughput requirements:

  - Under this policy consideration, the NFVO selects the existing virtualised WAN network resources only if it has enough capacity available to accommodate the throughput requirements of the newly Virtual Link.

NOTE 3: Throughput requirements of a Virtual Link are specified as the maxBitrateRequirements and minBitrateRequirements attributes of the VirtualLinkProfile information element in the NSD (see clause 6.3.4 in ETSI GS NFV-IFA 014 [i.12]).

- Aggregation decision of Virtual Links into virtualised WAN network resources based on Affinity and anti-affinity rules specified in the NSD:

  - Operators may set a specific affinity and anti-affinity rule to the corresponding VLD(s) in the NSD. Under this policy consideration, the NFVO selects an existing virtualised WAN network resource that meets the affinity and anti-affinity rules of the newly instantiated Virtual Link(s). The scope of affinity and anti-affinity rule needs to cover relationships such as "WAN", or "virtualised network resource at WAN".

NOTE 4: Affinity and anti-affinity rule of a Virtual Link are specified as the localAffinityOrAntiAffinityRule an affinityOrAntiAffinityGroupId attributes of the VirtualLinkProfile information element in the NSD (see clause 6.3.4 in ETSI GS NFV-IFA 014 [i.12]).

5.6 Use case 5: Checking multi-site connectivity

5.6.1 Introduction

In real network deployments, the distribution and number of sites (N-PoPs) can span different geographical locations. To support the instantiation and operation of NSs with VNFs and PNFs instantiated over different sites, connectivity provided by one or more WANs is needed. Furthermore, depending on the WAN topology, it can be the case that certain connectivity is only possible among certain sites. In order for the NFVO to perform the right selection of sites, also taking into account network operator's placement constraints, information about the connectivity (reachability) among sites is needed.

Figure 5.6.1-1 illustrates an example. It is assumed the instantiation of an NS composed of two VNFs, VNF#1 and VNF#2, with a Virtual Link connecting them, and with the requirement that the two VNF instances are anti-affine, thus to be placed in different NFVI-PoPs. In this case, the NFVO needs to know the connectivity reachability among the NFVI-PoPs. For example, if VNF#1 is placed in NFVI-PoP#1, then two NFVI-PoPs, NFVI-PoP#2 and NFVI-PoP#3, can be selected ensuring that connectivity is possible.

NOTE: In Figure 5.6.1-1, it is assumed that there is no routing/forwarding at NFVI-PoP#2 and NFVI-PoP#3 possible between WAN#1 and WAN#2.

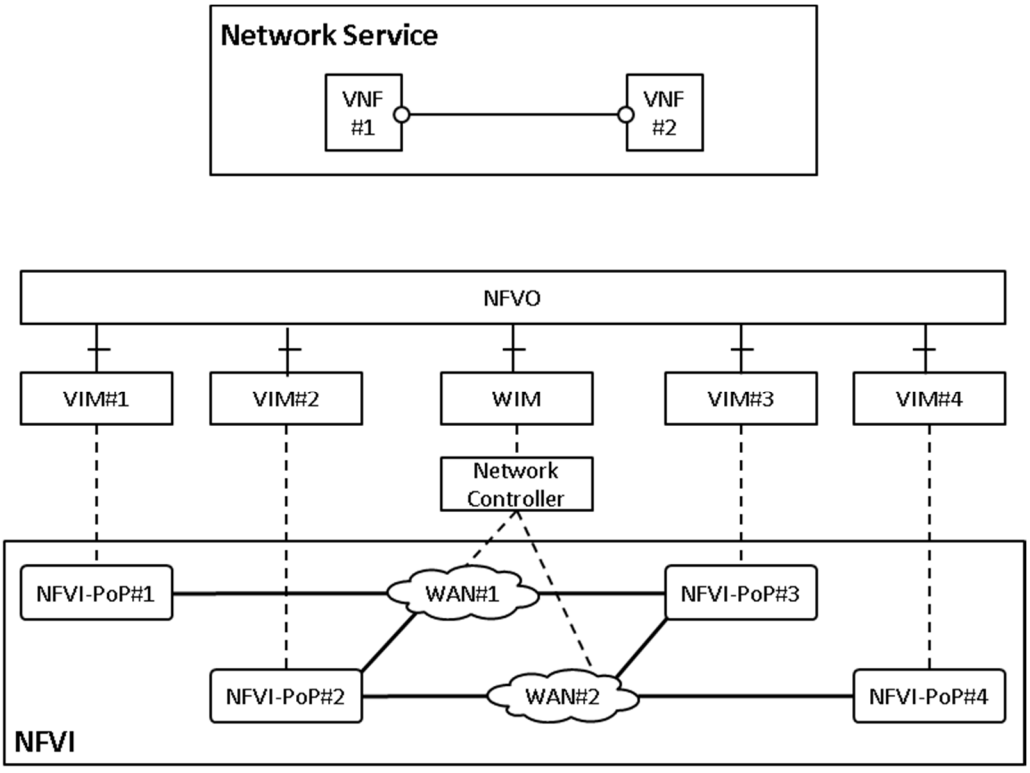

Figure 5.6.1-1: Example showing need to check multi-site connectivity

For building the multi-site connectivity topology, two main sources of information are needed:

a) the network connectivity information about the endpoints of the site (e.g. NFVI-PoP), which can be acquired from the VIM managing such NFVI-PoP (see clause 6.10 of ETSI GS NFV-IFA 010 [i.6]); and

b) the network connectivity information about the inter multi-site networks (e.g. WAN), to be acquired from the WIM managing the WAN resources.

The goal of the present use case is to enable the NFVO acquiring logical connectivity information about the different sites and the WAN networks, so that the NFVO can discover multi-site connectivity topology information and use such information to perform the required NS and resource orchestration tasks.

5.6.2 Trigger

Table 5.6.2-1 describes the use case trigger.

Table 5.6.2-1: Checking multi-site connectivity trigger

Trigger	Description
NFVO	The NFVO determines the need to check multi-site connectivity. The source can be diverse: a) internal to the NFVO, e.g. from a specific operator configuration (e.g. periodic updates), b) external to the NFVO, e.g. receiving an explicit update request, receiving a request for NS instantiation, or as a result of some notification of connectivity changes.

5.6.3 Actors and roles

Table 5.6.3-1 describes the use case actors and roles.

Table 5.6.3-1: Checking multi-site connectivity actors and roles

#	Actor	Description
1	NFVO	
2	WIM	
3	VIM	
4	Network Controller	

5.6.4 Pre-conditions

Table 5.6.4-1 describes the pre-conditions.

Table 5.6.4-1: Checking multi-site connectivity pre-conditions

#	Pre-condition	Description
1	The NFVO has the information about the VIM(s) and WIM(s) managing the corresponding NFVI-PoPs and WANs.	

5.6.5 Post-conditions

Table 5.6.5-1 describes the post-conditions.

Table 5.6.5-1: Checking multi-site connectivity post-conditions

#	Post-condition	Description
1	The NFVO has the multi-site connectivity topology information.	

5.6.6 Operational Flows

Table 5.6.6-1 describes the operational flow.

Table 5.6.6-1: Checking multi-site connectivity operational flow

#	Flow	Description
1	NFVO	The NFVO determines the need to check multi-site connectivity. It gets the list of VIM(s) and WIM(s) from which the connectivity information needs to be retrieved.
2	NFVO -> VIM	For each VIM from step 1, the NFVO queries NFVI-PoP network information from the VIM. See note. *Interface - Or-Vi*
3	VIM -> NFVO	The VIM responds to the query for NFVI-PoP network information providing information about the network connectivity endpoints to the NFVI-PoP. See note. *Interface - Or-Vi*
4	NFVO -> WIM	For each WIM from step 1, the NFVO queries WAN network information from the WIM. See note. *Interface - Or-Vi*
5	WIM -> Network Controller	Each WIM requests to the Network Controller network topology information of the WAN. See note.
6	Network Controller -> WIM	The Network Controller returns the response to the request with topology information of the WAN. See note.
7	WIM -> NFVO	The WIM returns to the NFVO the response to the query on WAN network information, in particular containing information about the network endpoints that can be reached over the WAN, the alternate paths between endpoints, and any other network capabilities, e.g. QoS supported, etc. See note. *Interface - Or-Vi*
8	NFVO	The NFVO correlates the information obtained from the VIM(s) in step 3 and the information obtained from the WIM(s) in step 7 and creates or updates the local view of the multi-site connectivity topology information.
NOTE: The set of steps {2, 3} and {4, 5, 6, 7} can be executed sequentially or in parallel for each VIM and WIM.		

5.6.7 Other Considerations (e.g. Performance)

The use case description focuses on the NFVO acquiring enough information to correlate and be able to build a view of the multi-site connectivity topology information. It should be considered that not only topology information is needed, but the NFVO should also be capable to acquire information about the capacity and performance of the network.

5.6.8 Analysis

The goal of this use case is to enable the NFVO acquiring connectivity information about the different sites and the WAN networks, so that the NFVO can discover multi-site connectivity topology information and use such information to perform the required NS and resource orchestration tasks. To achieve this goal, the connectivity information should at least contain the following items:

- NFVI-PoPs that can be reached over the WAN:
  - The NFVO needs this information to check the reachability between a VNF to be allocated and other VNFs that need to be connected to the VNF across the WAN, and subsequently select an appropriate site/NFVI-PoP for the VNF.
  - This information should also contain information to indicate which network connectivity endpoint of the WAN is peering to which network connectivity endpoint of the NFVI-PoP.
- Connectivity type(s) supported by the WAN (see note):
  - The NFVO needs this information to check if the WAN can accommodate a Virtual Link with certain connectivity type requirements as specified in the NSD (see clause 6.5.3 in ETSI GS NFV-IFA 014 [i.12]).

- Aggregation support:
  - The NFVO needs this information to check if a virtualised network resource provided by this WAN can be used for aggregation of Virtual Links as shown in Use Case 4 in clause 5.5. To support VL aggregation, differentiation of the data flows from different VL at WAN endpoints is needed.
  - This may depend on the connective type selected for the virtualised network resource.
- QoS supported by the WAN:
  - NFVO needs this information to check if the WAN can accommodate a Virtual Link with certain QoS requirements as specified in the NSD (see clause 6.5.6 in ETSI GS NFV-IFA 014 [i.12]).
- Bitrate supported by the WAN:
  - The NFVO needs this information to check if the WAN can accommodate a Virtual Link with certain throughput requirements as specified in the NSD (see clause 6.3.4 in ETSI GS NFV-IFA 014 [i.12]). This information is also used for making a decision by NFVO on whether to allocate/terminate a virtualised network resource (i.e. scale-in/scale-out) or to update the bitrate of an existing virtualised network resource (i.e. scale-up/scale-down) when throughput requirements from managed NSs change (see also BF#2 in Use Case 1 in clause 5.2).
  - This information can contain maximum/minimum bitrate of a virtualised network resource and step size for runtime bitrate control produced by the WIM.
  - It is also assumed that WAN may not support runtime bitrate control, but only support providing limited number of fixed bitrates (e.g. 100 Mbps, 1 Gbps and 10 Gpbs).
- Capacity information of the WAN:
  - The NFVO needs this information to check if the WAN has enough amounts of available resources to accommodate a Virtual Link.
  - This information can contain total capacity, reserved capacity, and available capacity of the WAN and/or network connectivity endpoints of the WAN, such as the number of virtualised network resources and bitrate.

NOTE: NFVI-PoPs and the WAN need to negotiate with each other about what specific protocol and its configuration parameters are used to support the certain connectivity type(s). However, this negotiation can be performed by operators when they physically interconnect the NFVI-PoPs to the WAN, therefore such a negotiation may not be necessary to perform in runtime. Thus, in this use case, such a negotiation is out of scope, and focuses only on network service level information.

5.7 Use case 6: Multi-site Virtual Link redundancy

5.7.1 Introduction

For any real networks which provide commercial services for customers, high availability is an essential requirement in order to minimize impacts to the services due to failures in the infrastructure.

WAN connectivity can fail due to a natural disaster, a malicious attack, a crash of the hardware or software which compose the underlying network and so on. Such failures can impact end-to-end NSs which utilize the WAN.

The goal of the present use case is to enable recovering from WAN connectivity failures by introducing multi-site Virtual Link redundancy. In the present use case, two or more NS Virtual Links connect two VNFs placed in different sites. The NS Virtual Links are anti-affine in terms of physical WAN resources, i.e. different pieces of WAN connectivity which are physically separated in WAN(s) are used. As a result, even if one of the NS Virtual Links fails, the two VNFs can continue to communicate with each other by using the other NS Virtual Link which is not affected by the failure. The use case assumes also that the VNF has port redundancy, and requirements for external connectivity have also been made aware to the Service Provider and/or NFV-MANO.

Figure 5.7.1-1 shows a connectivity overview for multi-site Virtual Link redundancy. The NS in Figure 5.7.1-1 of use case #1 in clause 5.2 is updated by adding a new Virtual Link#2 that also connects the vCPE and vAPL for redundancy. That is, the Virtual Link#1 is used as a primary link and the Virtual Link#2 is used as a secondary link. To ensure the required resilience, the Virtual Link#1 and the Virtual Link#2 are declared anti-affine. In order to satisfy the anti-affinity constraint, a virtualised network resource#2 for the Virtual Link#1 and a virtualised network resource#5 for the Virtual Link#2 are allocated in WAN#1 and WAN#2 respectively. As a result, the Virtual Link#1 consists of the virtualised network resource#1, #2 and #3 crossing WAN#1 while the Virtual Link#2 consists of the virtualised network resource#4, #5 and #6 crossing WAN#2.

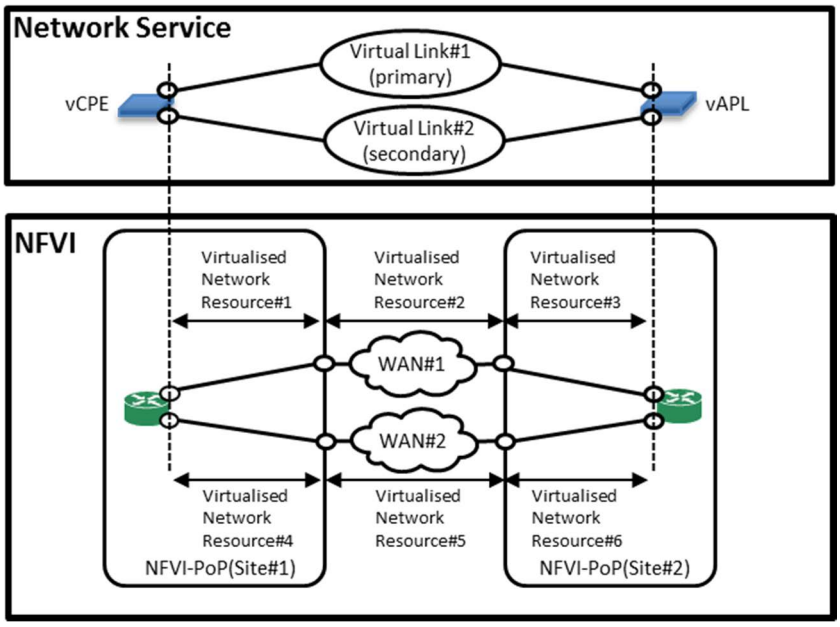

Figure 5.7.1-1: Connectivity overview for multi-site Virtual Link redundancy

5.7.2 Trigger

Table 5.7.2-1 describes the use case trigger.

Table 5.7.2-1: Multi-site Virtual Link redundancy trigger

Trigger	Description
WIM->NFVO	The WIM notifies the NFVO of an alarm resulting from a connectivity fault related to the virtualised network resource#2.

5.7.3 Actors and roles

Table 5.7.3-1 describes the use case actors and roles.

Table 5.7.3-1: Multi-site Virtual Link redundancy actors and roles

#	Actor	Description
1	EM	
2	NFVO	
3	VNFM	
4	WIM	

5.7.4 Pre-conditions

Table 5.7.4-1 describes the pre-conditions.

Table 5.7.4-1: Multi-site Virtual Link redundancy pre-conditions

#	Pre-condition	Description
1	The E2E EvCPE service is instantiated and works properly according to the SLA.	
2	The NFVO is subscribed with the WIM for notifications related to alarms and alarm state changes resulting from connectivity faults related to the virtualised network.	
3	The primary and secondary Virtual Links (Virtual Link#1 and Virtual Link#2, respectively) have been allocated.	According to Figure 5.7.1-1, the vCPE and vAPL use the Virtual Link#1 to communicate with each other.

5.7.5 Post-conditions

Table 5.7.5-1 describes the post-conditions.

Table 5.7.5-1: Multi-site Virtual Link redundancy post-conditions

#	Post-condition	Description
1	The vCPE and vAPL use the Virtual Link#2 to communicate with each other.	The E2E EvCPE service works properly according to the SLA.

5.7.6 Operational Flows

Table 5.7.6-1 describes the operational flow.

Table 5.7.6-1: Multi-site Virtual Link redundancy operational flow

#	Flow	Description
1	WIM -> NFVO	The WIM notifies to the NFVO an alarm resulting from a failure of a connectivity related to the virtualised network resource#2. *Interface - Or-Vi*
2	NFVO	The NFVO correlates the alarm and identifies the Virtual Link#1 affected by the failure.
3	NFVO->VNFM	The NFVO informs to the respective VNFM of the vCPE and vAPL that the corresponding external connection point connecting to the Virtual Link#1 is down. *Interface - Vi-Vnfm*
4	VNFM -> EM	The VNFM notifies to the respective EM of the vCPE and vAPL the change in the state of the external connection point that connects to the Virtual Link#1. See note. *Interface - Ve-Vnfm-em*
5	EM	The EM updates the routing configuration of the vCPE and vAPL to use the Virtual Link#2 instead of the Virtual Link#1 to communicate with each other.
NOTE: The EM might have already identified (e.g. direct alarm from the VNF) the need to perform the failover and use the connections points(s) for the Virtual Link#2, in which case, such a notification from the VNFM can be ignored by the EM.		

5.7.7 Other Considerations (e.g. Performance)

The use case assumes that the VNF supports dual connectivity modes for active/stand-by as shown on Figure 5.7.1-1. However, the relevant part of the use case concerns to multi-site connectivity in which NS Virtual Links are requested and established using virtualised network resources that are anti-affine not only in the WAN, but also in the NFVI-PoP. Therefore, the number of combinations of anti-affinity rules grows when virtualised network resources span different areas such as NFVI-PoP and WAN.

In addition, resource usage optimization should be considered when handling the affinity/anti-affinity rules and redundancy requirements. For instance, to fulfill the VL redundancy, virtualised network resources in the WAN may be provisioned from the same WAN instance, or from different WAN instances, as long as the anti-affinity and redundancy requirements are met.

5.7.8 Analysis

For enabling the multi-site Virtual Link redundancy, the NFV-MANO should be able to:

1) Handle affinity/anti-affinity constraints to ensure that NS Virtual Links are anti-affine in terms of physical WAN resources, when such NS VLs are set for redundancy purposes.

The capability is described in the clause 5.7.1 of the present use case and as part of the pre-conditions available in Table 5.7.4-1.

ETSI GS NFV-IFA 010 [i.6] already defines the affinity/anti-affinity of virtualised network resources (refer to clause 3.1 of [i.6]). Anti-affinity of virtualised network resources force VLs to not share any physical connectivity. Requirement Vim.Vrm.006 of [i.6] specifies the capability for the VIM to enforce affinity and anti-affinity policies for NFVI resource management.

NST_NSF006 requirement of ETSI GS NFV-IFA 014 [i.12] specifies also the support of an NS deployment flavour to describe affinity and anti-affinity rules between the constituent VLs of an NS, which is further specified as an attribute affinityOrAntiAffinityGroup of the NsDf information element (refer to clause 6.3.2 of [i.12]) and by the localAffinityOrAntiAffinityRule of the VirtualLinkProfile (refer to clause 6.3.4 of [i.12]).

Finally, ETSI GS NFV-IFA 005 [i.7] provides means for declaring affinity/anti-affinity constraints when handling the allocation/reservation of virtualised network resources by using the AffinityOrAntiAffinityConstraint information element (refer to clause 8.4.8 of [i.7]) in the offered Virtualised Network Resource Management interface (example in the AllocateNetwork operation in clause 7.4.1.2 of [i.7]).

The scope of the affinity/anti-affinity rules (be it a group or local rules) is particularly relevant in the case of considering WAN connectivity. The referred attributes and corresponding information elements provide examples about the usage of the scope for rules applicable to network virtualised resources within an NFVI-PoP, or between NFVI-PoPs. However, the referred attributes and information elements do not describe/specify for WAN type connectivity.

2) Receive and handle alarm notification in order to be able to determine the fault conditions of virtualised network resources on the WAN.

The capability is introduced in the steps 1 and 2 of the operational flow in Table 5.8.6-1. The capability is introduced in the steps 1 and 2 of the operational flow in Table 5.7.6-1.

The analysis in clause 5.8.8 of use case #7 is also applicable for the support of this capability (refer to clause 5.8.8).

3) The NFVO informing/notifying the VNFM about the changes/failures of connectivity on an NS Virtual Link, and subsequently the VNFM notifying the respective EM of the change of state of the external connection point that connect to the failing NS Virtual Link.

The capability is described in the steps 3 and 4 of the operationl flow in Table 5.7.6-1.

In the first step, the NFVO notifying/informing the VNFM about the corresponding external connection point connecting to the failing NS VL being down, such a capability is not explicitly supported on the ETSI GS NFV-IFA 007 [i.8], unless the virtualised resource management is performed in indirect mode via the NFVO. When the indirect mode is used, the AlarmWithRpNotification information element (refer to clause 8.4.7.3 of [i.8]) used in the Virtualised Resource Fault Management interface (refer to clause 6.4.6 of [i.8]) might be employed.

In the second step, the VNFM notifies the respective EM, the Notify operation of the VNF Fault Management interface can be employed (refer to clause 7.5.3 of ETSI GS NFV-IFA 008 [i.9]) to issue an AlarmNotification (refer to clause 9.3.2 of [i.9]) . The Alarm information element (refer to clause 9.3.4 of [i.9]) provides the necessary attributes information to identify the managedObjectId, the failure type and the failure details to notify the change in the state of a specific virtualised network resource, in this case, the external connection point connecting to the failing NS VL.

An alternative (or complementary) method for realizing the first step (see above) is by offering a mechanism by the VNFM to enable a consumer to disconnect/detach a specific external connection point of a VNF from its current connected external VL. Considering the use case and the description in step 3 of the operation flow in Table 5.7.6-1, and with the assumption that the NFVO has correlated enough state and failure information, the NFVO could request the VNFM to disconnect the external connection point connecting to the Virtual Link#1. In this way, the VNFM would learn of the unavailbility of the connectivity to the Virtual Link#1 (i.e. when the connection point is disconnected) and subsequently notifiy the EM about the change in the state of the external connection point. Currently, VNF LCM interface produced by the VNFM offers the ChangeExtVnfConnectivity operation (refer to clause 7.2.18 of ETSI GS NFV-IFA 007 [i.8]), which allows for changing existing connectivity of an external CP of the VNF from a source external VL to a target external VL. However, the operation does not offers the means to connect/disconnect a specific external CP.The VNF Forwarding Graph Descriptor defined in ETSI GS NFV-IFA 014 clause 6.4 [i.12] allows referencing multiple NS Virtual Link Descriptors, which support the functionality called for in this use case. However, neither the VNF forwarding Graph Descriptor nor the NSVirtualLinkDescriptor defined in ETSI GS NFV-IFA 014 [i.12], clause 6.5 do not currently specify whether these links are active at the same time (e.g. for multi-path forwarding), or which one of them is the primary and which one of them is the secondary link. Furthermore, with the existing definition of these information objects, it is not possible to unambiguously define flow rules (using the Nfpd information object) for the primary and secondary paths, nor is it possible to guarantee consistency of Nfpd associations to path segments in a multi-path forwarding environment. Extending these information elements should be considered to address these shortcomings.

This use case addresses only the provisioning of multiple virtual link resources between two sites for the purpose of redundancy. It is noted that forwarding protocols in the transport network (such as MPLS, Border Gateway Protocol (BGP), etc.) may, depending on the configuration, automatically provide a certain degree of redundancy for virtual links between two sites. The interaction between the WIM and the NFVO for provisioning resources in such cases is left for further study.

5.8 Use case 7: Multi-site Virtual Link healing

5.8.1 Introduction

For any real networks which provide commercial services for customers, high availability is an essential requirement in order to minimize impacts to the services due to failures in the infrastructure.

WAN connectivity can fail due to a natural disaster, a malicious attack, a crash of the hardware or software which compose the underlying network and so on. Though typically WAN has its mechanisms for recovering physical link failures and does the necessary re-arrangement to fulfil resiliency requirements, such resiliency mechanisms might not be able to recover all failures occurring in the WAN. Such failures, which cannot be recovered in the WAN, can impact end-to-end NSs which utilize the WAN.

The goal of the present use case is to enable recovering from such WAN failures which causes the connectivity failure of a virtual link, and in particular, with the possibility that virtualised resources have been pre-provisioned in the WAN before the healing action takes place. This use case introduces the notion of multi-site Virtual Link healing, which is conceptually similar to VNF healing, but relates to the recovery of Virtual Links in the face of failure. In multi-site Virtual Link healing, when a failure occurs in the WAN that cause connectivity failure of the virtualised network resources impacting the NS, the affected virtualised network resources of the Virtual Link(s) are replaced with other healthy virtualised network resources by the NFV-MANO. This healing process is transparent to the VNF instances which connect to the NS via the affected Virtual Link(s).

There are two major approaches for triggering multi-site Virtual Link healing:

- Automated multi-site Virtual Link healing: In this approach the NFV-MANO monitors conditions of the virtualised network resources over the WAN. If the NFV-MANO detects or is notified about failures of the monitored virtualised network resources , which may impact the NS Virtual Link(s), the NFV-MANO automatically triggers to heal the failing NS Virtual Link(s).

- On-demand multi-site Virtual Link healing: In this approach, the trigger for multi-site Virtual Link healing comes from outside of the NFV-MANO, e.g. from the network operator via OSS.

Even though the triggers are different between the automated multi-site Virtual Link healing and the on-demand multi-site Virtual Link healing, both derive into a common set of steps in the procedure in terms of replacing virtualised network resources allocated on the WAN (refer to the notes in Table 5.8.6-1). Therefore, the present use case focuses just on the automated multi-site Virtual Link healing. The present use case does not take into account any auto-healing capabilities at the WIM and below it.

Figure 5.8.1-1 shows a connectivity overview for multi-site Virtual Link healing. The NS in Figure 5.8.1-1 is the same as the one for the E2E EvCPE service shown in Figure 5.2.1-1 of use case #1 in clause 5.2. The use case assumes the case that virtualised resources are pre-provisioned in the WAN. In this case, the NFVI is expanded so that it has two WANs, i.e. WAN#1 and WAN#2, and virtualised network resource#2 and virtualised network resource#4 are allocated on the WAN#1 and the WAN#2, respectively. The vCPE and the vAPL are connected with a Virtual Link across WAN#1, and the Virtual Link is composed by the virtualised network resource#1, #2 and #3.

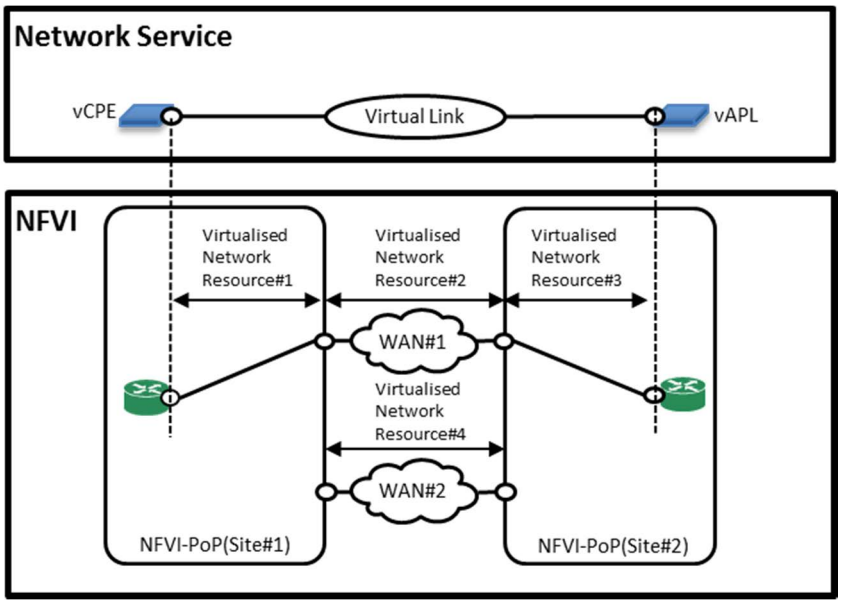

Figure 5.8.1-1: Connectivity overview for multi-site Virtual Link healing

This use case assumes that a connectivity failure occurs in the WAN#1, affecting the associated virtualised network recource#2. Figure 5.8.1-2 shows the connectivity overview after performing multi-site Virtual Link healing. The NFV-MANO detects the failure of the virtualised network resource#2 and finds that the Virtual Link loses its connectivity across WAN#1. Therefore, the NFV-MANO performs multi-site Virtual Link healing to replace virtualised network resource#2 with virtualised network resource#4 of WAN#2. As a result of the healing, the Virtual Link is composed by the virtualised network resources #1, #3 and #4 and its supporting WAN connectivity is recovered from the failure of the virtualised network resource#2 of WAN#1.

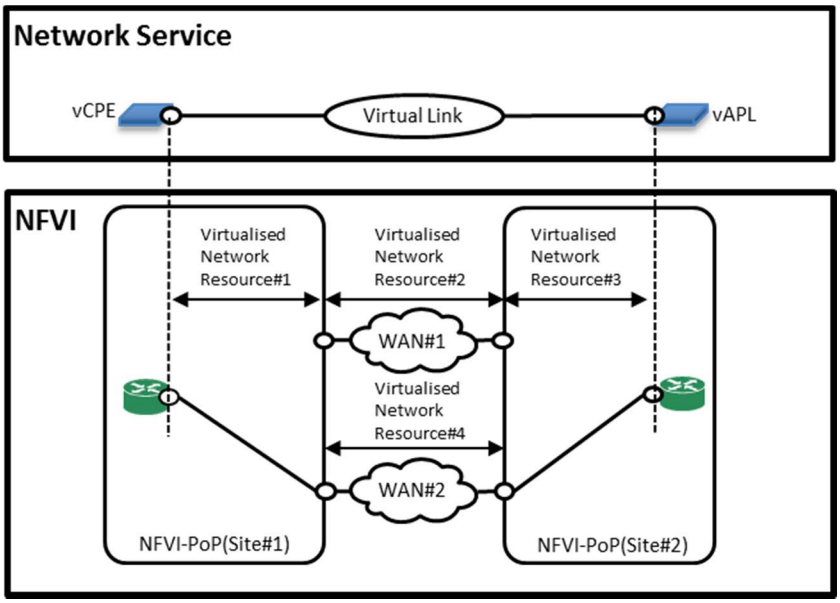

Figure 5.8.1-2: Connectivity overview after multi-site Virtual Link healing

5.8.2 Trigger

Table 5.8.2-1 describes the use case trigger.

Table 5.8.2-1: Multi-site Virtual Link healing trigger

Trigger	Description
WIM->NFVO	The WIM notifies the NFVO of an alarm resulting from a connectivity failure related to the virtualised resource#2.

5.8.3 Actors and roles

Table 5.8.3-1 describes the use case actors and roles.

Table 5.8.3-1: Multi-site Virtual Link healing actors and roles

#	Actor	Description
1	NFVO	
2	VIM	
3	WIM	

5.8.4 Pre-conditions

Table 5.8.4-1 describes the pre-conditions.

Table 5.8.4-1: Multi-site Virtual Link healing pre-conditions

#	Pre-condition	Description
1	The E2E EvCPE service is instantiated and works properly according to the SLA.	The Virtual Link in between vCPE and vAPL crosses the WAN#1.
2	The NFVO is subscribed with the WIM for notifications related to the alarms and their state changes resulting from connectivity failures related to the virtualised network resources.	
3	The redundancy of virtualised network resources for the Virtual Link healing is available.	For instance, according to the scenario depicted in Figure 5.8.1-2, the virtualised network resource#4 has been allocated.

5.8.5 Post-conditions

Table 5.8.5-1 describes the post-conditions.

Table 5.8.5-1: Multi-site Virtual Link healing post-conditions

#	Post-condition	Description
1	The Virtual Link in between vCPE and vAPL crosses WAN#2 and has recovered from the failure on the WAN#1.	The E2E EvCPE service works properly according to the SLA.

5.8.6 Operational Flows

Table 5.8.6-1 describes the operational flow.

Table 5.8.6-1: Multi-site Virtual Link healing operational flow

#	Flow	Description
1	WIM -> NFVO	The WIM notifies the NFVO of an alarm resulting from a connectivity failure related to the virtualised network resource#2. *Interface - Or-Vi*
2	NFVO	The NFVO correlates the alarm and identifies the Virtual Link affected by the failure. The NFVO determines to heal the Virtual Link to remedy the failure of virtualised network resource#2.
3	NFVO	The NFVO checks existing virtualised network resources in the WANs, and selects virtualised network resource#4 at the WAN#2 which is not affected by the failure and can meet the requirements of the Virtual Link in between vCPE and vAPL based on the NSD of the NS, its policy, etc. The NFVO retrieves the information for connecting to the WAN#2. See note 1 and note 3.
4	NFVO -> VIM at Site#1	The NFVO requests the VIM at Site#1 to update the virtualised network resource#1 for connecting to the WAN#2. The NFVO sends information for connecting to the network connectivity over the WAN#2 which is obtained in step 3. See note 2 and note 3. *Interface - Or-Vi*
5	VIM at Site#1	The VIM at Site#1 updates the virtualised network resource#1 for connecting to the WAN#2 at Site#1. See note 2 and note 3.
6	VIM at Site#1 -> NFVO	The VIM at Site#1 returns the response to the request for updating the virtualised network resource#1. See note 2 and note 3. *Interface - Or-Vi*
7	NFVO -> VIM at Site#2	The NFVO requests to the VIM at Site#2 to update the virtualised network resource#3 for connecting to the WAN#2. The NFVO sends information for connecting to the network connectivity over the WAN#2 which is obtained in step 3. See note 2 and note 3. *Interface - Or-Vi*
8	VIM at Site#2	The VIM at Site#2 updates the virtualised network resource#3 for connecting to WAN#2. See note 2 and note 3.
9	VIM at Site#2 -> NFVO	The VIM at Site#2 returns the response to the request for updating the virtualised network resource#3. See note 2 and note 3. *Interface - Or-Vi*
NOTE 1: If the NFVO fails to find any appropriate virtualised network resources, the NFVO can create a new virtualised network resource. This process follows step 2 to step 5 of Table 5.2.6-2 from Use Case 1 "NS for E2E Enterprise vCPE". NOTE 2: The set of steps {4, 5, 6} and set of steps {7, 8, 9} can be executed sequentially or in parallel. That is, the procedure to update connectivity at Site#1 can be executed in parallel to the procedure to update connectivity at Site#2. NOTE 3: With regards to the different two triggers described in clause 5.8.1, this is a step performed in the base flow for both triggers.		

5.8.7 Other Considerations (e.g. Performance)

As part of the Virtual Link healing process, the use case describes transferring the connectivity from the failed WAN virtualised network resources to the healthy ones. This process can take a certain amount of time by which the VNF instances and the NS can see their performance degraded or even fail. Such issues are not fully considered in the use case, which focuses on the multi-site connectivity aspects.

Similarly as with use case #6 (see clause 5.7.7), resource usage optimization should be considered when handling the affinity/anti-affinity rules and resiliency requirements. For instance, to fulfill the VL healing, virtualised network resources in the WAN may be provisioned from the same WAN instance, or from different WAN instances, as long as the anti-affinity and resiliency requirements are met.

5.8.8 Analysis

For enabling the multi-site Virtual Link healing, the NFV-MANO should be able to:

1) Receive and handle alarm notification in order to be able to determine the failure conditions of virtualised network resources on the WAN.

   The capability is introduced in the steps 1 and 2 of the operational flow in Table 5.8.6-1.

   Requirement Nfvo.NsRmpbNfvo.003 of ETSI GS NFV-IFA 010 [i.6] specifies the capability needed by the NFVO to receive notification of the resources that are allocated to or released from specific NS instances as well as events and relevant error or failure reports related to those resources. In addition, ETSI GS NFV-IFA 005 [i.7] specifies the Notify operation produced by the VIM (see clause 7.6.3 in [i.7]) as part of the Virtualised Resource Fault management interface, which allows for the producer to distribute notifications to subscribers, including AlarmNotifications. The requirement and existing operations align with the purpose of this capability. But, neither the requirement, nor the existing operations detail within what network boundaries/scope the reporting of alarms is performed. However, the assumption is that, in particular, the operation Notify of the Virtualised Resource Fault Management interface is produced according to the ETSI GS NFV-IFA 005 [i.7] by the VIM towards the NFVO for virtualised resources managed by the VIM, but not explicitly within WAN scope.

   Some alarms may be handled directly by the WIM, which could first attempt to perform healing on its own supported by control plane protocols associated to the network resources affected by the fault. However, in case the WIM is not successful in healing the connectivity or for other scenarios, such as when control protocol-capabilities of the resources are not configured to perform automatic healing, or when a policy dictates that the NFVO should unequivocally be involved in the healing process, a specific alarm could be provided to the NFVO by the WIM using the Notification mechanism. Other use cases of interaction between NFVO, WIM, and VIM for the purpose of multi-site connectivity healing are possible, but are left for further study.

2) Provision virtualised network resources not yet assigned or in support of a specific NS Virtual Link.

   The capability is described in the pre-conditions of the use case in Table 5.8.4-1.

   ETSI GS NFV-IFA 010 [i.6] and ETSI GS NFV-IFA 005 [i.7] do not detail any specific requirement, operation or information element relevant to this capability. However, the specifications neither specify any restriction with respect to having virtualised network resources only allocate to present NS Virtual Links. Furthermore, requirements and interfaces related to reservation of virtualised network resources can be potentially leveraged as a means to ensure that resources are available when needed to be allocated. Clause A.2 of ETSI GS NFV-IFA 010 [i.6] provides further information on how reservations can be used to fulfil different use cases.

3) Check the characteristics of existing virtualised network resources to help determine whether such resources can meet the requirements for the Virtual Links of the NS based on the information provided in the NSD.

   The relevant capability is described in step 3 of the operational flow in Table 5.8.6-1.

Requirement Nfvo.NsRmpbNfvo.001 of the same referred deliverable [i.6] specifies the support of the capability of the NFVO to issue requests to the VIM in order to allocate, identify, update and release resources needed for the connectivity of NSs. Similarly as with other capabilities, it is not explicitly stated neither by the requirements, nor the existing operations detail within what network boundaries/scope the query of information of existing network virtualised resources is performed. However, the assumption is that, in particular, the operation QueryNetwork of the Virtualised Network Resources Management interface is produced according to the ETSI GS NFV-IFA 005 [i.7] by the VIM towards the NFVO for virtualised network resources managed by the VIM, but not explicitly within WAN scope

4) Update an NS Virtual Link to replace a WAN virtualised network resource that has been assigned to the NS Virtual Link with another WAN virtualised network resource.

   The capability is used in the steps 3 of the operational flow in Table 5.8.6-1.

   Requirement Nfvo.NsU.004 of ETSI GS NFV-IFA 010 [i.6] specifies the capability for the NFVO to support updating the existing VL(s)/VNFFG(s) involved in an existing NS. The requirements does not detail within what network boundaries/scope such update can be performed. Furthermore, the NsVirtualLinkInfo information element (refer to clause 8.3.3.10 in [i.11]) present in the NsInfo of ETSI GS NFV-IFA 013 [i.11] identifies for each NS Virtual Link the ResourceHandle(s) related to the virtualised network resources realizing the VL.

5) Update, via the VIM, the virtualised network resources within the Site to support reconnecting from a WAN virtualised network resource to another WAN virtualised network resource.

   The capability is used in the steps 4, 5, 6 and 7, 8, 9 of the operational flow in Table 5.8.6-1.

   The analysis in clause 5.4.8 of use case #3 is also applicable for the support of this capability (refer to clause 5.4.8).

5.9 Use case 8: Multi-site VNF deployment

5.9.1 Introduction

For any real network which provides commercial services, high availability is an essential requirement in order to minimize impacts to the customers, for example, due to failures in the infrastructure. Realization of a VNF supporting geographical redundancy (e.g. in an active/standby configuration across different geographical sites) is a possible and useful way for dealing with site disasters. For instance, two equal VNFCs are deployed and synchronized, but each one of them executing in different geographically dispersed data centres. If one of the sites fails, the VNF can still perform its service relying on the components from the other site.

NOTE: The recommendation of which mechanisms, additional ones, or even alternative ones to be implemented for VNF high-availability may vary among VNF providers and types of VNF, and therefore, such a recommendation outside the scope of the present use case. Moreover, high availability of the NFV-MANO framework needs to be considered, but this goes beyond the scope of the present use case.

The high-availability realization as described above shows the relevance of supporting the deployment of a VNF across different geographical sites. In such a case, the connectivity across sites becomes an important aspect for the VNF deployment fulfilment.

Figure 5.9.1-1 shows the mapping of the NS to NFVI. Similarly, as in use case #1 in clause 5.2, vCPE and vAPL are placed on to different sites. As in use case #1, the vCPE is placed to Site#1. However, in the present use case, and in order to accommodate to the HA requirements described by the VNF Provider, the vAPL is placed to Site#2 and Site#3. The vCPE and the first set of component of vAPL are connected across WAN#1 with the Virtual Link using the virtualised network resource#1, #2 and #3 and the vCPE and the second set of component(s) of vAPL are connected across WAN#2 with the Virtual Link using the virtualised network resource#4, #5 and #6. The externally-managed internal Virtual Link within the vAPL consists of virtualised network resource#7, #8 and #9 crossing WAN#3.

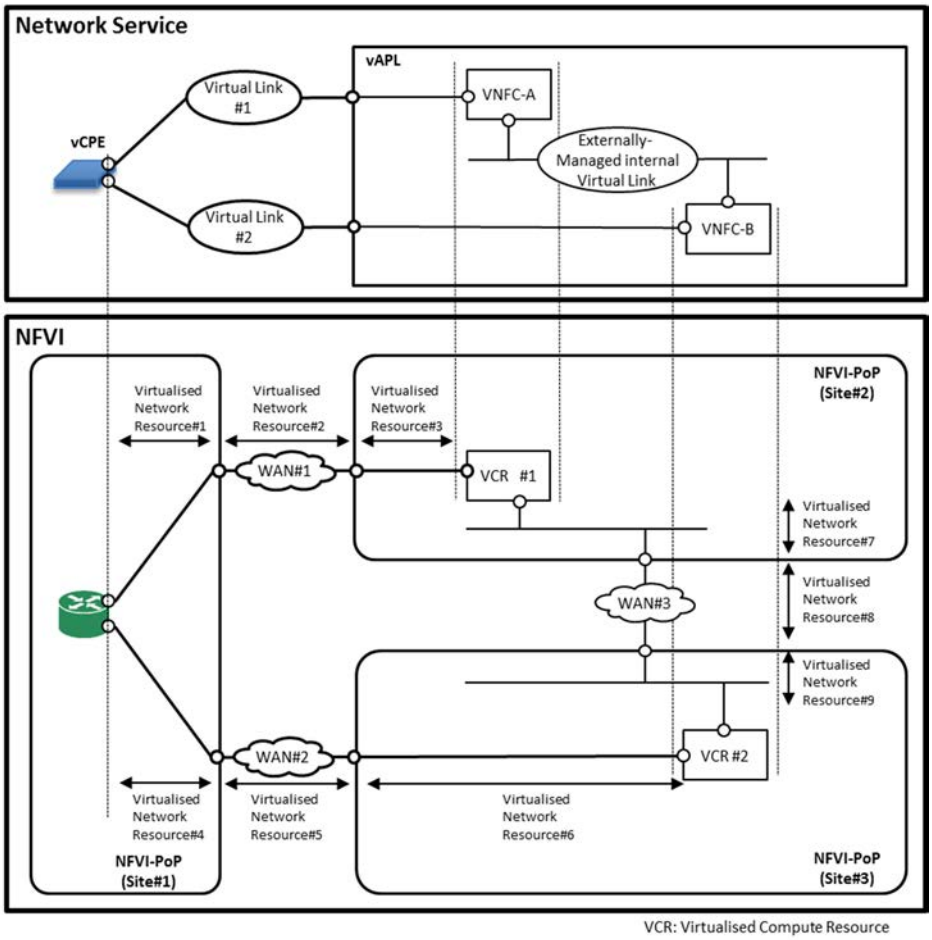

Figure 5.9.1-1: Connectivity overview for multi-site VNF deployment

This use case derives the base flow for deploying a VNF whose VNFCs are placed on different sites and connected with an externally-managed internal Virtual Link.

Figure 5.9.1-2 provides an architectural view of the use case with respect to MANO framework. It shows a multi-site model managed by a single Service Provider. To simplify the architectural model in the figure, it only shows NFVI-PoP (Site#1), NFVI-PoP (Site#2) and the WAN connecting the two sites (WAN#1). The figure also shows the related architectural components (e.g. WIM, Network Controller, NFVO, VNFM, etc.) and reference points, which are referred to in the present use case. Here the architecture includes a WIM for managing WAN#1. However, this does not draw a conclusion as to whether a single or multiple WIMs are needed. The VNFM is responsible for requesting virtualised resources on each site, and NFVO is responsible for requesting virtualised resources across the sites (WAN related).

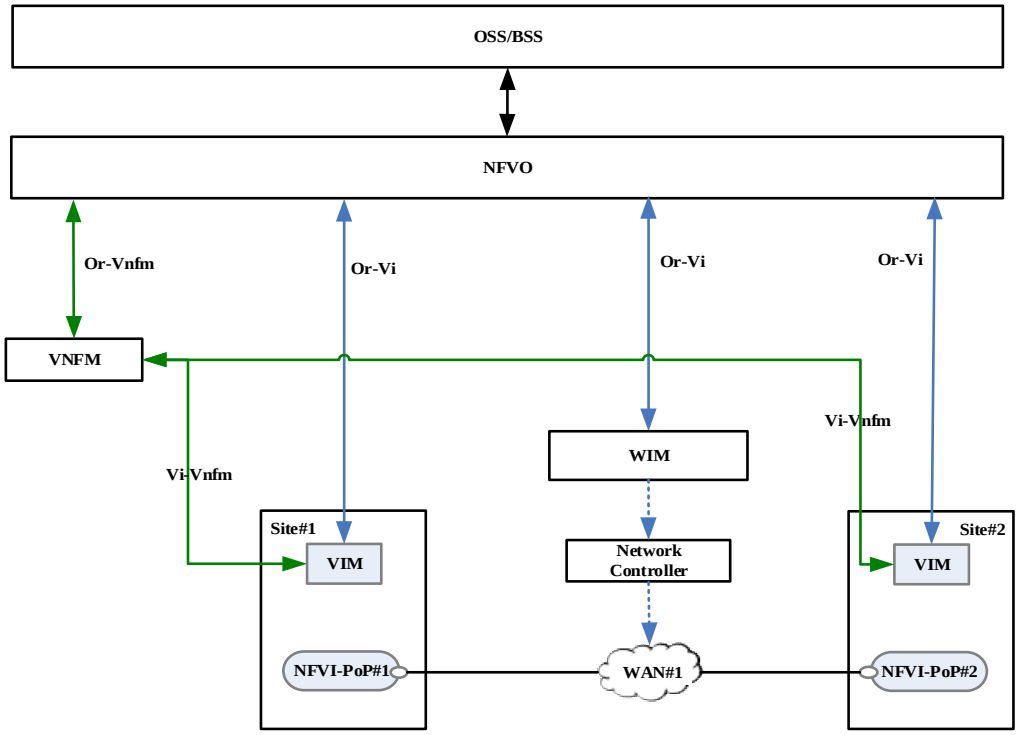

Figure 5.9.1-2: High-level architectural view supporting connectivity for multi-site VNF deployment

5.9.2 Trigger

Table 5.9.2-1 describes the use case trigger.

Table 5.9.2-1: Multi-site VNF deployment trigger

Trigger	Description
OSS/BSS->NFVO	When the NFVO is requested to instantiate a NS for E2E EvCPE service from the OSS/BSS, containing a vAPL VNF supporting geographical redundancy.

5.9.3 Actors and roles

Table 5.9.3-1 describes the use case actors and roles.

Table 5.9.3-1: Multi-site VNF deployment actors and roles

#	Actor	Description
1	OSS/BSS	
2	NFVO	
3	VIM	
4	WIM	
5	Network Controller	
6	VNFM	

5.9.4 Pre-conditions

Table 5.9.4-1 describes the pre-conditions.

Table 5.9.4-1: Multi-site VNF deployment pre-conditions

#	Pre-condition	Description
1	The infrastructure of the NFVI-PoP at Site#1, Site#2 and Site#3 and the network infrastructure of the WAN are physically connected.	
2	The vAPL VNF designed with support of geographical redundancy.	

5.9.5 Post-conditions

Table 5.9.5-1 describes the post-conditions.

Table 5.9.5-1: Multi-site VNF deployment post-conditions

#	Post-condition	Description
1	The Virtual Link#1 in between vCPE and vAPL crosses WAN#1.	
2	The Virtual Link#2 in between vCPE and vAPL crosses WAN#2.	
3	The externally-managed internal Virtual Link within vAPL crosses WAN#3.	
4	E2E EvCPE service can use VNFs across the three sites.	The E2E EvCPE service works properly according to the SLA.

5.9.6 Operational Flows

Table 5.9.6-1 describes the operational flow.

NOTE: According to ETSI GS NFV-IFA 007 [i.8], there are four operations which can provide external Virtual Link(s) to VNFM, i.e. Grant VNF Lifecycle Operation operation, Instantiate VNF operation, Change VNF Flavour operation, and Modify VNF Configuration operation. Similarly, there are three operations which can provide externally-managed internal Virtual Link(s) to VNFM, i.e. Grant VNF Lifecycle Operation operation, Instantiate VNF operation, and Change VNF Flavour operation. This base flow shows one case, which uses the Grant VNF Lifecycle Operation operation for providing external Virtual Link and externally-managed internal Virtual Link.

Table 5.9.6-1: Multi-site VNF deployment operational flow

#	Flow	Description
1	OSS/BSS -> NFVO	The OSS/BSS requests to instantiate a NS for E2E EvCPE service. *Interface - Os-Ma-nfvo*
2	NFVO -> VNFM	The NFVO requests to instantiate a vCPE and a vAPL. *Interface - Or-Vnfm*
3	VNFM -> NFVO	VNFM sends grant requests for instantiating the vCPE and vAPL (see note 2). *Interface - Or-Vnfm*
4	NFVO	The NFVO identifies the suitable sites for deployment of vCPE and vAPL VNF. The NFVO checks the capability (e.g. MPLS and QoS support) and capacity which are provided by the NFVI-PoP at Site#1, the NFVI-PoP at Site#2, the NFVI-PoP at Site#3 and the WANs. Then the NFVO decides: • to place the vCPE in Site#1; • to place the vAPL in Site#2 and Site#3 (i.e. to allocate resources for vAPL in Site#2 and Site#3 according to the grant request received from VNFM); • to setup network connectivity between Site#1 and Site#2 across the WAN#1 for the external Virtual Link#1 and network connectivity between Site#1 and Site#3 across the WAN#2 for the external Virtual Link#2 which connect the vCPE and vAPL; and • to setup network connectivity between Site#2 and Site#3 across the WAN#3 for the externally-managed internal Virtual Link which connects the VNFC-A and VNFC-B forming the vAPL.
5	NFVO, VIM at Site#1, VIM at Site#2, WIM, Network Controller	The network connectivity between Site#1 and Site#2 across the WAN#1 for the external Virtual Link#1 is setup according to the step 3 to step 13 of "NS for E2E Enterprise vCPE base flow#1.1" (Table 5.2.6-1). The external Virtual Link#1 consists of virtualised network resource#1 for Site#1, virtualised network resource#2 for WAN#1 and virtualised network resource#3 for Site#2. See note 1.
6	NFVO, VIM at Site#1, VIM at Site#3, WIM, Network Controller	The network connectivity between Site#1 and Site#3 across the WAN#2 for the external Virtual Link#2 is setup according to step 3 to step 13 of "NS for E2E Enterprise vCPE base flow#1.1" (Table 5.2.6-1). The external Virtual Link#2 consists of virtualised network resource#4 for Site#1, virtualised network resource#5 for WAN#2 and virtualised network resource#6 for Site#3. See note 1.
7	NFVO, VIM at Site#2, VIM at Site#3, WIM, Network Controller	The network connectivity between Site#2 and Site#3 across the WAN#3 for the externally-managed internal Virtual Link is setup according to the step 3 to step 13 of "NS for E2E Enterprise vCPE base flow#1.1" (Table 5.2.6-1). The externally-managed internal Virtual Link consists of virtualised network resource#7 for Site#2, virtualised network resource#8 for WAN#3 and virtualised network resource#9 for Site#3. See note 1.
8	NFVO -> VNFM	NFVO sends the grant response for instantiating the vCPE indicating the virtualised network resource#1 for the external Virtual Link#1 and the virtualised network resource#4 for the external Virtual Link#2. NFVO also sends the grant response for instantiating the vAPL indicating the allocation of virtual compute resources on Sites 2 and 3, virtualised network resource#3 for the external Virtual Link#1, the virtualised network resource#6 for the external Virtual Link#2 and the virtualised network resource#7 and #9 for the externally-managed internal Virtual Link. *Interface - Or-Vnfm*
9	VNFM	The VNFM completes the instantiation process for the vCPE and vAPL.
10	VNFM -> NFVO	VNFM returns the results of the VNF instantiation. *Interface - Or-Vnfm*
11	NFVO -> OSS/BSS	NFVO returns the results of the NS instantiation. *Interface - Os-Ma-nfvo*
NOTE 1: The steps 5, 6 and 7 can be executed sequentially or in parallel. That is, the procedures to setup connectivity for the external Virtual Link#1, the external Virtual Link#2 and the externally-managed internal Virtual Link can be executed in parallel. NOTE 2: The grant request may include the anti-affinity constraint for VR supporting vAPL (allowing deployment of vAPL VNFCs on geographically distributed NFVI PoPs).		

5.9.7 Other Considerations (e.g. Performance)

In this use case, the VNF is deployed in multiple NFVI-PoPs for high availability purpose. Although the traffic of the VNF passes through multiple NFVI-PoPs, the NFVO selects virtual links with appropriate QoS (e.g. bandwidth, latency) for the VNF. Therefore, the performance of the VNF can be guaranteed.

The use case also assumes the capability of the VNFM to connect to two VIMs controlling resources on two different sites to fulfill the resource provisioning for a single VNF instance.

5.9.8 Analysis

For enabling the multi-site VNF deployment, the NFV-MANO should be able to:

1) Process the requirements for the deployment of a VNF concerning affinity/anti-affinity constraints for virtualised resources, in particular for resources to be geographically distributed among NFVI-PoPs.

   The capability is described in the step 3 and 4 of the operation flow in Table 5.9.6-1.

   Regarding the capability to define affinity/anti-affinity constraints of components that constitute a VNF, ETSI GS NFV-IFA 011 [i.10] specifies the information elements LocalAffinityOrAntiAffinityRule (refer to clause 7.1.8.11 of ETSI GS NFV-IFA 011 [i.10]) and AffinityOrAntiAffinityGroup (refer to clause 7.1.8.12 of ETSI GS NFV-IFA 011 [i.10]). The scope attribute in both information elements specifies the possible value to determine a VNF deployment where some of the components need to be affine or anti-affine at the NFVI-PoP (Site) level. The affinity/anti-affinity information in the VNFD can be further extended during the granting process between the VNFM and NFVO. The GrantVnfLifecycleOperation operation on the VNF Lifecycle Granting interface produced by the NFVO (refer to clause 6.3.2 of ETSI GS NFV-IFA 007 [i.8]) includes the placementConstraint parameter, which in turn provides the possibility to define affinity/anti-affinity at the NFVI-PoP scope during runtime VNF LCM management.

   With the information provided by the affinity/anti-affinity constraints, plus the information/requirements for the internal VLs of the VNF, the NFVO has the necessary information to determine the placement of components across multiple sites, if required. Nonetheless, the NFVO should be capable to determine the usage of an externally-managed internal VL to fulfil the multi-site connectivity requirements.

2) Maintain and provide the information to the relevant management entities about externally-managed internal Virtual Links with corresponding virtualised network resources realizing such VLs used for multi-site VNF deployment.

   The capability is described in the steps 4, 7 and 8 of the operational flow in Table 5.9.6-1.

   As depicted in step 8 of the operational flow, the NFVO provides to the VNFM only information about the virtualised network resources #7 and #9 of the externally-managed internal VL. The virtualised network resource #8 that realizes the multi-site WAN connectivity is not provided, which is entirely managed by the NFVO.

   The VnfInfo information element managed by the VNFM (refer to clause 8.5.2 of ETSI GS NFV-IFA 007 [i.8]) can contain information about externally-managed internal VL. The VnfInfo information kept by the NFVO (refer to clause 8.3.3.3 of ETSI GS NFV-IFA 013 [i.11]) can contain also information about externally-managed internal VL. However, differently to the NsVirtualLinkInfo used for NS VL, the ExtManagedVirtualLinkInfo of ETSI GS NFV-IFA 013 [i.11] does not provide the flexibility of having more than one virtualised network resource realize such an externally-managed internal VL, which is the common scenario as depicted in the use case (refer to virtualised network resources #7, #8 and #9). Furthermore, when considering such an extension, information is also needed about the link ports, as well as to which virtualised network resource these link ports belong to.

3) Virtualised resource management on a per-VIM basis for VNF multi-site deployment.

   As introduced in clause 5.9.7 and referring to the capability described in step 9 of the operation flow in Table 5.9.6-1, VNFM needs to be able to connect and request virtualised resource management from different VIMs in order to fulfill the resource provisioning for a single VNF instance.

   The ResourceHandle information element specified in ETSI GS NFV-IFA 007 [i.8] already supports the identification of VIM connectivity information to manage a specific virtualised resource (refer to VimConnectionInfo information element in ETSI GS NFV-IFA-007 [i.8]).

The VNF Lifecycle Operation Granting interface in clause 8.3 of ETSI GS NFV-IFA 007 [i.8] also supports indicating the specific VIM connections associated to a specific granted virtualised resource, as specified in the GrantInfo information element. In addition, providing information about more than one VimConnectionInfo in the granting operation response is supported.

Finally, reference is also provided to the note in clause 6.3.2.1 of ETSI GS NFV-IFA 007 [i.8], for which the current use case and enhancements proposed in the present analysis address the limitations stated in the referred Release 2 ETSI GS specification. With respect to the two issues identified in the note:

- "A mechanism is needed to manage the VNF-internal Virtual Link (VL) requirements across multiple VIMs": The use case and analysis propose using the capability of "externally-managed VLs" to fulfil the provisioning of the VNF-internal VL. The task of ensuring the requirements across multiple VIMs and the WAN is performed by the NFVO as entity responsible for the orchestration of virtualised resources across different NFVI-PoPs and WAN.

- "signalling external and externally-managed VLs in the lifecycle management operations assumes single-VIM VNFs and does not fulfil the requirements of multi-VIM scenarios": As addressed in the analysis of the present use case, enhancements to the ExtManagedVirtualLinkInfo are needed (refer to point 2) in the present clause).

5.10 Use case 9: Addressing multi-site deployment requirements in NSDs

5.10.1 Introduction

Multi-site NS deployments might be required due to a number of reasons: e.g. redundant/HA architectures, load balancing necessities, regulatory constraints, etc.

It is reasonable to assume that a service provider might be aware of the need to deploy a given NS instance across multiple sites already at design time. According to NFV Release 2, the only mechanisms supported by NSDs on which a service provider can leverage to this end are AffinityOrAntiAffinityGroup and LocalAffinityOrAntiAffinityRule information elements (see ETSI GS NFV-IFA 014 [i.12], clauses 6.3.5 and 6.3.8, respectively). The former is intend to address the description of affinity and anti-affinity rules between constituent VNFs of a given NS (see ETSI GS NFV-IFA 014 [i.12], clause 5.3, requirement NST_NSF_004) while the latter is supposed to address the description of affinity and anti-affinity rules between different instances of the same constituent VNF (see ETSI GS NFV-IFA 014 [i.12], clause 5.3, requirement NST_NSF_003).

NOTE: For the sake of simplicity, the present use case focuses only on VNFs. However, it is worth noticing that AffinityOrAntiAffinityGroup applies indiscriminately to VNF, VL and nested NS instances while LocalAffinityOrAntiAffinityRule applies to both VNF and VL instances.

Even though they can be sufficient in some cases, AffinityOrAntiAffinityGroup and LocalAffinityOrAntiAffinityRule information elements are characterized by a level of inefficiency and non-determinism, as discussed in clause 5.10.8. Therefore, after proper analysis, this use case aims at highlighting the potential value of an alternative approach.

5.10.2 Trigger

Table 5.10.2-1 describes the use case trigger.

Table 5.10.2-1: Addressing multi-site deployment requirements in NSDs trigger

Trigger	Description
	A service provider needs to deploy an NS across multiple sites and wants to specify the corresponding NSD reflecting this requirement.

5.10.3 Actors and roles

Table 5.10.3-1 describes the use case actors and roles.

Table 5.10.3-1: Addressing multi-site deployment requirements in NSDs actors and roles

#	Actor	Description
1	Service Designer	Service provider function responsible for defining and providing requirements (functional and non-functional) for required services. Also responsible for creating services to be deployed by the service provider.
2	OSS/BSS	
3	NFVO	

5.10.4 Pre-conditions

Table 5.10.4-1 describes the pre-conditions.

Table 5.10.4-1: Addressing multi-site deployment requirements in NSDs pre-conditions

#	Pre-condition	Description
1	N.A.	

5.10.5 Post-conditions

Table 5.10.5-1 describes the post-conditions.

Table 5.10.5-1: Addressing multi-site deployment requirements in NSDs post-conditions

#	Post-condition	Description
1	The NSD addressing multi-site deployment requirements is successfully on-boarded.	

5.10.6 Operational Flows

Table 5.10.6-1 describes the operational flow.

Table 5.10.6-1: Addressing multi-site deployment requirements in NSDs operational flow

#	Flow	Description
1	Service Designer	The Service Designer creates an NSD which addresses multi-site deployment requirements for the NS to be instantiated.
2	OSS/BSS → NFVO	The newly created NSD is provided to the NFVO via the On-board NSD operation (see ETSI GS NFV-IFA 013 [i.11] (V2.1.1), clause 7.2.2).

5.10.7 Other Considerations (e.g. Performance)

No other considerations are derived from the present use case.

5.10.8 Analysis

Quoting from ETSI GS NFV-IFA 014 [i.12], AffinityOrAntiAffinityGroup can be used to describe "the affinity or anti-affinity relationship applicable between the VNF instances created using different VnfProfiles". Please note that in order to specify a multi-site NS deployment, the scope attribute is supposed to be set to "NFVI-PoP" (a.k.a., site).

Consider the following:

- ***n*** the number of sites on which the NS instance is intended to be deployed;
- N_1 the number of required affinity groups (i.e. AffinityOrAntiAffinityGroup information elements with the affinityOrAntiAffiinity attribute set to "affinity");
- N_2 the number of required anti-affinity groups (i.e. AffinityOrAntiAffinityGroup information elements with the affinityOrAntiAffiinity attribute set to "anti-affinity");
- ***N*** the total number of required affinity and anti-affinity groups (i.e. $N = N_1 + N_2$).

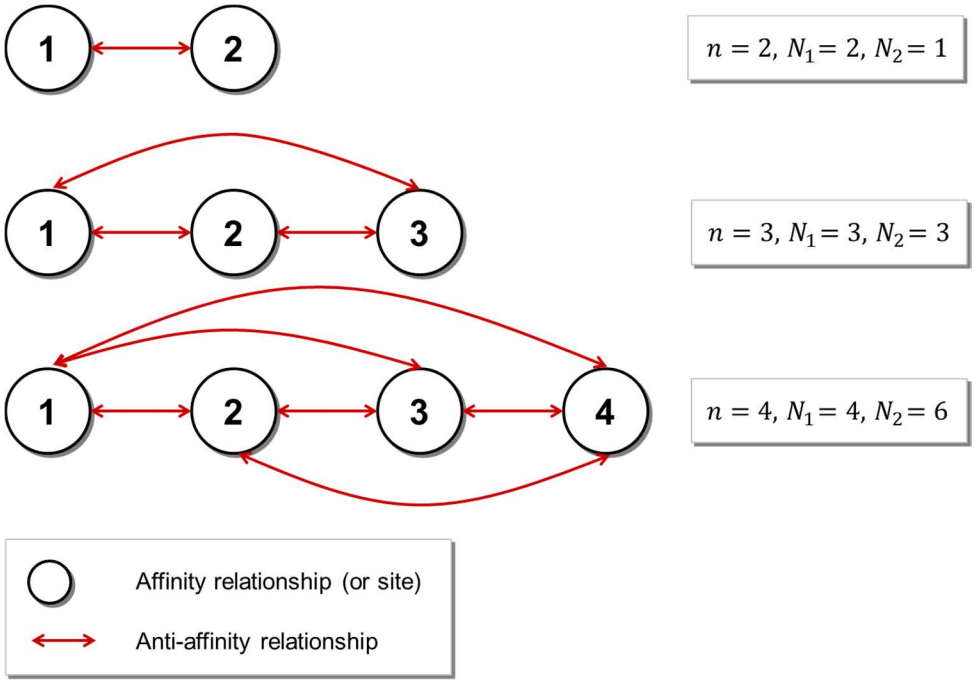

Figure 5.10.8-1: Usage of AffinityOrAntiAffinityGroup information element

Figure 5.10.8-1 depicts the number of required affinity and anti-affinity groups for small values of ***n***. It can be proved that the number of affinity and anti-affinity groups required to specify a multi-site NS deployment grows as the square of the number of sites. More precisely:

$$N = \frac{n^2+n}{2}.$$

Therefore, the semantic provided by the AffinityOrAntiAffinityGroup information element appears to be as exhaustive but not efficient.

Quoting again from ETSI GS NFV-IFA 014 [i.12], LocalAffinityOrAntiAffinityRule can be used to specify "affinity or anti-affinity rules applicable to VNFs […] instantiated from the same VNFD". As for AffinityOrAntiAffinityGroup, in order to specify a multi-site NS deployment, the scope attribute is supposed to be set to "NFVI-PoP" (a.k.a., site).

With respect to this information element, the drawback is due to the fact that ***M*** VNF instances created from the same descriptor can either be placed in a single site or in ***M*** sites, one instance for each. No intermediate placing method is allowed.

Therefore, the semantic provided by the LocalAffinityOrAntiAffinityRule information element appears to be as not exhaustive.

Finally, given that the definition of AffinityOrAntiAffinityGroup refers to "different VnfProfiles" while the definition of LocalAffinityOrAntiAffinityRule mentions "same VNFD", it is not clear which information element is to be used in order to specify affinity and anti-affinity rules between VNF instances created from the same descriptor, but using different profiles. Figure 5.10.8-2 depicts the potential clash between the two information elements. It is thus important to check the scope of definitions for the attribute and the attribute type in ETSI GS NFV-IFA 014 [i.12] if there is a conflict.

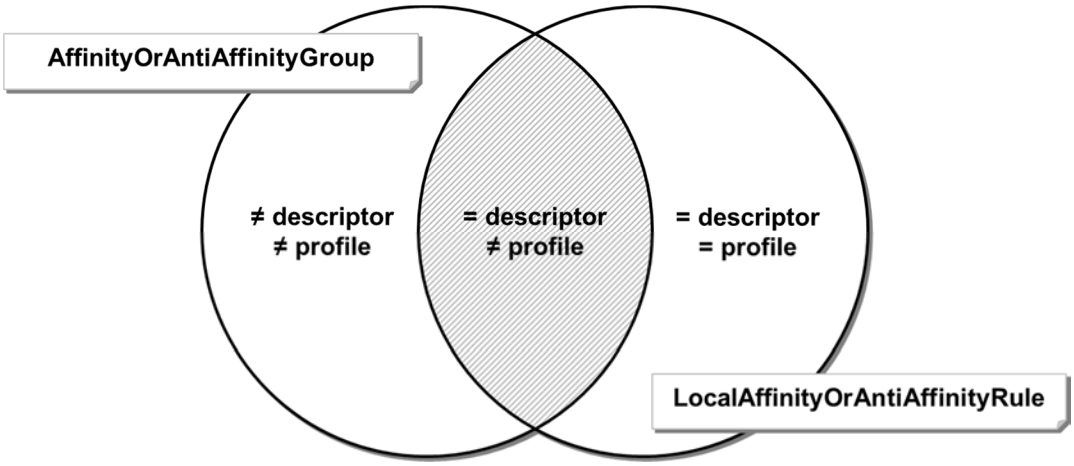

Figure 5.10.8-2: Overlapping scope of AffinityOrAntiAffinityGroup and LocalAffinityOrAntiAffinityRule information elements

In order to overcome the aforementioned limitations, it would be useful to:

1) introducing a new attribute reflecting the NFVI-PoP(s) on which the NS instance needs to be deployed; and

2) use such information to control how many VNF instances created from a given VnfProfile are to be placed in each of the specified NFVI-PoP, by extending the VnfToLevelMapping information element (see ETSI GS NFV-IFA 014 [i.12], clause 6.7.4).

Figure 5.10.8-3 summarizes the potential enhancements directed to ETSI GS NFV-IFA 014 [i.12].

An nfviPops attribute would list the NFVI-PoP(s) applicable to the NS instance, according to the present NS deployment flavour. Please note that the NFVI-PoP(s) are referred to via generic identifiers (e.g. integers): the mapping between those generic identifiers and the actual service provider's facilities is intended to take place at run-time (e.g. via placing policies or configuration). Once this kind of information is available, it can be leveraged to control how many VNF instances created from a given VnfProfile are to be placed in each of the specified NFVI-PoP(s). Quoting from ETSI GS NFV-IFA 014 [i.12], the "VnfToLevelMapping information element specifies the profile to be used for a VNF involved in a given NS level and the required number of instances".

NOTE: An NS level consists of a list of involved entities, i.e. VNFs, VLs and/or nested NSs. For each involved VNF/nested NS, the number of instances required by the NS level is specified. For each involved VL, the bitrate requirements corresponding to the NS level are specified.

A vnfInstancesToNfviPopMappings attribute would be a structure listing a series of InstanceToPoPMapping information elements, each of them specifying the subset of the VNF instances allowed by the present NS level correspond to the referenced NFVI-PoP. Please note that, in this case, a multi-site NS deployment across ***n*** sites require (at most) ***n*** InstanceToPoPMapping information elements for each VnfToLevelMapping. Therefore, the relationship is linear, not quadratic.

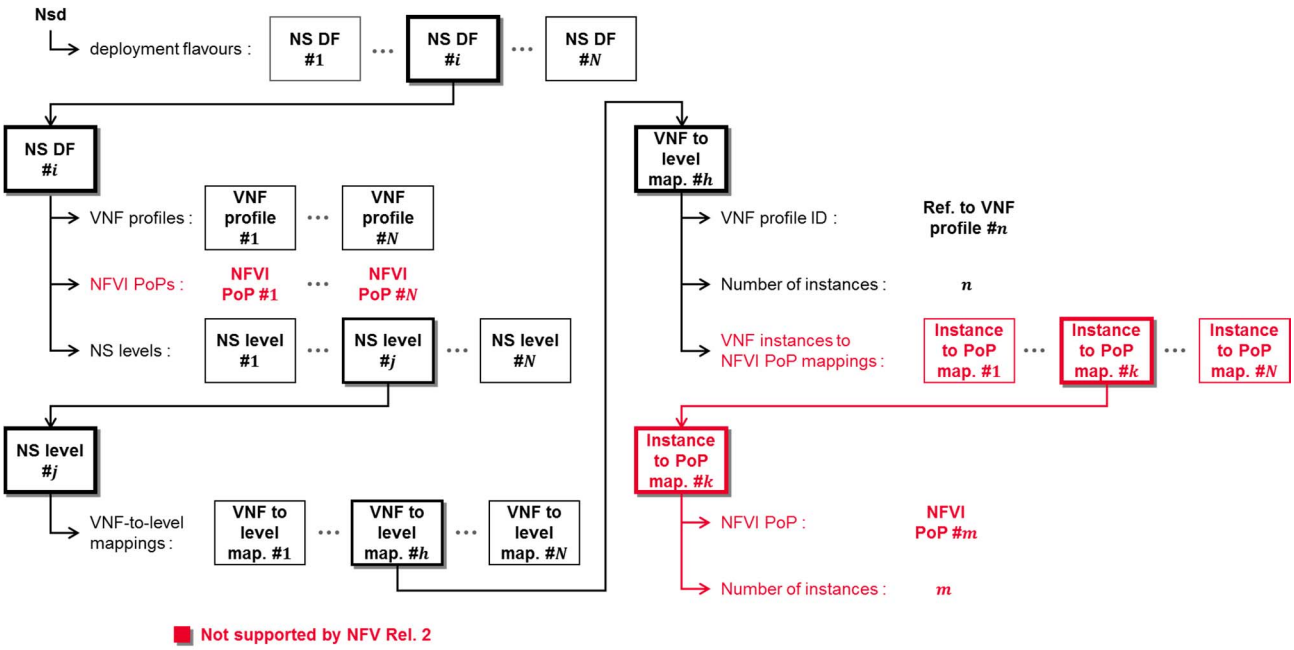

Figure 5.10.8-3: Potential enhancements directed to IFA 014 aimed at overcoming existing limitations

ETSI GS NFV-IFA 013 [i.11] currently specifies the information element VnfLocationConstraints (see clause 8.3.4.4 in ETSI GS NFV-IFA 013 [i.11]) used as a parameter in some NS LCM interface operations such as InstantiateNs (see clause 7.3.3 of the referred document) and ScaleNs (see clause 7.3.4 of the referred document). As the description of the information element states, the "VnfLocationConstraints information element defines the location constraints for the VNF to be instantiated". It has two attributes: vnfProfileId and locationConstraints, which remains "Not specified." in stage 2-level specification.

The locationConstraints provides a similar functionality as the one proposed in the present clause that extends the NSD specification. The locationConstraints refers to the vnfProfileId, so location constraints are linked to a specific VNF profile. If locationConstraints for different VNF deriving from the same VNFD are needed, then different VNF profiles would need to be defined in the NSD in order to cover any differences in terms of location constraints for the placement of the different VNF instances.

Finally, locationConstraints are related to runtime NS LCM operation, so the values of the parameters can be tuned to current known runtime information, whereas the enhancements on the NSD apply at design time. Therefore, the use of locationConstraints and the enhancements proposed in the present use case analysis should not be understood as being incompatible, but rather complementary.

5.11 Use Case 10: User Equipment (UE) Location Triggered Network Service Migration Across NFVI PoPs

5.11.1 Introduction

This use case covers the migration of a NS from one NFVI-PoP to another within the scope of same NFVO. The migration is triggered by a change in the location of the UE making use of the NS. The trigger is detected and subsequent migration of the NS is directed by the OSS/BSS functional block.

Figure 5.11.1-1 shows a multi-site NFV environment where the NS can be migrate from the VNFs in one NFVI-PoP to another NFVI-PoP based on different triggers (further elaborated in the next clause 5.11.2).

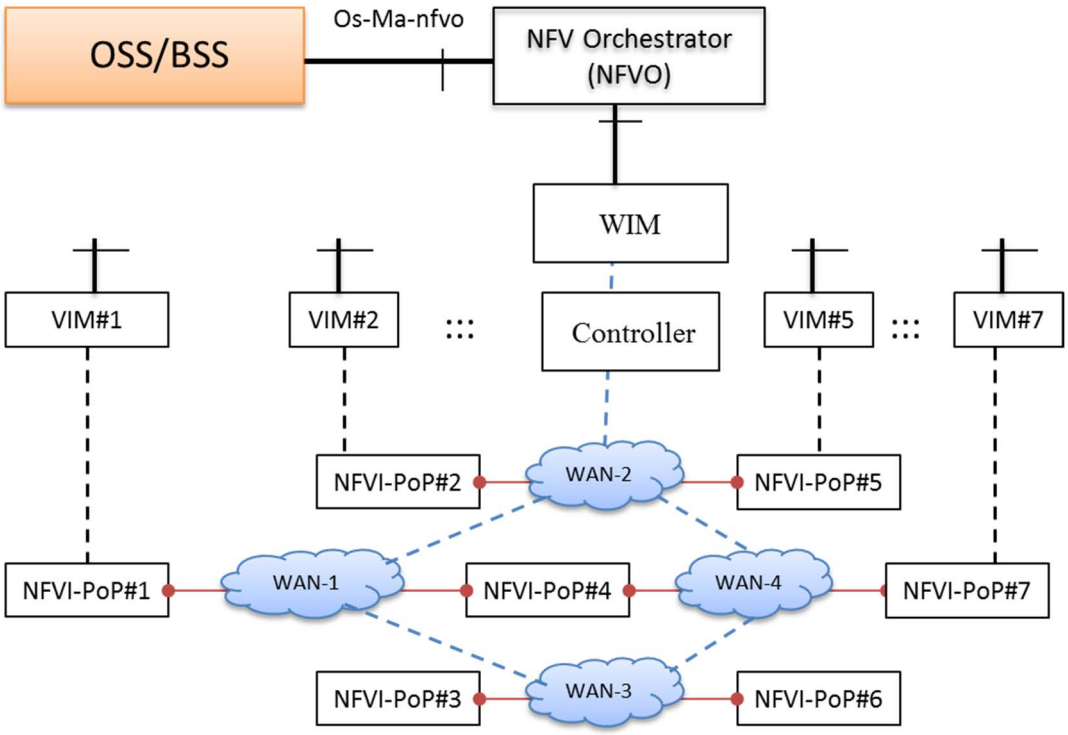

Figure 5.11.1-1: Multi-Site NFV System supporting NS Migration

This use case describes a NS in a multi-NFVI PoP scenario.

It is assumed that this NS utilizes one or more VNFs in one NFVI PoP, and as this NS moves from one NFVI PoP to another, some or all of the VNFs that are parts of this service need to be migrated to the destination NFVI PoP.

In addition to connectivity, other features and functions that are related to this service may need to be adjusted in the destination NFVI PoP.

NS migration may not migrate all of the components of the NS.

In this case, the NS at the destination NFVI PoP has VNFs that still need connectivity with the VNFs at the original NFVI PoP that were not migrated.

For the case in which all VNFs of the NS are migrated, there may be still a need for connectivity between the original NFVI PoP and target NFVI PoP during the migration process in order to migrate the content related to the VNFs of the NS from the origin NFVI PoP to the destination NFVI PoP. For example, if a virtual Content Delivery Network (vCDN) NS is migrated, the contents of the virtual Storage VNFs also needs to be moved (this requires connectivity between the NFVI PoPs).

5.11.2 Triggers

A change in the location of the user triggers a migration of the NS, the related VNFs, and the associated features and functions (capabilities). This requires that some or all of the constituent VNFs be migrated.

A change in the user's location can be determined automatically (e.g. by a 3GPP mobility management function, or via tracing of the UE or hand-held device using methods compliant to relevant 3GPP or IEEE standards) or the user may be required to register at a new location and specifically indicate a desire to have their NS migrated. Degradation of the service level agreement (SLA) in the original host may also trigger the detection. In any case, the location change is detected by the relevant network function which in turn, for the case when action on the allocated resources is needed, informs either OSS/BSS or the MANO functional blocks on the need to change. Table 5.11.2-1 describes these options.

Table 5.11.2-1: Network Service migration across NFVI PoPs: Triggers

Trigger	Options	Description
	Detection of end-user location change	Location is determined by the mobility management function or by tracing the end-user of the service (e.g. a hand-held device).
Request from OSS/BSS	Host-based tracking (end-user opts-in or does not care); SLA degradation may be the reason	Host determines new locations based on factors like loading and other conditions (proximity of services); NFVI-PoP is hosting the NS.
Request from OSS/BSS	End-user registration at new location	End-user is required to register at new location and indicate that service migration is desired.
Request from OSS/BSS	Schedule-based location change	A predetermined schedule for location change is set by the end-user. For the use case presented in this clause, it is assumed that the OSS/BSS FB maintains the NS migration schedule.

5.11.3 Actors and roles

If the target (destination) NFVI PoP for migration of the NS (and associated VNFs) network is already known, a direct pre-established connection may be utilized. Otherwise, connectivity between the original NFVI PoP and the destination (target) NFVI PoP needs to be established with the help of WIM. The Actors and their roles are as presented in Table 5.11.3-1.

Table 5.11.3-1: Network Service migration across NFVI PoPs: Actors and roles

#	Actor	Description
1	OSS/BSS FB	As defined in the ETSI/ISG NFV arch.
2	NFVO FB	As defined in the ETSI/ISG NFV arch.
3	WIM	As defined in the ETSI/ISG NFV arch.
4	Originating NFVI (Origin.NFVI) PoP	For the case where the NS migrates across NFVI PoPs, the Originating NFVI PoP is where the NS was instantiated and its associated virtualised resources and VNF(s) were being managed before the migration.
5	Destination NFVI (Dest.NFVI) PoP	For the case where the NS migrates across NFVI PoPs, the Destination NFVI PoP is where the NS will be instantiated and its associated virtualised resources and VNF(s) are managed after the migration.
6	Relevant mobility management or tracing function	For a LTE network, the mobility management functions as described in [i.28], [i.29] or the subscriber tracing function as specified in [i.28].

5.11.4 Pre-conditions

Table 5.11.4-1 describes the pre-conditions.

Table 5.11.4-1: Network Service migration across NFVI PoPs: Pre-conditions

#	Pre-condition	Description
1	Determination of a set of Target NFVI PoPs	Multiple NFVI PoPs may exist in the system for supporting the NS migration.
2	Selection of one Target NFVI PoP based on availability of capacity, capability to satisfy the service quality requirements, and migration option (cold, warm, or hot)	The most suitable NFVI PoP needs to be selected for the NS migration. For hot and warm migration of NS, the destination NFVI PoP has to be known a priori because of the state synchronization requirements. In order to ensure both service continuity and NS synchronization, connectivity between NFVI-PoPs is needed.
3	Selection or establishment of a connection between Origin and Target NFVI-PoPs	Section of a pre-established direct connection between Origin and Target NFVI-PoPs based on the required capacity, capability to satisfy the service quality requirements. If no pre-established direct connection is available, a connection between Origin and Target NFVI-PoPs is established with the help of WIM.

5.11.5 Post-conditions

Table 5.11.5-1 describes the post-conditions.

Table 5.11.5-1: Network Service migration across NFVI PoPs: Post-conditions

#	Post-condition	Description
1	The NS has successfully migrated to a new set of VNFs in a new location (NFVI PoP); this is supported via cold migration of NS	The NS is now supported by VNFs in another (destination) NFVI PoP. It is possible in some cases that only some of the VNFs need to be moved (the main criteria are meeting the SLA to the consumer).

5.11.6 Operational Flows

As mentioned before, both direct connection and WIM-based connection can be utilized for NS migration.

Further, scheduled migration can be offered as an advanced option, i.e. the user can schedule a migration to a specific location at a specific time in the future and for a given duration. The schedule could also be recurring.

In addition, the change of location may be detected by the host although the host may not migrate the NS unless and until the associated pre-established threshold for SLA violation is crossed.

Tables 5.11.6-1, 5.11.6-2 and 5.11.6-3 describe the flows to show migration of an NS from one NFVI PoP to another.

Table 5.11.6-1: Operational Flow - WIM-based connection establishment between origin and destination (target) NFVI-PoPs

#	Flow	Description
1	Relevant virtual network functions → OSS/BSS	The OSS/BSS is informed by the relevant virtual network about certain KPIs and can determine whether NS migration is needed.
2	OSS/BSS → NFVO Establishment of connectivity between origin and destination (target) NFVI-PoPs	The OSS/BSS requests for establishing connectivity - based on service quality requirements - between origin and destination (target) NFVI-PoPs for NS migration.
3	NFVO → WIM NFVO submits the request to WIM	The NFVO sends the request to WIM for establishing connectivity - based on service quality requirements - between origin and destination (target) NFVI-PoPs for NS migration.
4	WIM → NFVO WIM responds to NFVO after establishing the connectivity that can satisfy the service quality requirements	The WIM establishes (via the controller) connectivity with desired characteristics between origin and destination (target) NFVI-PoPs, and responds to NFVO with information and parameters of the connection.
5	NFVO → OSS/BSS The NFVO responds to the connectivity establishment request from the OSS/BSS	The NFVO responds with connectivity - between origin and destination (target) NFVI-PoPs - information and parameters.

Table 5.11.6-2: Operational Flow - NS migration via Scaling (NS at origin is left in place)

#	Flow	Description
1	Relevant virtual network functions → OSS/BSS	The OSS/BSS is informed by the relevant virtual network about certain KPIs and can determine whether NS migration is needed.
2	OSS/BSS → NFVO Instantiate NS at destination NFVI PoP	The OSS/BSS requests that the NFVO instantiate a NS at the destination NFVI.
3	NFVO → OSS/BSS The NFVO responds to the request from the OSS/BSS	The NFVO instantiates the requested NS. The situation at this point is shown in Figure 5.11.6-1.

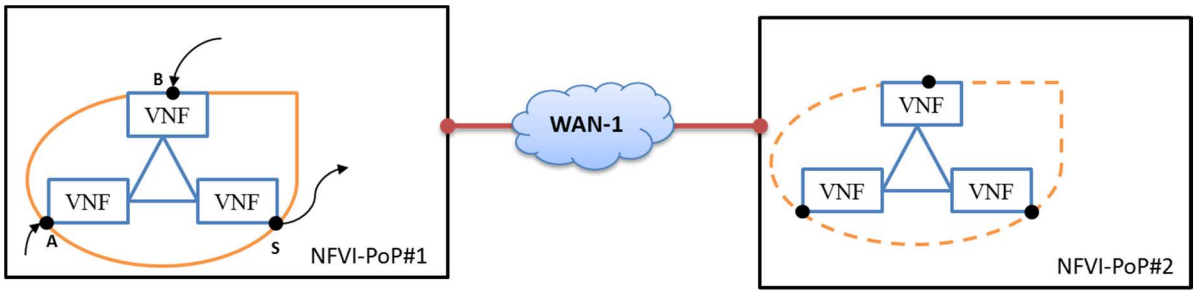

Figure 5.11.6-1: VNF-based Network Service Migration

Table 5.11.6-3: Operational Flow - NS migration where NS at origin is terminated

#	Flow	Description
1	Relevant virtual network functions → OSS/BSS	The OSS/BSS is informed by the relevant virtual network about certain KPIs and can determine whether NS migration is needed.
2	OSS/BSS → NFVO Instantiate NS at destination NFVI PoP	The OSS/BSS requests that the NFVO instantiate a NS at the destination NFVI.
3	NFVO → OSS/BSS The NFVO responds to the NS instantiation request from the OSS/BSS	The NFVO instantiates the requested NS.
4	OSS/BSS → NFVO Terminate NS at origin NFVI PoP	The OSS/BSS requests that the NFVO terminate the NS at the origin.
5	NFVO → OSS/BSS The NFVO responds to NS termination request from the OSS/BSS	The NFVO terminates the NS at the origin.

5.11.7 Other Considerations (e.g. Performance)

A change in location on the part of the consumer may not be sufficient to warrant migration of a NS. If the NS is still performing within the agreed SLA, then it may not be necessary to migrate the NS. Once the SLA is violated (due to a location change of the consumer), then the NS migration would be required.

The use of tracing functions incurs a significant overhead on the resource usage of the infrastructure and therefore is recommended only for small numbers of UEs. 3GPP networks handle user mobility events via the mobility management functions in order to provide the scale required for handling large numbers of such events in the network. Rather than acting on individual user mobility events, OSS/BSS may receive aggregate mobility events from virtual network functions and decide to act on such aggregate events, notifying MANO functions of the need for migrating NS components. Also, for the cases when fast migration is needed due to individual user mobility events, it is preferable to have a possibility for the virtual network function that detected the need for such migration to express it to the MANO functions.

5.11.8 Analysis

There needs to be a mechanism to determine the most-suitable - based on pre-specified criteria - target or destination NFVI-PoP (to support the NS) when the UE moves. Furthermore, it is possible that only some of the components of the NS need to migrate (this also needs to be part of the analysis and decision mechanism). It is assumed that the flows are visible for NFV/MANO. However, since the MANO is not fully aware of those states within the VNFs of the NS, and the VNFs may not be aware of the migration that MANO is arranging for (some of) those, therefore some signalling are needed to the VNFs.

The relevant NFV-MANO elements need to inform the OSS/BSS about the location where the NS is deployed.

The lifecycle of NS needs to be managed when the NS constituents are distributed among multiple NFVI PoPs.

This is common to many use cases discussed in the present document. Accordingly, a requirement is developed as mentioned in clause 6.1 along with a recommendation (Nfvo.Oam.001 in Table 7.3-1).

The connectivity between the source and destination NFVI PoPs needs to be managed seamlessly and reliably in order to maintain the service continuity as specified in the associated SLA.

The synchronization of states among the NS constituents may need to be managed when these are distributed among multiple NFVI PoPs.

The states of the NS constituents may need to be migrated across the NFVI-PoPs.

The resources across NFVI PoPs may need to be managed for operations and planning of NS migration across sites, if applicable. This is supported by the ETSI GS NFV-IFA 010 [i.6], clause 6.1.1.

5.12 Use case 11: Modification to the WAN Connectivity Resource of a Multi-site NS

5.12.1 Introduction

Based on use case #1 in clause 5.2, this clause shows a use case on modification to the WAN connectivity resource of a multi-site NS. As introduced in use case #1, the NS in this case is for an EvCPE, which is reused in the present use case description.

Within the context of such an NS (e.g. the NS for the EvCPE), the bandwidth requirement of the Virtual Link in between the VNFs may increase or decrease in accordance with, for example, the change of traffic volume of a connectivity service between Site#1 and Site#2. The WAN controller or WIM controls the bandwidth of the WAN connectivity to match the change of traffic volume between the two sites.

5.12.2 Trigger

Table 5.12.2-1 describes the use case trigger.

Table 5.12.2-1: Modification to the WAN connectivity resource

Trigger	Description
	The OSS requests the NFVO to increase the capacity of an existing NS (e.g. the NS for the EvCPE), because the workload on the current VNFs has become high.

5.12.3 Actors and roles

Table 5.12.3-1 describes the use case actors and roles.

Table 5.12.3-1: Modification to the WAN connectivity resource actors and roles

#	Actor	Description
1	OSS/BSS	
2	NFVO	
3	VIM	
4	Network Controller	
5	WIM	

5.12.4 Pre-conditions

Table 5.12.4-1 describes the pre-conditions.

Table 5.12.4-1: Modification to the WAN connectivity resource

#	Pre-condition	Description
1	An E2E EvCPE service is instantiated and works properly according to the SLA.	See base flow #1.1, base flow #1.2, or base flow #1.3 in clause 5.2.
2	The virtual network bandwidth of WAN is limited by the capacity requirement according to NS.	

5.12.5 Post-conditions

Table 5.12.5-1 describes the post-conditions.

Table 5.12.5-1: Modification to the WAN connectivity resource

#	Post-condition	Description
1	The capacity / bandwidth of the virtualised network resources at site#1, site#2 and WAN that consist of the NS have been increased.	An EvCPE service is instantiated and works properly according to the SLA.

5.12.6 Operational Flows

Table 5.12.6-1 describes the operational flow.

Table 5.12.6-1: Modification to the WAN connectivity resource operational flow

#	Flow	Description
1	OSS/BSS -> NFVO	Requests an update to increase the capacity of the Virtual Link of an existing NS between Site#1 and Site#2. *Interface - Os-Ma-nfvo*
2	NFVO ->WIM	Requests to update the network bandwidth of the virtualised resource#2 at the WAN. The NFVO sends the resource identifier which is obtained at step 7 of base flow #1.1, base flow #1.2, or base flow #1.3 in clause 5.2. *Interface - Or-Vi*
3	WIM -> Network Controller	Requests to update the network bandwidth of the virtualised resource#2.
4	Network Controller	Updates the network bandwidth of the virtualised resource#2. See note.
5	WIM -> NFVO	Returns the response to update the network bandwidth of the virtualised resource#2. *Interface - Or-Vi*
6	NFVO ->VIM at site#1	Requests to update the network bandwidth of the virtualised resource#1 at site#1. The NFVO sends the resource identifier which is obtained at step 10 of base flow #1.1, base flow #1.2, or base flow #1.3 in clause 5.2. See note. *Interface - Or-Vi*
7	VIM at site#1	Update the network bandwidth of the virtualised resource#1. See note.
8	VIM at site#1 -> NFVO	Returns the response to update the network bandwidth of the virtualised resource#1. See note. *Interface - Or-Vi*
9	NFVO ->VIM at site#2	Requests to update the network bandwidth of the virtualised resource#3 at site#2. The NFVO sends the resource identifier which is obtained at step 13 of base flow #1.1, base flow #1.2, or base flow #1.3 in clause 5.2. See note. *Interface - Or-Vi*
10	VIM at site#2	Update the network bandwidth of the virtualised resource#3. See note.

#	Flow	Description
11	VIM at site#2 -> NFVO	Returns the response to update the network bandwidth of the virtualised resource#3. See note. *Interface - Or-Vi*
12	NFVO -> OSS/BSS	Returns the result of the update for the NS. *Interface - Os-Ma-nfvo*
NOTE: The set of steps 6, 7, 8 and the set of steps 9, 10 and 11 can be executed sequentially or in parallel. That is, the procedure to update the network bandwidth at Site#1 can be executed in parallel to the procedure to update the network bandwidth at Site#2.		

5.12.7 Other Considerations (e.g. Performance)

The use case focuses on the modifications to perform on the virtualised network resources within the NFVI-PoP and on the WAN. However, to fulfill the whole use case, the bitrate supported by the virtual network interfaces realizing the the VNF instances connection points needs to be also considered.

5.12.8 Analysis

For the modification of the WAN connectivity resource of a multi-site NS, the NFV-MANO should be able to:

1) Support controlling the bitrate provided by the virtualised network resource.

   As shown in the steps #2 and #6, NFVO requests WIM and VIM to update the network bandwidth of the virtualised network resources in the WAN and within the site, respectively. In both cases for WAN and NFVI-PoP virtualised network resources, controlling the bitrate to any possible value in between a minimum and a maximum may not be possible, thus only a limited number of fixed bitrates (e.g. 100 Mbps, 1 Gbps and 10 Gpbs) may be supported.

   The UpdateNetwork operation provided by the Virtualised Network Resource Management interface in ETSI GS NFV-IFA 005 [i.7] is relevant to the present use case. The input parameter updateNetworkData of type VirtualNetworkData has the attribute "bandwidth" which enables specifying the minimum network bandwidth (in Mbps) for a virtualised network resource. Currently, the interface applies to resources managed by the VIM within an NFVI-PoP. Similar capabilities and specification are also applicable in the case of WAN virtualised network resources managed by a WIM.

5.13 Use Case 12: Network Service for virtual Radio Access Network (vRAN)

5.13.1 Introduction

This use case is discussed in the context of vRAN network service orchestration. For 5G, Radio Access Network (RAN) consists of Centralized Unit (CU) and Distributed Unit (DU), which are under discussion in 3GPP [i.27]. Based on the definition of interface between CU and DU in 3GPP, CU and DU may be provided by different vendors in the future. In the use case, CU and DU are deployed as a VNF and a PNF, respectively, which is an example of CU/DU deployment. As shown in Figure 5.13.1-1 the overall model focuses on NFVI-PoPs and N-PoPs located at two different sites connected over a shared WAN infrastructure (e.g. IP/MPLS, optical network, etc.).

NOTE: The connectivity between PNFs is not included in the use case.

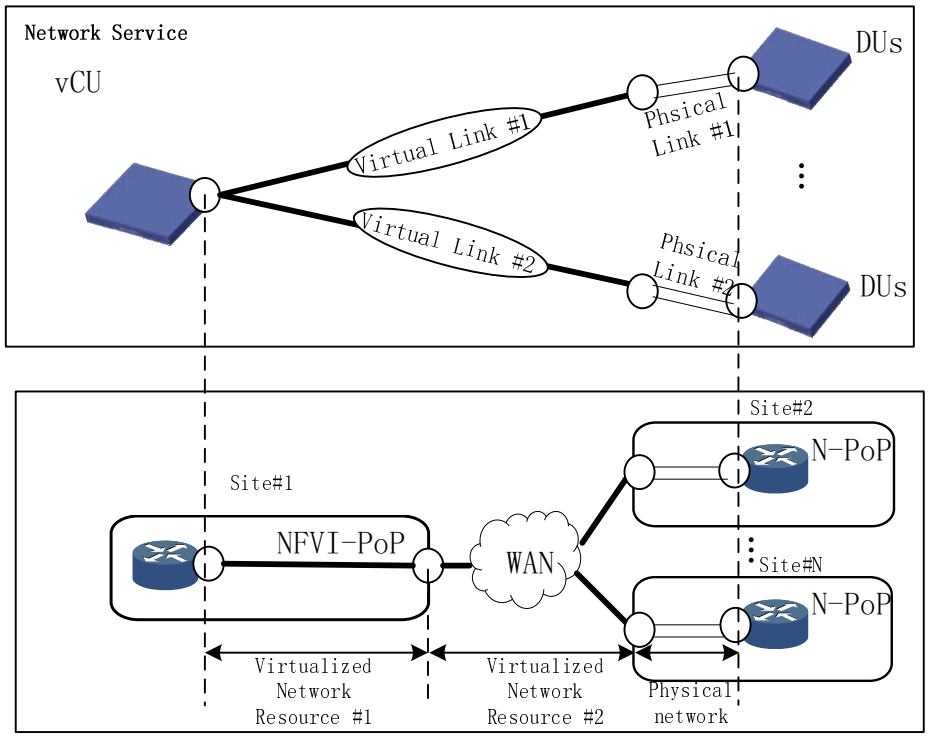

Figure 5.13.1-1: Connectivity overview for enabling Network Service

A network service consisting of VNF and PNF is instantiated as shown in Figure 5.13.1-1.VNF and PNF are virtualised CU (vCU) and DU respectively, which are installed in different sites. All the DUs are located in at least one site. Moreover, the VNFs and PNFs of the network service are connected across a WAN infrastructure.

The virtualised network resources for Site#1 and for the WAN are referred to as virtualised network resource#1 and #2, respectively. The virtualised network resources assigned to the vCU VNFs and DUs PNFs are terminated at virtual network ports which are attached to the WAN infrastructure. However, depending on the existing PNF connectivity, the virtualised network may have to end at a physical port. As a result, a unified Virtual Link is created by combining the virtualised network resource#1 and #2. The link in N-PoP may be physical link, which is transparent for the VIM and the WIM.

Base operational flows for deploying network services across two sites are examined. The vCU VNFs are deployed in Site#1 and the DU PNFs are deployed in Site#2. In some scenarios, the DU PNFs may be deployed in many sites. A network connectivity is configured among those sites. The network connectivity among those sites should be coordinated in such a way as to deliver a unified service. The PNFs at each site will be connected to the VNFs across the WAN.

Figure 5.13.1-2 provides a more detailed view of the use case. The figure also shows the related architectural components (e.g. WIM, Network Controller, NFVO, etc.) and reference points, which are further referred in the present use case.

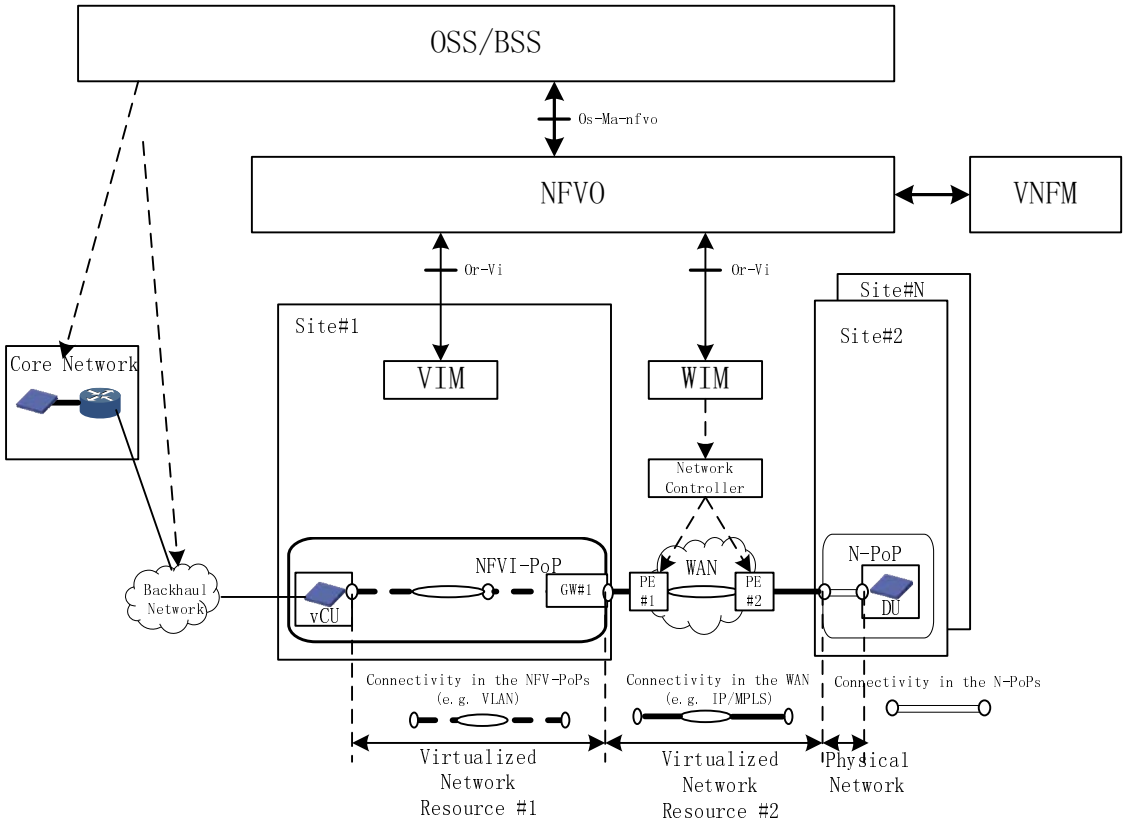

Figure 5.13.1-2: High-level view of the vRAN service across WAN

5.13.2 Trigger

Table 5.13.2-1 describes the use case trigger.

Table 5.13.2-1: Network Service for vRAN trigger base flow #1

Trigger	Description
BF#1.1 and BF#1.2	The OSS requests the NFVO to instantiate a Network Service with a VNF in Site#1. The VNF was connected with at least one PNF in Site#2 by a virtual link.

5.13.3 Actors and roles

Table 5.13.3-1 describes the use case actors and roles.

Table 5.13.3-1: Network Service for vRAN actors and roles

#	Actor	Description
1	OSS/BSS	
2	NFVO	
3	VIM	
4	Network Controller	
5	WIM	

5.13.4 Pre-conditions

Table 5.13.4-1 describes the pre-conditions.

Table 5.13.4-1: Network Service for vRAN Pre-conditions

#	Pre-condition	Description
1	Backhaul network between the core network site and Site#1 shown in Figure 5.2.1-2 works properly according to the SLA.	
2	The infrastructure of the NFVI-PoP at Site#1, N-PoP at Site#2 and the network infrastructure of the WAN are also physically connected. See note.	
3	The physical network connectivity in N-PoP at Site#2 has been established via OSS/BSS and EM. The physical network connectivity in N-PoP at Site#2 is managed by OSS and EM. See note.	
NOTE: There are several N-PoPs in Site#2, Site#3 and so on in some scenarios.		

5.13.5 Post-conditions

Table 5.13.5-1 describes the post-conditions for base flow #1 (i.e. BF#1.1 and BF#1.2).

Table 5.13.5-1: Network Service for vRAN post-conditions for base flow #1

#	Post-condition	Description
1	A vRAN service is instantiated with vCU (VNF) in Site#1 and DU (PNF) in Site#2, etc. The virtual link between the VNF and the PNF is supported across a WAN.	

5.13.6 Operational Flows

Table 5.13.6-1 describes the base flow #1.1 (BF#1.1) and the base flow #1.2 (BF#1.2) for the approach of translating/mapping in between in-site and WAN virtual networks (see clause 5.13.1).

The BF#1.1 shows the approach of translating/ mapping between in-site and in-WAN virtual networks based on information provided by WIMs. WIMs allocate Virtualised Network Resource#2 between NFVI-PoP at Site#1 and N-PoP at Site#2 with a designated maximum latency first. Then VIMs allocate Virtualised Network Resource#1 connecting to the WAN with the designated maximum latency according to the information provided by WIMs. The BF#1.2 shows the approach of translating/mapping between in-site and in-WAN virtual networks based on information provided by VIMs. The first 10 steps of BF#1.2 are similar to BF#1.1. The steps from 11 to 15 describe the interactions between the NFVO, the WIM and the Network Controller, which complete the re-configuration of the Virtualised Network Resource#2 at the WAN.

Table 5.13.6-1: Network Service for vRAN base flow #1.1

#	Flow	Description
1	OSS/BSS -> NFVO	Requests to instantiate a Network Service across Site#1 and Site#2. Generally OSS/BSS requests the instantiation with the location constraints for the NFVI. Optionally OSS/BSS can specify the site identifier where its constituent VNF should be allocated. OSS sends the relevant information of physical network in Site#2 to NFVO to enable "stitching" the connectivity in between the WAN and Site#2. *Interface - Os-Ma-nfvo*
2	NFVO	Starts an instantiation process for the vCU (VNF) with the VNFM. If OSS/BSS does not specify the site identifier where the VNF should be instantiated, then the NFVO decides the location where to instantiate the vCU according to the location constraints. According to the location constrain of VNF and the connectivity requirement between the VNF and PNF defined in NSD, the NFVO checks the capability (e.g. MPLS and QoS support) and capacity which are provided by the NFVI-PoP at site#1 and the WAN. The NFVO decides to setup network connectivity between two sites across the WAN.
3	NFVO ->WIM	Requests to allocate Virtualised Network Resource#2 between NFVI-PoP at Site#1 and N-PoP at Site#2 with a designated maximum latency. NFVO sends the relevant information of physical network in Site#2 to WIM to enable "stitching" the connectivity in between the WAN and Site#2. *Interface - Or-Vi*
4	WIM -> Network Controller	Requests to create network connectivity between PE#1 and PE#2 with the designated maximum latency between Site#1 and Site#2, taking into account the relevant information of physical network in Site#2.
5	Network Controller	Creates the network connectivity between PE#1 and PE#2 with the designated maximum latency. The IP/MPLS path configurations are PE#1, PE#2 and other provider routers in the WAN infrastructure.
6	Network Controller -> WIM	Returns the response to the network creation request. In this context, the information for connecting to the WAN (e.g. IP address, VXLAN ID, and MPLS-VPN RD) are returned.
7	WIM -> NFVO	Returns the response to the virtualised resource allocation request between NFVI-PoP at Site#1 and N-PoP at Site#2. In this context, the resource identifier, which is used for identifying the virtualised network resource at the WIM and the information for connecting to the WAN (e.g. IP address and VXLAN ID, and MPLS-VPN RD) are returned. *Interface - Or-Vi*
8	NFVO -> VIM at Site#1	Requests to allocate Virtualised Network Resource#1 connecting to the WAN with the designated maximum latency. The NFVO sends information for connecting to the network connectivity over the WAN which are obtained in step 7. *Interface - Or-Vi*
9	VIM at Site#1	Allocates Virtualised Network Resource #1for connecting to the WAN at Site#1 with the designated maximum latency.
10	VIM at Site#1 -> NFVO	Returns the response for allocating the virtualised resource for connecting to the WAN. The VIM returns resource identifier which is used for identifying virtualised resource at the VIM. *Interface - Or-Vi*
11	NFVO	Completes the instantiation process for the vCU and DU with the VNFM(s).
12	NFVO -> OSS/BSS	Returns the results of NS instantiation request.

Table 5.13.6-2: Network Service for vRAN base flow #1.2

#	Flow	Description
1-10		See note 1.
11	NFVO ->WIM	Requests to update the Virtualised Network Resource#2 at the WAN, according to the maximum latency requirement of the whole Virtual Link between vCU and DU PNF. The NFVO sends the information for connecting to the endpoints of the site#1 which is obtained in step 10. See note 2. *Interface - Or-Vi*
12	WIM -> Network Controller	Request to configure the PE#1 and PE#2 at WAN. *Interface - e.g. NBI for Network controllers*
13	Network Controller	Configures the PE#1 and PE#2 at WAN.
14	Network Controller -> WIM	Returns the response for configuring the PE#1 and PE#2 at WAN.
15	WIM -> NFVO	Returns the response for updating the Virtualised Network Resource#2.
16	NFVO	Completes the instantiation process for the vCU and DU with the VNFM(s).
17	NFVO -> OSS/BSS	Returns the results of NS instantiation request.
NOTE 1: The steps from 1 to 10 see the BF#1.1. NOTE 2: For the step 11, the designated maximum latency of virtualised resource#1 + the designated maximum latency of virtualise resource #2 + the maximum latency of physical link ≤ the maximum latency of the whole VL between vCU and DU PNF.		

5.13.7 Other Considerations (e.g. Performance)

In this use case, the vCU (VNF) connects with multiple DUs (PNF), which may be deployed in different N-PoPs. vRAN needs a performance guarantee for the maximum latency of the virtual links. For example, the performance requirements of the virtual link which connects vCU and DU should be specified in the NSD. As for maximum latency aspect, the sum of the individual maximum latency in Virtualised Network Resource #1, #2 and Physical network should be equal to or smaller than the latency requirement of the overall virtual link between vCU and DU. The bandwidth requirements for Virtualised Network Resource #1, #2 and Physical network should also be selected by NFVO, so that the performance requirements are guranteed by the NFV and WAN infrastructure.

5.13.8 Analysis

The goal of this use case is to instantiate vRAN service with vCU (VNF) in Site#1 and DU (PNF) in Site#2, etc. The virtual link #1 and #2 between the VNF and the PNF are supported across a WAN. NFVO should be able to decide how to allocate the virtualised network resources for Virtual Links. By comparing attributes and contents in the target NSD and the current status of the virtualised network resources managed by VIM at Site#1 and WIM, the NFVO requests for resource allocations to the VIM and the WIM. In the operational procedure, the operational policies may contain the rules based on following criteria:

- The NFVO can instantiate the VNF based on the location constraint indicated by OSS, which has been supported in IFA 013 (see clause 8.3.4.4 in ETSI GS NFV-IFA 013 [i.11]).
- The NFVO needs to have the capability to process the requirements for the virtual link (e.g. QoS, serviceAvailabilityLevel) as specified in the NSD according to the different parts that the NS VL can span (see clause 6.1.1 in ETSI GS NFV-IFA 010 [i.6])). For instance, in the vRAN use case, the VL requirements should be processed by the NFVO and the specific applicable requirements be derived for the different parts of the network encompassing the virtualised network resources #1 managed by VIM at Site#1, virtualised network resources #2 managed by WIM and physical network resource at Site #2. The accommodation of the NS VL requirement to the specific network parts may be supported by some policy.
- The WIM needs to be able to check the reachability between network gateways of the NFVI-PoPs/N-PoPs.
- The NFVO needs to send network allocation request to the WIM according to the above requirements of virtualised network resources of WAN (e.g. QoS, serviceAvailabilityLevel).
- The NFVO needs to update the information of an instantiated virtualised network resource managed by WIM. The interface function should be defined.

5.14 Use case 13: Use of WAN connectivity by compute-only NFVI-PoP deployments

5.14.1 Introduction

While transitioning from the current "network of physical functions" to a "network of VNFs", the supporting NFVI available at different NFVI-PoPs is connected to the existing WAN infrastructure equipment in order to ensure multi-site connectivity. During this period of transition the NFV-enabled network and the legacy network coexist. It becomes necessary to enable direct network connectivity of the VNFs in an NFVI-PoP with the physical WAN infrastructure equipment. A typical scenario may consist of VNFs (e.g. virtual Broadband Network Gateway (vBNG) and vSec-GW) in a highly distributed NFVI-PoPs (for example in Edge Cloud locations) to get connected directly to the WAN equipment in order to have access to some central NFVI-PoP (such as a Central Cloud location).

In this kind of setups, the deployment of a hardware switching fabric as part of the NFVI-PoP may not be necessary since it would provide no traffic aggregation towards the WAN equipment, which needs to be there anyway to allow for the multi-site scenarios and the backhauling of traffic towards a Central Cloud location. Moreover, in many cases for performance reasons, for these kind of deployments, the networking functions of the compute domain (e.g. SR-IOV, PCI-PT) are favoured over the networking functions of the hypervisor domain (e.g. vSwitch) and the virtual networks in this use case are accordingly provided by the NFVI following a virtual partitioning approach, instead of a Layer 2 overlay model, without the need for a gateway at the NFVI. On the other hand, the gateway [i.4] is assumed as a function to provide an encapsulation/de-encapsulation function between the overlay and the external network domain at the Ex-Nd interface. In another model [i.30], [i.31], the gateway can be implemented as a stand-alone device/ equipment or embedded in an external device/ equipment.

Therefore these computes at distributed locations need to be connected directly to the WAN infrastructure equipment. As such, the network services on-boarding these minimal compute-only NFVI-PoPs would rely heavily on the use of WIM connectivity services, since practically all of their connectivity would be towards the outside of the NFVI-PoP.

The compute-only NFVI-PoPs would provide a Layer 2 service to the on-boarded VNFs up to the WAN equipment in the form of a virtualised network resource. The WAN infrastructure would provide typically either a Layer 2 VPN service or a Layer 3 VPN service with a remote NFVI-PoP across the WAN. However, other type of WAN services can be envisioned to be potentially automated by a Network Controller in the WAN infrastructure. An example would be a "Carriers' Carrier" service, according to [i.14].

This use case thus discusses in the general context of orchestrating a NS consisting of two VNFs in different NFVI-PoPs as shown in Figure 5.14.1-1. Each VNF in the respective NFVI-PoP, making use of virtual partitioning in the connection to the WAN equipment, is connected by WAN infrastructure that provides Layer 2 or Layer 3 VPN services, whereby the VNFs are directly connected to the external WAN infrastructure equipment.

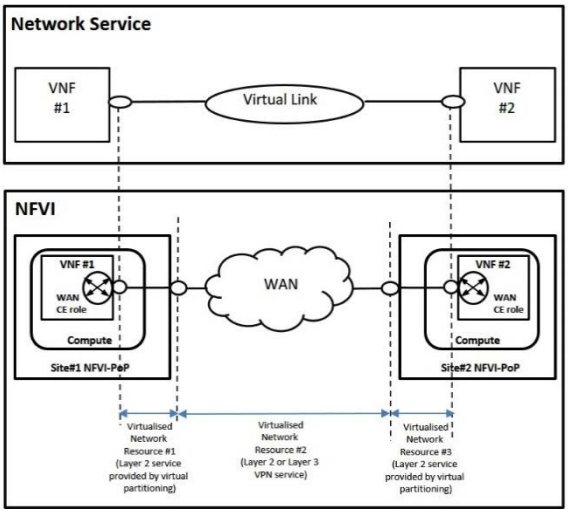

Figure 5.14.1-1: Connectivity overview of Network Service in compute-only NFVI-PoPs

The virtualised network resources connecting VNF#1 and VNF#2 with the WAN infrastructure equipment are referred as Virtualised Network Resource #1 and Virtualised Network Resource #3, respectively. These virtualised network resources provide a Layer 2 service. The virtualised network resource implemented across the WAN infrastructure is referred as Virtualised Network Resource #2. This virtualised network resource provides either a Layer 2 VPN service or Layer 3 VPN service. As a result, the unified Virtual Link is created by combining the virtualised network resource#1, #2 and #3 and it provides an end-to-end Layer 2 VPN or Layer 3 VPN service depending on the nature of the WAN virtualised network resource #2.

For the WAN infrastructure, the VNFs in this use case play the role of a CE equipment consuming the end-to-end service provided by the Virtual Link.

Figure 5.14.1-2 provides an architectural view of the use case showing the related architectural components (e.g. WIM, Network Controller, NFVO, etc.) and reference points, which are further referred to in the present use case.

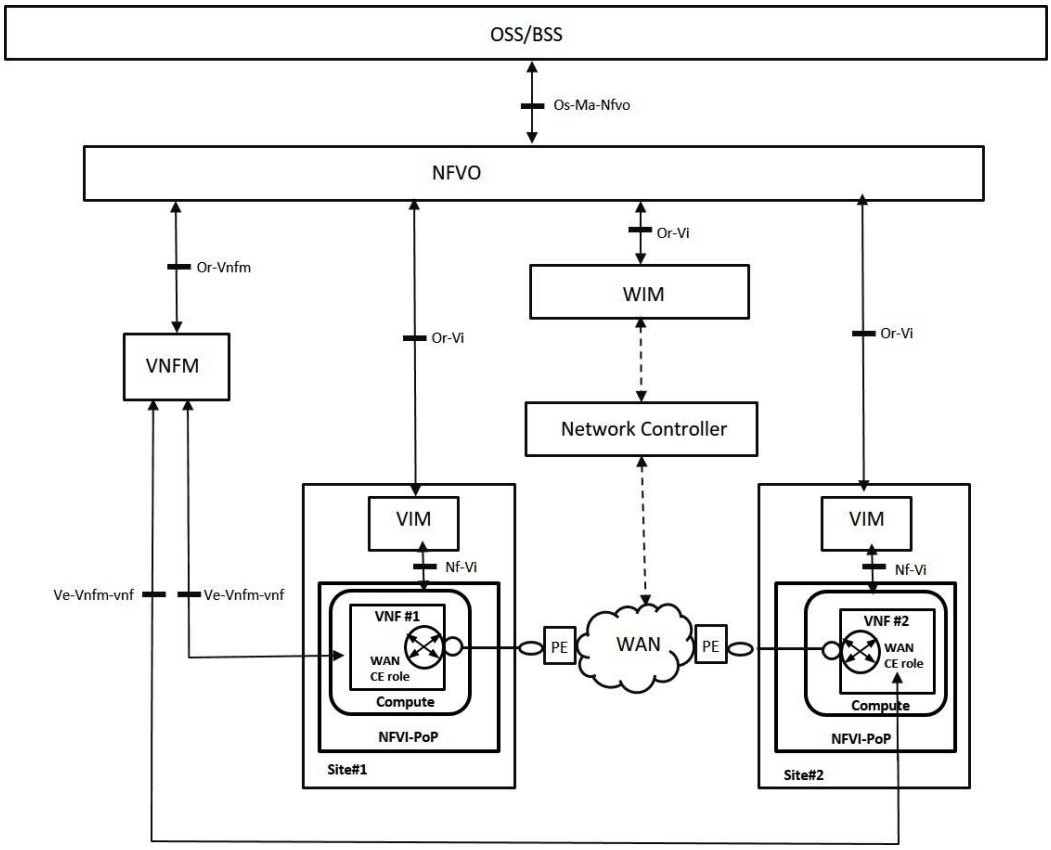

Figure 5.14.1-2: High level use case of WAN connectivity in compute-only NFVI-PoPs

Supported network connectivity services of WIM and NC could be in L2 or L3 and whether any underlay or overlay is used is beyond the scope of discussion.

5.14.2 Trigger

Table 5.14.2-1 describes the use case trigger.

Table 5.14.2-1: Use of WAN connectivity by compute-only NFVI-PoP deployments trigger

Trigger	Description
Request from OSS/BSS to NFVO	As shown in Figure 5.14.1-1, the OSS requests the NFVO to instantiate a NS with VNF#1 in Site#1 and VNF#2 in Site#2, with these VNFs connected by Virtual Link.

5.14.3 Actors and roles

Table 5.14.3-1 describes the actor and roles.

Table 5.14.3-1: Use of WAN connectivity by compute-only NFVI-PoP deployments actors and roles

#	Actor	Description
1	OSS/BSS	
2	NFVO	
3	VIM	
4	VNFM	
5	WIM	
6	Network Controller	

5.14.4 Pre-conditions

Table 5.14.4-1 describes the actor and roles.

Table 5.14.4-1: Use of WAN connectivity by compute-only NFVI-PoP deployments pre-conditions

#	Pre-condition	Description
1	Compute-only NFVI-PoPs	Both Site #1 and Site #2 consist of one compute node connected directly to a WAN equipment of the WAN network connecting the two sites.
2	NFVI Network Resources Virtual Partitioning	VNF#1 and VNF#2 deployed in Site #1 and Site #2 make use of Layer 2 Virtual Partitioning of the NFVI-PoP network resources to reach the Ex-Nd interface, hosted at the WAN equipment.
3	WAN VPN service	The WAN network is capable of providing either Layer 3 or Layer 2 VPN connectivity services.
4	WAN CE role in VNF	The VNF#1 and VNF#2 are capable of playing the Customer Edge (CE) role.

5.14.5 Post-conditions

Table 5.14.5-1 describes the actor and roles.

Table 5.14.5-1: Use of WAN connectivity by compute-only NFVI-PoP deployments post-conditions

#	Post-condition	Description
1	NFVI Network Resources Virtual Partitioning	NFVI Network resources at Site # 1 and Site #2 are partitioned accordingly to the Layer 2 information corresponding to the WAN VPN service (e.g. VLAN info, physical port info)
2	WAN VPN service	The VPN service connecting the NFVI-PoPs on behalf of the NS connecting VNF#1 and VNF#2 is configured in the required WAN PE equipment
3	WAN CE role in VNF	The CE configuration parameters corresponding to the WAN VPN service connecting VNF#1 and VNF#2 are configured in VNF #1 and VNF #2 (e.g. IP address to use in the interaction with the WAN equipment, AS numbers to use, etc.)
4	VNF connectivity	VNF #1 and VNF #2 in Site #1 and Site #2 respectively can exchange data across the NS established

5.14.6 Operational Flows

Table 5.14.6-1 describes the operational flow.

Table 5.14.6-1: Use of WAN connectivity by compute-only NFVI-PoP deployments operational flow

#	Flow	Description
1	OSS/BSS -> NFVO	OSS/BSS requests NFVO to instantiate a NS across Site #1 and Site #2. Optionally OSS/BSS can specify the site where its constituent VNFs should be allocated as local constraints. OSS/BSS specifies that the constituent VNFs play the CE role in the WAN VPN service. *Interface - Os-Ma-nfvo*
2	NFVO	Starts an instantiation process for VNF #1 and VNF #2 with the VNFM(s). The NFVO checks the capability (e.g. type of virtual partitioning support in the NFVI-PoPs, type of VPN support in the WAN) and the capacity which are provided by the NFVI-PoP at site#1, the NFVI-PoP at site#2 and the WAN. The NFVO determines that the NFVI-PoPs at Site #1 and Site #2 are compute-only PoPs and that Virtual Partitioning is to be used across the NFVI-PoPs to connect the VNFs to the WAN equipment, that will host the Ex-Nd interface. The NFVO determines the kind of VPN service required across the WAN based on the kind of NS requested by the OSS/BSS. If a Layer 2 NS is requested, the WAN VPN service is determined to be a WAN Layer 2 VPN service (e.g. EVPN service). If a Layer 3 NS is requested, the WAN VPN service may be either a Layer 2 VPN service or a Layer 3 VPN service (e.g. MPLS IP VPN service), if the WAN supports both types of VPN. In this latter case, the kind of VPN service can be left for local NFVO policy to determine, or either a preference regarding the type of WAN service can be expressed through the Os-Ma-nfvo interface
3	NFVO, WIM and Network Controller	Virtualised Network Resource #2 is created accordingly to steps 3 to 7 of Table 5.2.6-1. As a result of this step, and as part of the response, the NFVO receives the Layer 2 (e.g. VLAN and/or port to be used) and Layer 3 information (e.g. IP address/AS number) to be used to connect the constituent VNFs to the WAN equipment at Site #1 and at Site #2.
4	NFVO -> VIM at Site#1	Virtualised Network Resource #1 is created accordingly to steps 8 to 10 of Table 5.2.6-1. Since Virtual Partitioning is used to connect the VNFs to the WAN equipment in Site #1, only Layer 2 information obtained in Step 3 is required by the VIM to create Virtualised Network Resource #1. *Interface - Or-Vi*
5	NFVO -> VIM at Site#2	Virtualised Network Resource #3 is created accordingly to steps 11 to 13 of Table 5.2.6-1. Since Virtual Partitioning is used to connect the VNFs to the WAN equipment in Site #2, only Layer 2 information obtained in Step 3 is required by the VIM to create Virtualised Network Resource #1. *Interface - Or-Vi*
6	NFVO -> VNFM	Completes the instantiation process for VNF #1 and VNF #2 with the VNFM(s). This instantiation process includes the configuration of the required Layer 2 and Layer 3 parameters obtained in Step 3 from the WAN network to configure the WAN CE role inside VNF #1 and VNF #2. *Interface - Or-Vnfm*
7	NFVO -> OSS/BSS	Returns the results of the NS instantiation request.
NOTE: Steps 4 and 5 can be executed sequentially or in parallel. That is, the procedure to establish connectivity at Site#1 can be executed in parallel to the procedure to establish connectivity at Site#2.		

5.14.7 Other Considerations (e.g. Performance)

No other considerations are derived from the present use case.

5.14.8 Analysis

In an overlay model, there is usually a network gateway element which terminates tunnelling end-points in the NFVI-PoP. This network gateway element is interfaced with the internal network through Nd-Nd reference point, and it is also attached to the external network over the Ex-Nd reference point. The network gateway is recognized as a network connectivity endpoint and characterized by the NfviPoP IE [i.7]. This has been a base assumption in all the other use cases this far.

However, in this use case a different option for the network connectivity endpoint is considered, where a compute node hosting VNFs in an NFVI-PoP is directly connected to an external network. This is illustrated in Figure 5.14.8-1, where a VNF#1 is instantiated on Compute Node#1 which in turn is directly interfaced to the external network hosting PE#1. In this case, the Compute Node #1 serves as the network connectivity end-point, whereas the connectivity of VNF#1 is over the respective VNF's Connection Point (CP). Since PE#1 is a network node that is outside the NFVI-PoP, therefore the connectivity between Compute Node#1 and PE#1 is established over the Ex-Nd reference point. As highlighted above, since there is no formal network gateway, therefore this option of "no gateway" should be recognized and expressed within the information model. The same consideration is applicable to the attachment between Compute Node#2 and PE#2. In this use case it is assumed that lower level connectivity (e.g. at the L2 level) between the compute node in the NFVI-PoP and the external network already exists and visible to the NFVO.

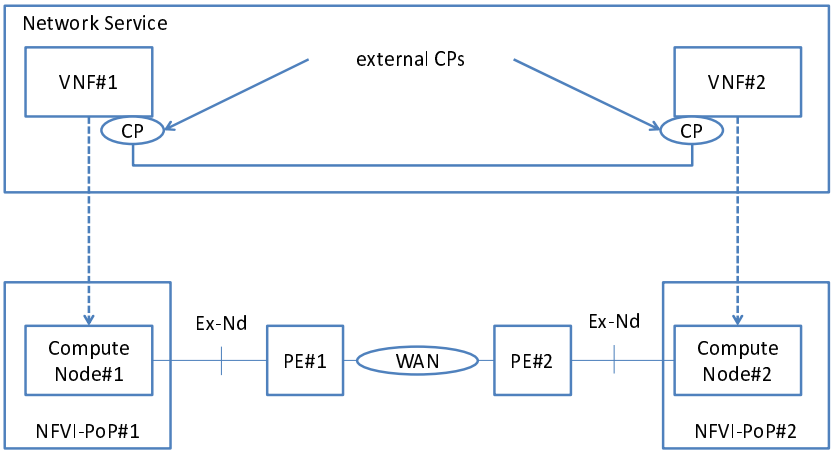

Figure 5.14.8-1: Direct attachment case between Compute Node and WAN PE

This issue should be considered an extension to the study about `networkConnectivityEnponit` attribute of `NfviPoP` IE in the use case#1.

Regarding the use of Virtual Partitioning in Compute Node#1 and Compute Node#2, an extra configuration can be used. The configuration information related to specific virtual network interface type (e.g. SR-IOV) can be specified in the `typeConfiguration` attribute of the `VirtualNetworkInterface` IE. However, the content of `typeConfiguration` is undefined and requires relevant descriptions or examples.

Moreover, in `VirtualNetworkInterface` IE [i.7], `typeVirtualNic` attribute is used to describe the type of network interface. The type allows for defining how such interface is to be realized, e.g. normal virtual NIC, with direct PCI passthrough, etc.. However, the content of `typeVirtualNic` is undefined and requires relevant descriptions or examples. It is suggested to expand on this description with some examples. For example, in the context of SR-IOV, "direct pci passthrough without macvtap" can be included to expand upon the example. This new example should be added in `typeVirtualNic` attribute in `VirtualNetworkInterface` IE and `VirtualNetworkInterfaceData` IE.

It is also noted that the terminology of "Nic" should be described as "Network Interface Controller" to harmonize it with the official terminology specified in [i.2].

6 Analysis

6.1 Use Case analysis with a focus on the NFV-MANO functions

The following clauses provide a summary of gaps identified in the use cases. Some of the use cases with a focus on NFV-MANO bring forth the following aspects that should be considered by NFV-MANO system:

- NS Lifecycle Management aspects: It is concerned with the lifecycle management of NS across multiple NFVI-PoPs. To this effect, there needs to be means for:
  - Support for the instantiation of a NS across multiple NFVI-PoPs over WAN infrastructure. See use case in clauses 5.2 and 5.3.
  - Support for modifying WAN connectivity among NFVI-PoPs. See use case in clause 5.12.
  - UE Location-triggered NS Migration support among NFVI-PoPs. See use case in clause 5.11.
  - NS Expansion support to other NFVI-PoP. See use case in clause 5.4.
  - NS Virtual Link healing support among NFVI-PoPs over WAN. See use case in clause 5.8.
  - Updating existing NS Virtual Links within an NFVI-PoP to expand across the WAN. See use case in clause 5.4.
  - NS Virtual Link redundancy support among NFVI-PoP over WAN. See use case in clause 5.7.
- VNF Lifecycle Management aspects: it is concerned with the lifecycle management of VNF across multiple NFVI-PoPs. To this effect, there needs to be means for:
  - Multi-site VNF deployment support. See use case in clauses 5.9 and 5.10.
- Virtualised network resources management aspects: It is concerned with the management of virtualised network resources within and among multiple NFVI-PoPs. To this effect, there needs to be means for:
  - Provisioning of virtualised network resources to be deployed in WAN infrastructures which have different network characteristics. See use case in clause 5.3.
  - Combining of the virtualised network resources among multiple NFVI-PoPs and WAN. See use case in clause 5.2.
  - The overlay and inter-AS connection support among NFVI-PoPs. See use case in clause 5.2.
  - Aggregation support of multiple VLs through WAN among NFVI-PoPs. See use case in clause 5.5.
  - QoS support for virtualised network resource among multiple NFVI-PoPs and WAN. See use case in clause 5.6.
  - Handling of alarms for virtualised network resources over WAN. See use case in clause 5.8.
  - Acquiring connectivity information, including connectivity type, capability, and capacity check for virtualised network resources among NFVI-PoPs and WAN. See use cases in clause 5.6 and clause 5.8.
  - Updating existing virtualised network resources within an NFVI-PoP to reconnect existing virtualised network resources among different virtualised network resources on the WAN. See use case in clause 5.8.
  - Allocating new and updating existing virtualised network resources within an NFVI-PoP to connect to the WAN. See use case in clause 5.4.
  - Support of affinity/anti-affinity constraints for virtualised network resources among NFVI-PoPs and WAN. See use case in clause 5.7.

- Informing/notifying to relevant management entities (e.g. the VNFM) about connectivity alarms resulting from NS Virtual Link failures that have an impact on the connectivity of the VNF as a constituent of the NS. See use case in clause 5.7.
- Connecting/disconnecting a specific external CP of the VNF. See use case in clause 5.7.
- Support of affinity/anti-affinity constraints for virtualised network resources used by a single VNF among NFVI-PoPs and WAN. See use case in clause 5.9.
- Maintain and provide the information to the relevant management entities about externally-managed internal Virtual Links with corresponding virtualised network resources realizing such VLs used for multi-site VNF deployment. See use case in clause 5.9.

- Architectural aspects: It is concerned with connectivity among multiple NFVI-PoPs. To realize this, there needs to be means for:
  - Exchanging parameters among VIMs. See use case in clause 5.2.
  - Information model and Interfaces for WIM. See use case in clauses 5.2 and 5.3.
  - Information model of NFVI-PoP connectivity. See use case in clause 5.2.

6.2 Analysis about WIM role

6.2.1 Existing concept of WIM and Network Controller

In [i.5] a WAN Infrastructure Manager (WIM) component and a network controller were introduced with a very high level definition that has already been summarized in clause 4.1. In case of WIM, it is considered as a particular example of a specialized VIM. WIM manages network resources across multiple NFVI-POPs, usually within one operator's Infrastructure Domain. WIM is typically used to establish connectivity between different NFVI-PoPs, or between a PNF that are externally located at the operator's Infrastructure Domain and a NFVI-PoP. In contrast to WIM, a VIM manages network resource as well as NFVI compute and storage resources within the domain of a single -NFVI-PoP.

With regards to the Network Controller, it is described as follows in clause 5.6.2 in [i.5]:

"Network Controllers may form a hierarchy in a client/server relationship where each "server" Network Controller exposes an interface to request connectivity services, i.e. virtual networks, to its clients. At the lowest layer, Network Controllers have visibility into the devices they control directly. At the highest layer, Network Controllers provide connectivity services to an application and provide abstraction of the underlying resources. Each layer in the hierarchy provides a different level of abstraction and may establish connectivity services by configuring the forwarding tables of the Network Functions within its domain directly or by requesting connectivity from "server" Network Controllers or a combination of both".

From NFVO perspective, different levels of abstraction from different layers and interfaces with network controllers for multiple domains may cause complex interactions. WIM, therefore, is considered as a component to hide the diversity. So WIM supports a variety of southbound interfaces towards the Network Controllers in order to fulfil WAN resource requirements, but the implementation of WAN and its southbound interface(s) is out of scope of the present document. However, in the context of the present document, the northbound interface(s) exposed by WIMs towards the NFVO are in-scope of the present document.

During the analysis of the use cases in clause 5 some gaps have been found between WIM and VIM, which will be highlighted in order to derive the requirements that will help define the necessary north-bound interface(s).

6.2.2 Analysis about connectivity service decomposition

As discussed in the use cases, VNFs are connected by (external) Virtual Links across the WAN infrastructure. The connectivity service which instantiates the Virtual Link is specified by `connectivityType` parameter in the `NsVirtualLinkDesc` information element. The parameter `layerProtocol` identifies the protocol that the VL supports (Ethernet, MPLS, ODU2, IPV4, IPV6, Pseudo-Wire, etc.), and the parameter. `flowPattern` identifies the flow pattern of the connectivity (Line, Tree, Mesh, etc.). A Virtual Private LAN Service (VPLS) [i.17] is one possible example of a connectivity which can be used to create an emulated LAN segment between NFVI-PoPs.

The connectivity fulfilled by a Virtual Link between VNFs across NFVI-PoPs can be decomposed into segments of connectivity realized within the NFVI-PoPs and segments of connectivity in the WAN as shown in Figure 6.2.2-1. As depicted in Figure 6.2.2-1 the decomposed segments map to specific nodes (e.g. network gateway, WAN node) inside NFVI-PoP and WAN. Relevant methods need to be implemented in order to allocate network resources within the NFVI-PoPs and WAN infrastructures.

The interconnection point between NFVI-PoPs and WAN infrastructure can be defined by `networkConnectivityEndpoint` in `NfviPop` information element. The attribute is intended to show information about network connectivity endpoints to the NFVI-PoP that the VIM manages. However, the content of this attribute is pending and hence the detailed information for the internal and external ports should be specified. As defined in [i.7], the VIM, which manages the NFVI-PoP, needs to fulfil the relevant information with respect to the network gateway and its external ports in order to instantiate the NFVI-PoP connectivity.

On the other hand, WIM should be responsible for the fulfilment of the network resources inside the WAN infrastructure, as well as the fulfilment of the external ports which linked with network nodes in NFVI-PoPs.

Further interactions between VIM and WIM will be necessary to transparently connect network gateways and WAN nodes through their external ports. It is considered that NFVO brokers the interactions.

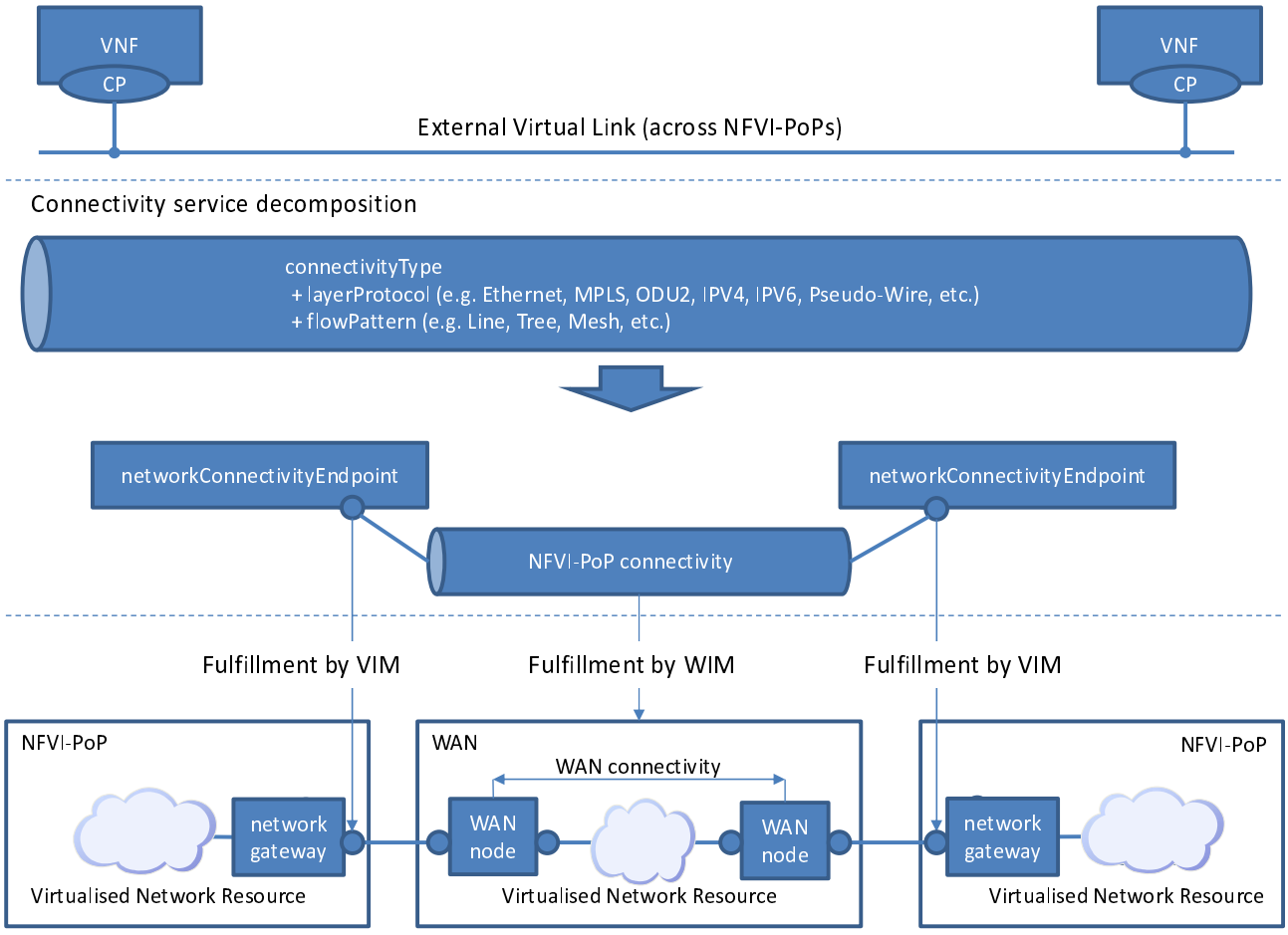

Figure 6.2.2-1: Mapping and decomposition of connectivity service

6.2.3 Analysis about WIM role in multi-site connectivity

A non-exhaustive set of functions performed by WIM in the context of providing multi-site connectivity is provided below:

- Virtualised Network Resources Management for WAN resources (e.g. allocate, query, update, terminate). WIM can rely on the Network Controller for the fulfilment procedures.
- Virtualised Network Resources Reservation Management for WAN resources (e.g. create, query, update, terminate). WIM can rely on the Network Controller for the fulfilment procedures.

- Virtualised Network Resources Capacity Management for WAN resources (e.g. subscribe, notify, query).
- Virtualised Network Resources Information Management for WAN resources (e.g. subscribe, notify, query).
- Virtualised Resources Performance Management for WAN resources (e.g. subscribe, notify, get for performance information).
- Virtualised Resources Fault Management for WAN resources (e.g. query, subscribe, notify for fault information).

The above listed functionalities may be exposed by means of interfaces defined in [i.7] and consumed by other NFV-MANO functional blocks.

6.3 Potential architecture options

6.3.1 Introduction

This clause provides the potential architecture options for the placement of WIM functional entity within the MANO architecture for supporting multi-site network services. This clause also describes the enhancements to MANO descriptors, reference points, and function blocks for each option:

- Architecture option #A: WIM integration as specialized VIM:
  - The VIM is defined as function block that is responsible for controlling and managing the NFVI compute, storage and network resources, usually within one operator's Infrastructure domain (e.g. NFVI-PoP) [i.2]. On the other hand, the WIM is introduced as a specialized VIM [i.5]. In this option, the WIM exposes the interfaces with Network Controllers of WAN infrastructure and is responsible for controlling and managing network connectivity of WAN between endpoints in different NFVI-PoPs.
- Architecture option #B: WIM integration into OSS/BSS:
  - As discussed [i.5], it is not expected that the first NFV deployments will use Network Controllers with programmatic/open interfaces for all network segments. This option, therefore, considers a model where the WIM functionality is in the OSS/BSS (EMS/NMS). As described in [i.5], this model may be the case when the resources are not reconfigured regularly, e.g. for static provisioning, or when they are pre-provisioned, or when a Network Controller with programmatic interfaces is not available for these resources. Or NFVO may be allowed to trigger resources of WAN via OSS. The WIM functionality is out of scope of MANO but the enhancement of Os-Ma-nfvo reference point needs to be considered.

Several use cases refer to "reference point Or-Vi" when highlighting the interaction between the NFVO and WIM. When the use cases have been introduced, references have been taken to ETSI GS NFV-MAN 001 [i.5], clause 5.6.2, which names the reference point in between the NFVO and the WIM also as Or-Vi. As introduced in clause 6.3.2, the reference points enabling interactions in between the NFVO and the WIM is proposed to be named "Or-Wi", and be based on a subset of Or-Vi to manage WAN connectivity.

6.3.2 Architecture option #A: WIM integration as specialized VIM

In this option, Or-Wi reference point between NFVO and WIM as subset of Or-Vi is specified to manage WAN connectivity as shown in Figure 6.3.2-1. The WIM function block is responsible for the management of virtualised network resources of WAN for NFV services that extends across multiple NFVI-PoPs.

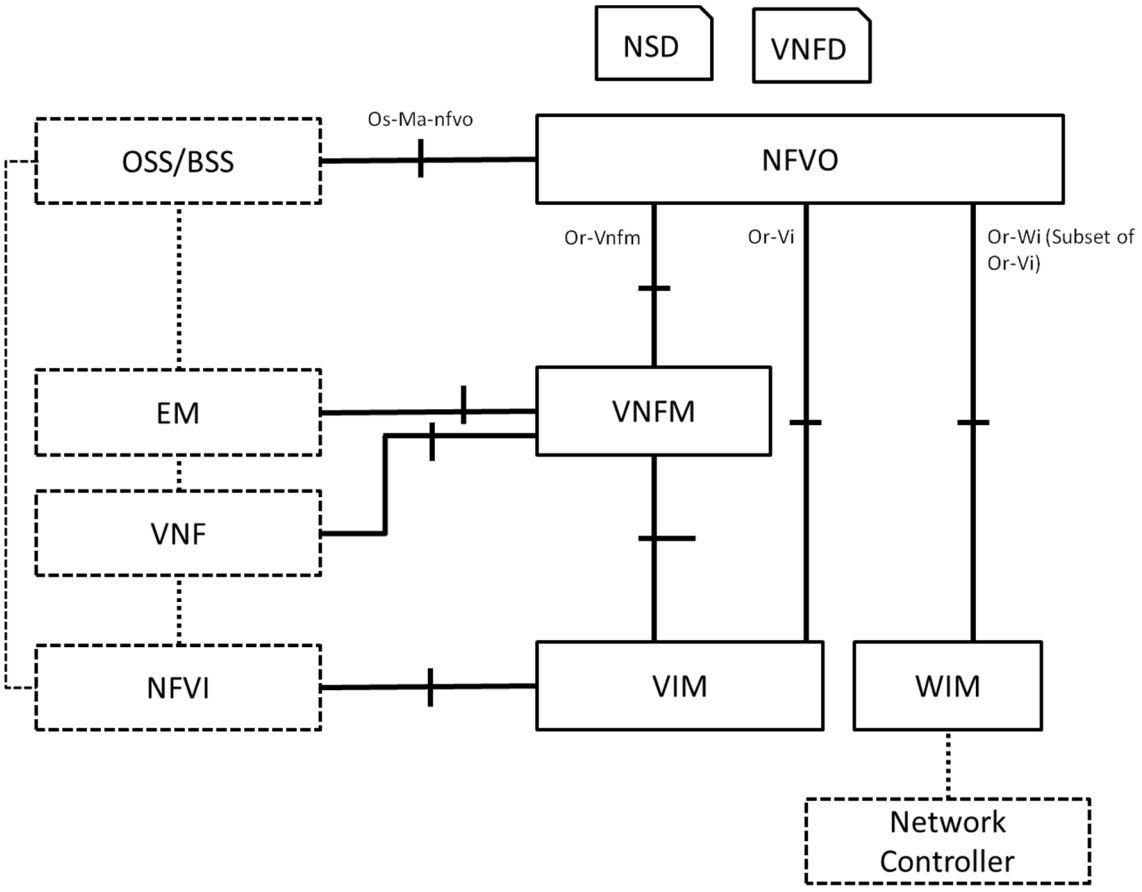

Figure 6.3.2-1: Managing WIM function blocks using Or-Wi reference point

Table 6.3.2-1 lists the descriptors specified in NFV-MANO stage 2 specifications, and maps them to the descriptors for this option.

Table 6.3.2-1: Mappings of descriptors

MANO Descriptors	Descriptors in this option	Changes
NSD	NSD	Following enhancements are necessary in ETSI GS NFV-IFA 014 [i.12]: • Specifying requirements for multi-site network services
VNFD	VNFD	Following enhancements are necessary in ETSI GS NFV-IFA 011 [i.10]: • Specifying requirements for multi-site VNF deployments
VLD	VLD	Following enhancements are necessary in ETSI GS NFV-IFA 014 [i.12]: • Specifying requirements for connectivity of multi-site network services

Table 6.3.2-2 lists the reference points specified in NFV-MANO stage 2 specifications, and maps them to the reference points applied for this option.

In this option, the reference point specified in ETSI GS NFV-IFA 005 [i.7] are basically reused for this Or-Wi reference point. However such necessary enhancements to existing ETSI GS NFV-IFA 005 [i.7] interfaces and/or new interface should be specified in order to enable the WIM to manage the WAN resources and connectivity. This is because the management interface for WAN transport devices is standardized in several communities such as [i.24] and [i.33]. The NFVO thus needs to be provided relevant WAN and WAN topology information for management of network connectivity among NFVI-PoPs.

Table 6.3.2-2: Mapping of reference points

MANO Reference Point	Reference Points in this option	Changes
Os-Ma-nfvo	Os-Ma-nfvo	Following enhancements are necessary in ETSI GS NFV-IFA 013 [i.11]: • Exchanging multi-site requirements
Or-Vnfm	Or-Vnfm	Following enhancements are necessary in ETSI GS NFV-IFA 007 [i.8]: • Managing multi-site VNF deployments • Managing external managed internal VLs supporting multi-sites
Or-Vi	Or-Vi	Following enhancements are necessary in ETSI GS NFV-IFA 005 [i.7]: • Extending management of network gateway at NFVI-PoP • Providing information for connecting NFVI-PoPs
Vi-Vnfm	Vi-Vnfm	Unchanged
Ve-Vnfm	Ve-Vnfm	Unchanged
Or-Vi	Or-Wi (Subset of Or-Vi)	ETSI GS NFV-IFA 005 [i.7] interfaces are reused for this reference point and following enhancement are necessary in ETSI GS NFV-IFA 005 [i.7]: • Virtualised network resource management for WAN connectivity • Providing information for connecting WAN and WAN topology

Table 6.3.2-3 summarizes the function enhancements of the NFV-MANO function blocks.

Table 6.3.2-3: NFV-MANO function blocks

MANO Function Block	Changes
NFVO	The NFVO needs to consider the interface changes as described in Table 6.3.2-2. The NFVO needs to support multi-site functionality as follows: Lifecycle management of NS across NFVI-PoPs. • Orchestration of actions related to virtualised network resources among multiple NFVI-PoPs managed by one or more VIMs and WIMs
VNFM	The VNFM needs to consider the interface changes as described in Table 6.3.2-2. The VNFM needs to support multi-site functionality as follows: • Multi-site VNF deployment
VIM	The VIM needs to consider the interface changes as described in Table 6.3.2-2. The VIM needs to support multi-site functionality as follows: • Management of network gateway at NFVI-PoP

6.3.3 Architecture option #B: Managing WIM functionality of OSS/BSS with Os-Ma-nfvo reference points

The Os-Ma-nfvo reference point needs to be enhanced to manage the newly required WAN management functions, as shown in Figure 6.3.3-1. The NFV-MANO does not have responsibility for the management of the virtualised network resources inside the WAN. Instead the NFVO can requests the management of virtualised network resource of WAN for NFV services with OSS/BSS that span across multiple NFVI-PoPs. If WAN connectivity is pre-provisioned (refer to clause 6.3.1), the NFVO can be provided information about the relevant connectivity that spans across the multiple NFVI-PoPs.

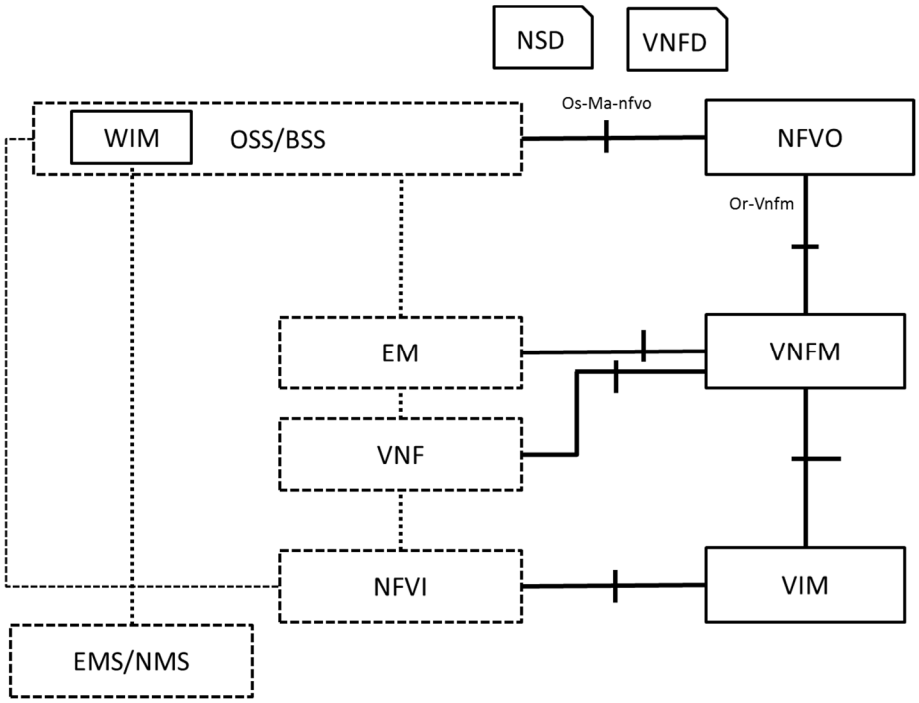

Figure 6.3.3-1: Managing WIM function blocks using Os-Ma-nfvo reference point

Table 6.3.3-1 lists the descriptors specified in NFV-MANO stage 2 specifications, and maps them to the descriptors applied for this option.

Table 6.3.3-1: Mapping of descriptors

MANO Descriptors	Descriptors in this option	Changes
NSD	NSD	Following enhancements are necessary in ETSI GS NFV-IFA 014 [i.12]: • Specifying requirements for multi-site network services
VNFD	VNFD	Following enhancements are necessary in ETSI GS NFV-IFA 011 [i.10]: • Specifying requirements for multi-site VNF deployments
VLD	VLD	Following enhancements are necessary in ETSI GS NFV-IFA 014 [i.12]: • Specifying requirements for connectivity of multi-site network services

Table 6.3.3-2 lists the reference points specified in NFV-MANO stage 2 specifications, and maps them to the reference points applied for this option. In this case, Os-Ma-nfvo reference point needs to include operations to manage virtualised network resource of WAN. If WAN connectivity is pre-provisioned, then the Os-Ma-nfvo reference point needs to include the capability for the OSS/BSS to provide information to the NFVO about the relevant connectivity that spans across the multiple NFVI-PoPs.

Table 6.3.3-2: Mapping of reference points

MANO reference Point/descriptor	Reference Points in this Use Case	Change due to the use case
Os-Ma-nfvo	Os-Ma-nfvo	Following enhancements are necessary in ETSI GS NFV-IFA 013 [i.11]: • Exchanging parameters for multi-site network service In addition, following enhancements are necessary to support WIM function operation in ETSI GS NFV-IFA 013 [i.11]: • Requesting Virtualised network resource management for WAN • Providing information for connecting WAN (VPN) and WAN (VPN) topology
Or-Vnfm	Or-Vnfm	Following enhancements are necessary in ETSI GS NFV-IFA 007 [i.8]: • Managing multi-site VNF deployments • Managing external managed internal VLs supporting multi-site
Or-Vi	Or-Vi	Following enhancements are necessary in ETSI GS NFV-IFA 005 [i.7]: • Extending management of the network gateway at NFVI-PoP • Providing information for connecting NFVI-PoPs
Vi-Vnfm	Vi-Vnfm	Unchanged
VeVnfm	VeVnfm	Unchanged

Table 6.3.3-3 summarizes the function enhancements of the NFV-MANO function blocks.

Table 6.3.3-3: NFV-MANO function blocks

MANO Function Block	Changes
NFVO	The NFVO needs to consider the interface changes as described in Table 6.3.3-2. The NFVO needs to support multi-site functionality as follows: • Orchestration of actions related to virtualised network resources among multiple NFVI-PoPs managed by one or more VIMs and/or WIM
VNFM	The VNFM needs to consider the interface changes as described in Table 6.3.3-2. The VNFM needs to support multi-site functionality as follows: • Multi-site VNF deployment
VIM	The VIM needs to consider the interface changes as described in Table 6.3.3-2. The VIM needs to support multi-site functionality as follows: • Management of network gateway at NFVI-PoP

6.4 Information modelling analysis

6.4.1 General

Clause 6.4 analyses the use cases and provides a summary of gaps with respect to the NFV Information Model, including design time information, i.e. NS Descriptor and VNF Descriptor, and runtime, i.e. NS, VNF and VR related information elements.

6.4.2 Gap analysis and extensions to NSD and VNFD

6.4.2.1 Current connectivity model in the NSD (IFA 014)

Figure 6.4.2.1-1 illustrates the current information modelling available in the NSD. The figure only shows the most relevant information elements used to define connectivity aspects such as NS VLs, etc., and it is therefore not exhaustive.

NOTE: The purpose of the modeling illustrated on the Figure 6.4.2.1-1 is to provide an indication of the type of information relevant to connectivity and it should not be understood as an alternative to the already available NFV Information Model of ETSI GR NFV-IFA 015 [i.13].

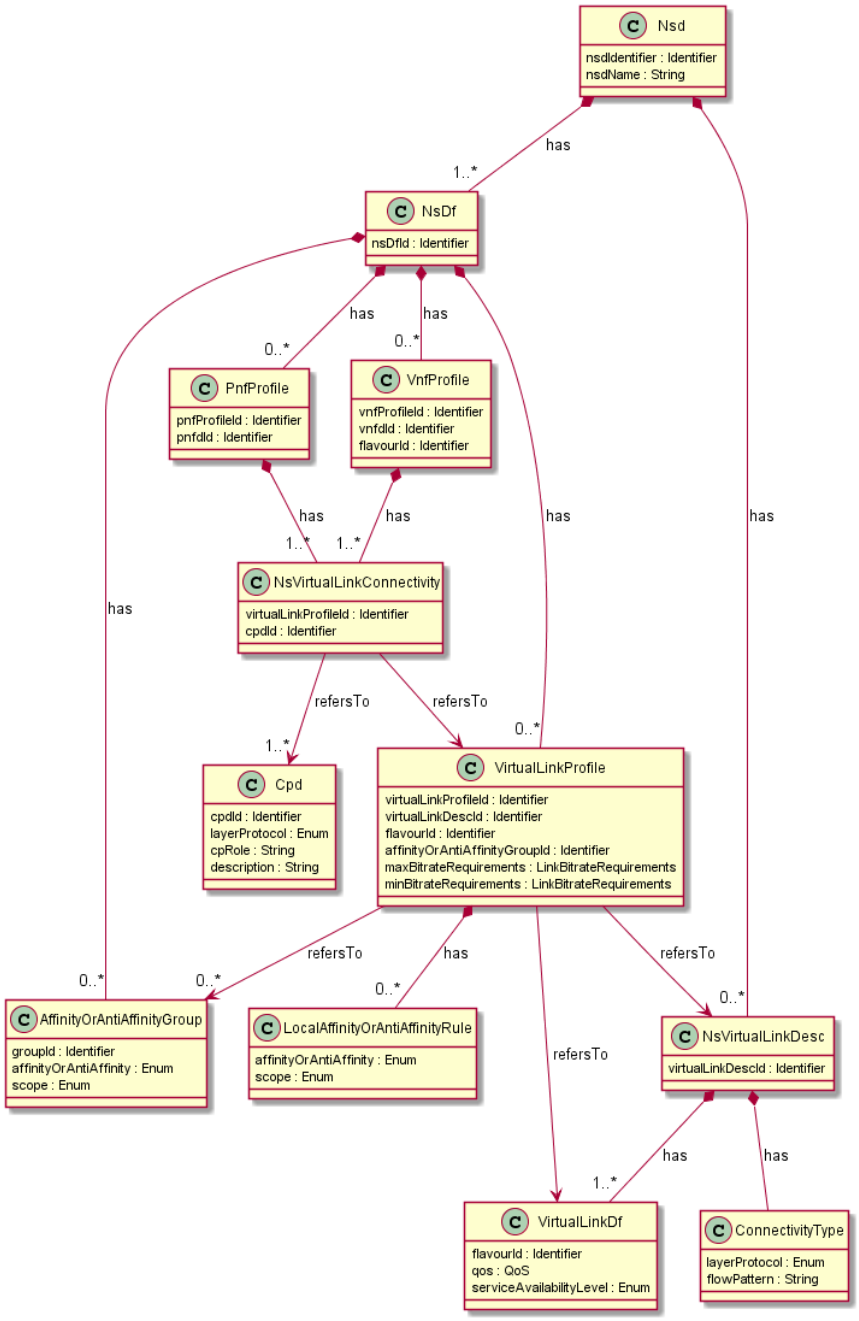

Figure 6.4.2.1-1: Current NSD connectivity model based on ETSI GS NFV-IFA 014 [i.12]

6.4.2.2 Affinity/anti-affinity constraints

6.4.2.2.1 Description

As introduced in clause 6.4.2.1, affinity/anti-affinity constraints can be described in an NSD to determine the affinity/anti-affinity requirements, not only for VNF instances, but also for NS VLs.

With respect to affinity/anti-affinity constraints, and as derived from the use cases, the following items are relevant:

1) Handling affinity/anti-affinity constraints to ensure that NS Virtual Links are anti-affine in terms of physical WAN resources, when such NS VLs are set for redundancy purposes.

Assuming the example of two NS Virtual Link to be anti-affine for redundancy purposes, the modeling to support the affinity/anti-affinity constraints can potentially be performed with two variants:

Option #1:

1) Create two `VirtuaLinkProfile`, e.g. *virtualLinkProfile-1* and *virtuaLinkProfile-2*. The two `VirtualLinkProfile` can refer to the same `NsVirtualLinkDesc` and same `VirtualLinkDf`, i.e. `virtualLinkDescId` and `flavourId` in *virtualLinkProfile-1* and *virtualLinkProfile-2* have same value.

2) The anti-affinity requirement can be specified in two ways:

   a) Case #1: Usage of `AffinityOrAntiAffinityGroup` (see Figure 6.4.2.2.1-1).

      Create an `AffinityOrAntiAffinityGroup` in the `NsDf`, e.g. *affinityOrAntiAffinityGroup-1*. Set the `affinityOrAntiAffinity` = "*anti-affinity*" with a new scope value of *network-link-and-node*.

      In the two `VirtualLinkProfile`, use affinityOrAntiAffinityGroupId = "*affinityOrAntiAffinityGroup-1*".

   b) Case #2: Usage of `LocalAffinityOrAntiAffinityRule` (see Figure 6.4.2.2.1-2).

      The `localAffinityOrAntiAffinityRule` of the two `VirtualLinkProfile` will have `affinityOrAntiAffinity` = "*anti-affinity*" with a new scope value of "*network-link-and-node*".

3) The `nsVirtualLinkConnectivity` of the involved `VnfProfile` in the NS will contain the link to the corresponding `VirtualLinkProfile`, i.e. *virtualLinkProfile-1* or *virtualLinkProfile-2*, for the required different connection points exposed by the VNF, which will need to be represented by different CPD.

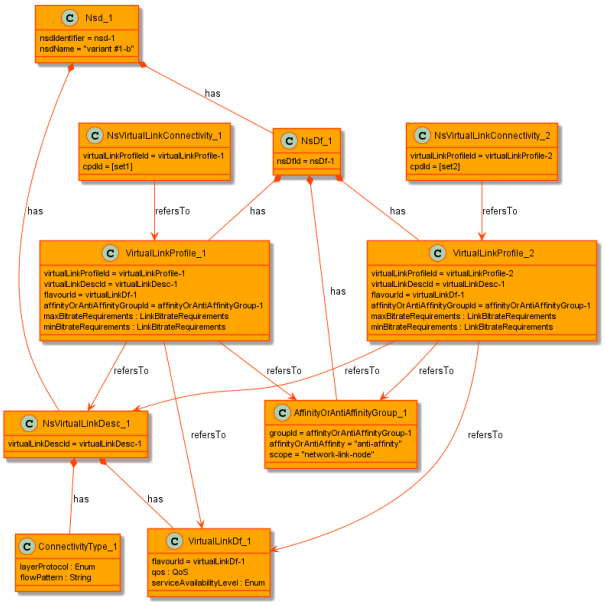

Figure 6.4.2.2.1-1: Option #1 Case #1

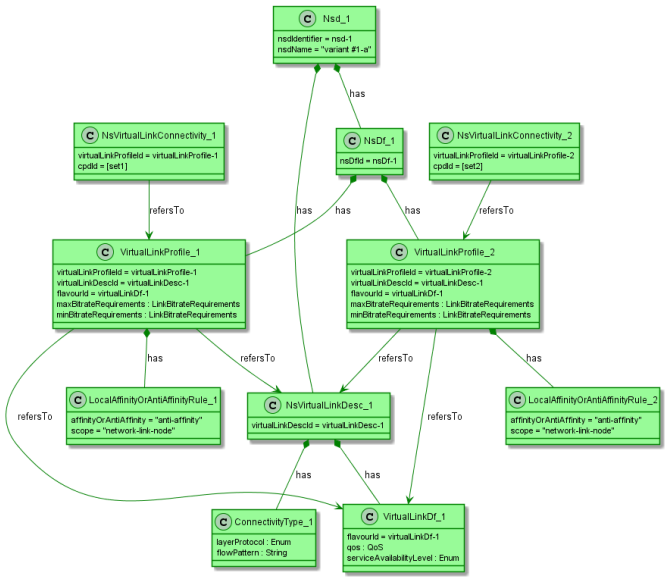

Figure 6.4.2.2.1-2: Option #1 Case #2

Option #2:

1) Create two `NsVirtualLinkDesc`, e.g. *virtualLinkDesc-1* and *virtualLinkDesc-2*.

2) From each `virtualLinkDesc`, create a `VirtualLinkProfile`, e.g. *virtualLinkProfile-1* (from *virtualLinkDesc-1*) and *virtualLinkProfile-2* (from *virtuaLinkDesc-2*).

3) Create an `AffinityOrAntiAffinityGroup` in the `NsDf`, e.g. *affinityOrAntiAffinityGroup-1*. Set the `affinityOrAntiAffinity` = "*anti-affinity*" with a new scope value of "*network-link-and-node*".

4) In the two `VirtualLinkProfile` from step 2, use `affinityOrAntiAffinityGroupId` = *affinityOrAntiAffinityGroup-1*.

5) The `nsVirtualLinkConnectivity` of the involved `VnfProfile` in the NS will contain the link to the corresponding `VirtualLinkProfile`, i.e. *virtualLinkProfile-1* or *virtualLinkProfile-2*, for the required different connection points exposed by the VNF, which will need to be represented by different CPD.

Figure 6.4.2.2.1-3 illustrates an example according to option #2.

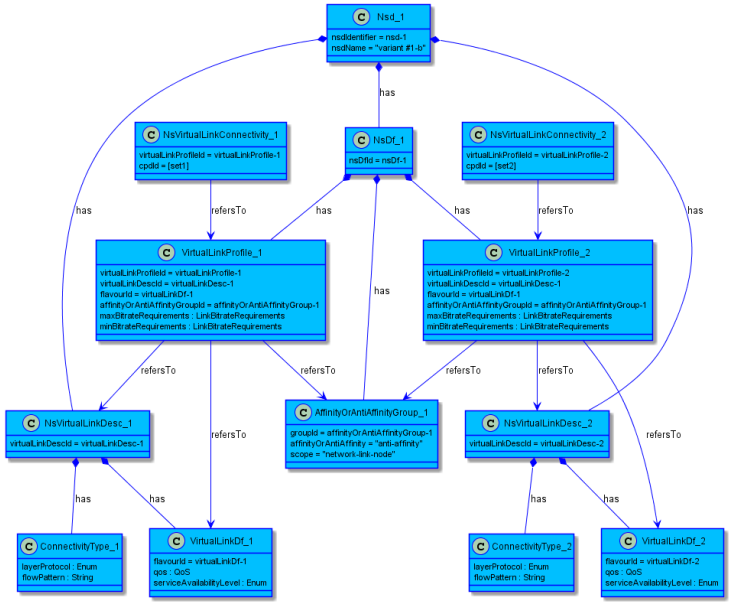

Figure 6.4.2.2.1-3: Option #2

6.4.2.2.2 Identified gaps and/or extensions

Following are a list of identified gaps and/or needed extensions to affinity/anti-affinity constraints in the NSD:

1) Define a new scope value of *network-link-and-node* for `localAffinityOrAntiAffinityRule` or `AffinityOrAntiAffinityGroup` in the NSD.

   The *network-link-and-node* scope is conceptually similar to link and node disjoint paths capabilities used commonly in network traffic engineering (TE) (for example, as in Fast Reroute Resource Reservation Protocol Traffic Engineering (RSVP-TE) for Label-Switched Path (LSP) tunnels as introduced in IETF RFC 4090 [i.22]).

6.4.2.3 NS VL service availability features

6.4.2.3.1 Description

As introduced in clause 5.8.8, the NS VL healing use case illustrates the need to enable capabilities for provisioning redundant virtualised network resources in the WAN and/or to determinte the reuse of existing virtualised network resources to fulfil service availability of the NS VL.

The `VirtualLinkDf` information element in clause 6.5.4 of ETSI GS NFV-IFA 014 [i.12] specifies the property of `serviceAvailabilityLevel` according to the three levels (Level 1, Level 2 and Level 3) defined in ETSI GS NFV-REL 001 [i.23]. According to Table 1 in clause 7.3.2 of ETSI GS NFV-REL 001 [i.23], the characteristics of the three levels with regards to redundancy and handling priority are:

- Level 1: it may require 1+1 redundancy with instantaneous switchover.
- Level 2: it may require 1:1 redundancy with fast (maybe instantaneous) switchover.
- Level 3: it may require M+1 redundancy with fast switchover.

NOTE 1: Level 3 in ETSI GS NFV-REL 001 [i.23] refers to M+1, but in networking, the terminology 1:N (or M:N, with M =< N) is commonly used instead.

ETSI GS NFV-REL 001 [i.23] does not detail the applicability of the service availability levels for NFV constructs such as VL, or VNF, and the reduncancy towards the virtualised resources. However, the `serviceAvailabilityLevel` might be reused in the multi-site NS VL context as follows, i.e. when a value of `serviceAvailabilityLevel` is specified for the `VirtualLinkDf`:

NOTE 2: The present analysis does not take into account any service availabilty features at the WIM/VIM and below it.

- Level 1: 1+1 virtualised network resource redundancy is provided for a VL created based on such `VirtualLinkDf`. In this case, virtualised network resources are instantiated in a 1+1 configuration to support a single NS VL, i.e. active-active configuration.
- Level 2: 1:1 virtualised network resource redundancy is provided for a VL created based on such `VirtualLinkDf`. In this case, virtualised network resources are instantiate in a 1:1 configuration to support a single NS VL, i.e. active-passive, or active-active with possibility to pre-empt traffic on the redundant resources.
- Level 3: 1:N virtualised network resource redundancy is provided for a VL created based on such `VirtualLinkDf`. In this case, virtualised network resource is instantiated for redundancy, but it support redundancy for the virtualised network resources of more than one NS VL.

NOTE 3: Active-active redundancy configuration can have an impact on the resource handling by the VIM/WIM, and on the connectivity configuration itself, which are not further analysed in the present document.

While the `serviceAvailabilityLevel` can fulfil the need for specifying redundancy requirements, the scope and applicability of the redundancy requirement applies to the whole NS VL without differentiating per virtualised network resource segments. According to the use case in clause 5.8, the multi-site NS VL can span NFVI-PoP and WAN segments, for which different virtualised network resources are instantiated, but in the use case, only the virtualised network resource in the WAN is redundant.

In addition, use case 8: multi-site VNF deployment in clause 5.9 showcases the deployment of an internal VNF VL across multiple sites and on the WAN by making use of the externally-managed internal VL. Considering the analysis above, `serviceAvailabilityLevel` might also be needed to be defined for the internal VNF VL. Currently, the internal VNF VL deployment flavour specification, refer to information element `VirtualLinkDescFlavour` (see clause 7.1.8.5 of ETSI GS NFV-IFA 011 [i.10]), does not specify any attribute related to service availability level.

6.4.2.3.2 Identified gaps and/or extensions

Following is a list of identified gaps and/or needed extensions related to NS VL service availability features:

1) Service availability level information may need to be extended to indicate its applicability to the different multi-site NS VL part(s) (e.g. NFVI-PoP or WAN).
2) The internal VNF VL specification may need to be extended to specify service availability level information associated to specific VL flavours.

6.4.3 Gap analysis and extensions to NS runtime information

6.4.3.1 Current connectivity model in the NS runtime information (ETSI GS NFV-IFA 013)

Figure 6.4.3.1-1 illustrates the current information modelling available in the NsInfo information element. The figure only shows the most relevant information elements used to define connectivity aspects such as NS VLs, etc., and it is therefore not exhaustive.

NOTE: The purpose of the modeling illustrated on the Figure 6.4.3.1-1 is to provide an indication of the type of information relevant to connectivity and it should not be understood as an alternative to the already available NFV Information Model of ETSI GR NFV-IFA 015 [i.13].

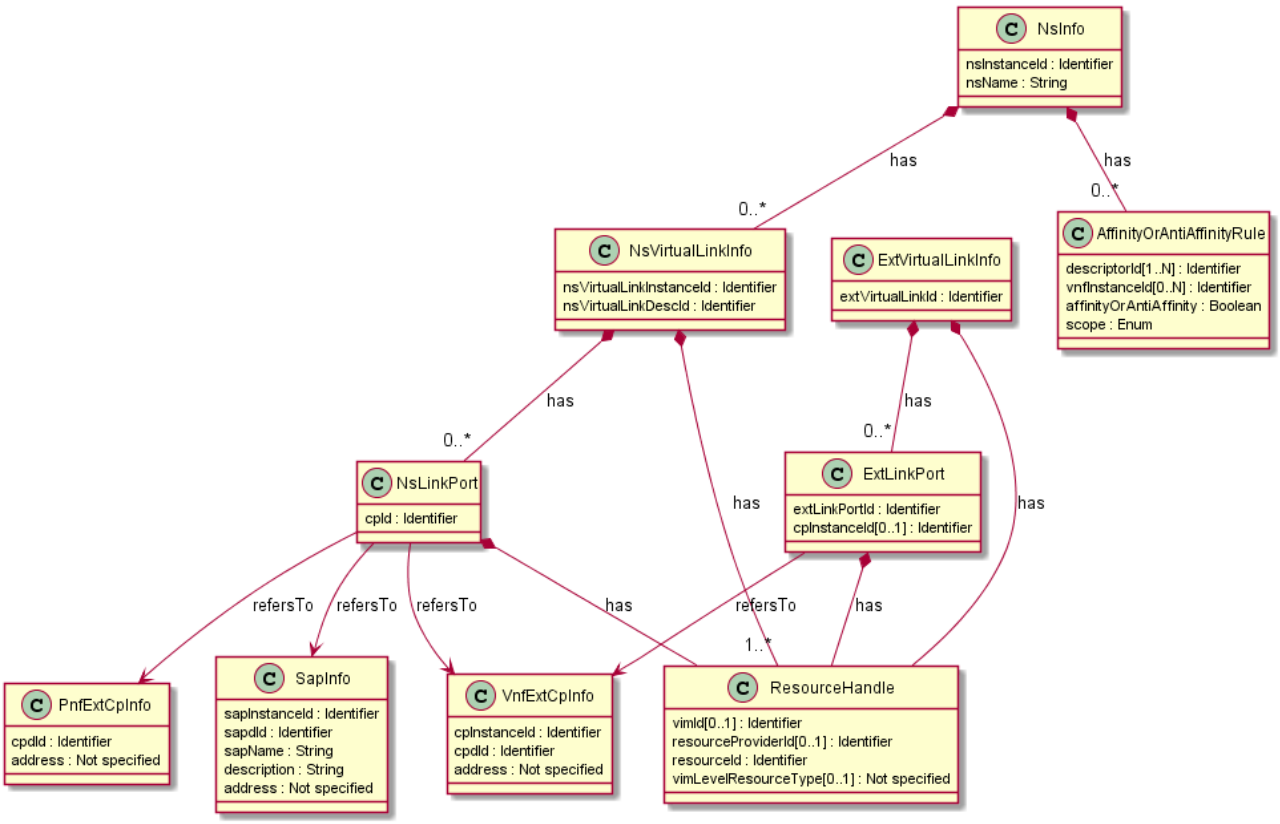

Figure 6.4.3.1-1: Current NS information model from ETSI GS NFV-IFA 013 [i.11]

6.4.3.2 NS VL runtime view

6.4.3.2.1 Description

As introduced in clause 6.4.3.1, NS VL runtime information is available at the NFVO level.

With respect to NS VL runtime information, and as derived from the use cases, the following items are relevant:

1) Handling NS VL aggregation at the NFVO level.

   The NFVO has a view of the one or more VL of an NS. When the NS VL agreggation is performed, i.e. a virtualised network resource is mapped/used to fulfill the resources for more than one NS VL, the NFVO needs to know and handle such aggregation.

   There are possible options with regards to handling NS VL aggregation at the NFVO level:

   Option #1:

   - A new information element holds the relationship between NS VL and `ResourceHandle` of corresponding virtualised network resource. The new information element potentially also holds information about the characteristics (rules) for the aggregation.
   - A benefit of this option is that aggregation information minimizes impact to current `NsInfo` modelling. In addition, it provides a means for holding aggregation information that is potentially relevant to more than one `NsInfo` (e.g. if NS VL aggregation is performed among VLs of different NS), thus simplifying the synchronization of such type of information.

The impact might depend on whether a reference association is established between the `NsVlAggregate` and the `ResourceHandle` (see example in Figure 6.4.3.2.1-1), or whether the value of the `resource` attribute in the `NsVlAggregate` identifies the specific resources. In the latter case, just a copy of the value of the `resourceId` of the `ResourceHandle` might not be enough, as `resourceId` may not be unique across different VIM or resource providers, and therefore, some sort of additional identifier might be needed which can be derived from existing information in the `ResourceHandle` (e.g. by concatenating `vimId/resourceProviderId` (whichever is present) with the `resourceId`).

Figure 6.4.3.2.1-1 illustrates the NS VL aggregation description option #1.

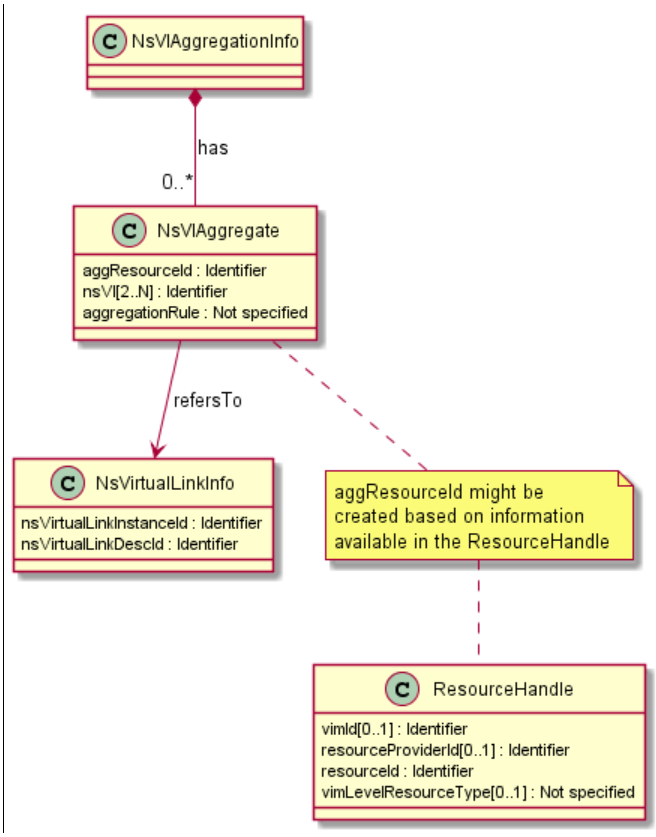

Figure 6.4.3.2.1-1: Option #1 for NS VL aggregation

Option #2:

- The `ResourceHandle` corresponding to a virtualised network resource holds information about the NS VLs that are aggregated.

This option does not impact the modelling with regards to the need of creating new information elements. However, it impacts current existing information elements. Furthermore, considering the potential case that NS VL aggregation is performed among VLs of different NS, and even VLs in the same NS, and the fact that `ResourceHandle`(s) are part of the `NsVirtualLinkInfo`, this can potentially result in duplicated information and complexity on keeping synchronized the aggregation information (i.e. the new `usedByNsVl` attribute) for the different contained `ResourceHandle`(s) of the different `NsVirtualLinkInfo`.

Figure 6.4.3.2.1-2 illustrates the NS VL aggregation description option #2 with the introduction of the attribute `usedByNsVl` referencing to `NsVirtualLinkInfo`.

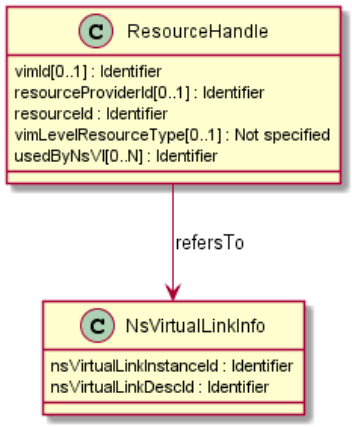

Figure 6.4.3.2.1-2: Option #2 for NS VL aggregation

Option #3:

- A new information element holds the relationship between NS VL and `ResourceHandle` of corresponding virtualised network resource. The new information element is only used as an attribute when a specific `ResourceHandle` is used by more than one NS VL. The new information element potentially also holds information about the characteristics (rules) for the aggregation.

This option impacts current existing information elements as well it requires creating additional information elements. Furthermore, considering the potential case that NS VL aggregation is performed among VLs of different NS, and even VLs in the same NS, and the fact that `ResourceHandle`(s) are part of the `NsVirtualLinkInfo`, this can potentially result in duplicated information and increased complexity on keeping synchronized the aggregation information (i.e. the new `NsVlAggregate`) for the different contained `ResourceHandle`(s) of the different `NsVirtualLinkInfo`.

Figure 6.4.3.2.1-3 illustrates the NS VL aggregation description option #3.

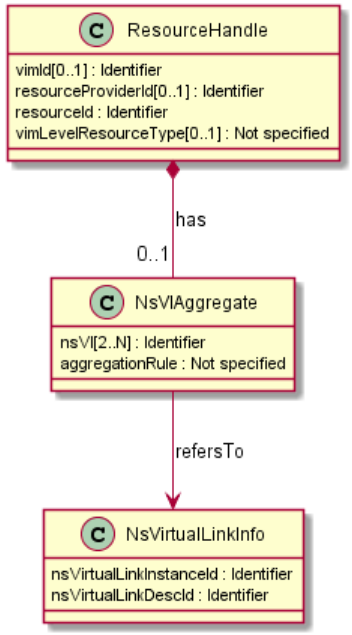

Figure 6.4.3.2.1-3: Option #3 for NS VL aggregation

2) Handling NS VL aggregation at VIM/WIM level.

   The `VirtualNetwork` information element corresponding to a virtualised network resource (refer to clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7]) already specifies the attribute `isShared`, which defines whether or not the virtualised network is shared among consumers. The `isShared` attribute can be used to indicate support of NS VL aggregation at the VIM/WIM level.

6.4.3.2.2 Identified gaps and/or extensions

Following are a list of identified gaps and/or needed extensions:

1) Information to identify the NS VL original profiles is not available in the `NsVirtuaLinkInfo` contained in the NsInfo.

   The `NsVirtualLinkInfo` information element only provides information about the `NsVirtualLinkDesc` (VLD in the NSD) that is derived from. However, according to NSD specification, it is not restricted that there is only one `VirtualLinkProfile` per `NsVirtualLinkDesc`, as `VirtualLinkProfile` is used also to determine the NS VL connectivity among specific CPD.

2) NS VL aggregation is not traced easily in the current `NsVirtualLinkInfo` information.

   Currently, no restriction is specified in the ETSI GS NFV-IFA 013 [i.11] in the usage of a `ResourceHandle` corresponding to a WAN virtualised network resource on more than one `NsVirtualLinkInfo`. The NFVO needs to be able to determine that certain virtualised network resource is used by more than one NS VL, and what type of virtualised network resource or NS VL characteristic is used as the basis for the NS VL aggregation.

6.4.4 Gap analysis and extensions to VNF runtime information

6.4.4.1 Current connectivity model in the VNF runtime information (ETSI GS NFV-IFA 007)

Figure 6.4.4.1-1 illustrates the current modelling available in the VnfInfo information element. The figure only shows the most relevant information elements used to define connectivity aspects such as internal VLs, etc., and it is therefore not exhaustive.

NOTE: The purpose of the modeling illustrated on the Figure 6.4.4.1-1 is to provide an indication of the type of information relevant to connectivity and it should not be understood as an alternative to the already available NFV Information Model of ETSI GR NFV-IFA 015 [i.13].

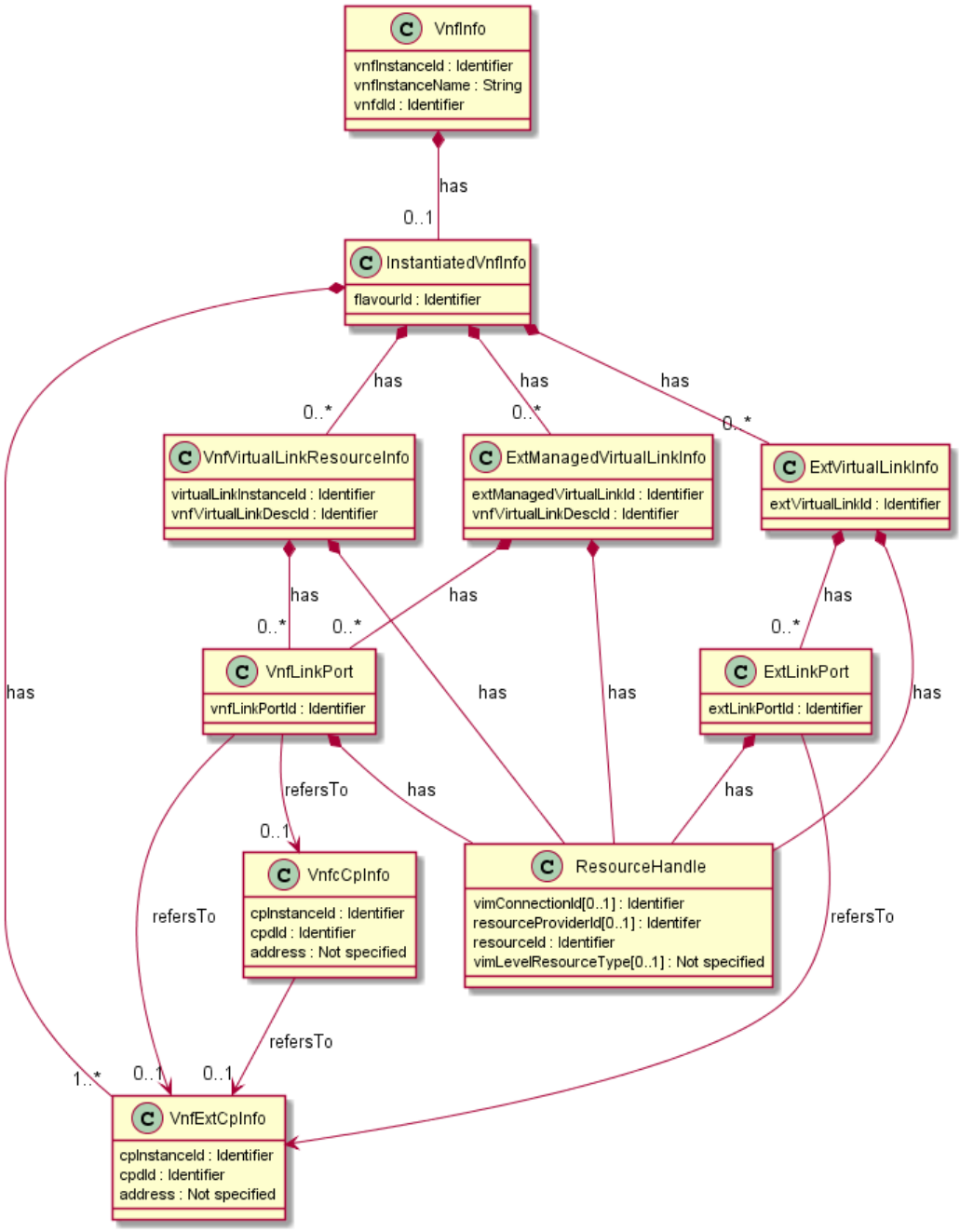

Figure 6.4.4.1-1: Current VNF connectivity information model from ETSI GS NFV-IFA 007 [i.8]

6.4.4.2 VNF VL runtime view

6.4.4.2.1 Description

VNF connectivity information is available both at VNFM and NFVO level. The relevant connectivity information available at the VNFM level is introduced in clause 6.4.4.1.

With respect to VNF runtime information related to connectivity, and as derived from the use cases, the following items are relevant:

1) Realization of multi-site VNF internal VL as externally-managed internal VL.

   A multi-site VNF deployment can be enabled when the VNF internal VL is realized as an externally managed internal VL The example is described in the use case in clause 5.9. In the use case, the NFVO is responsible for triggering the network connectivity for the externally-managed internal VL with required resources within NFVI-PoPs and across WAN. As a result, different virtualised network resources can be utilized to instantiate a externally-managed internal VL.

   To support this case, the `ExtManagedVirtualLinkInfo` needs to be enabled to be "composed" by more than one ResourceHandle. Each one of the `ResourceHandle` mapping to one particular virtualised network resource, either in the NFVI-PoP or on the WAN. Differences can still apply with regards to the `ExtManagedVirtualLinkInfo` maintained by the VNFM and the one maintained by the NFVO:

   - `ExtManagedVirtualLinkInfo` maintained/known by the VNFM: it includes only the `ResourceHandle` for the virtualised network resources that are directly "in touch" with VNF resources, for example, to enable adding/removing `VnfLinkPort`(s) in order to connect VNFC (realized via corresponding virtualised containers and its network interfaces).

   - `ExtManagedVirtualLinkInfo` maintained by the NFVO: it includes `ResourceHandle` for "all" virtualised network resources, both in the NFVI-PoP and used to connect VNF resources, as well as virtualised network resources on the WAN.

Figure 6.4.4.2.1-1 shows a possible realization of the `ExtManagedVirtualLinkInfo` maintained by the NFVO to support multi-site VNF internal VL.

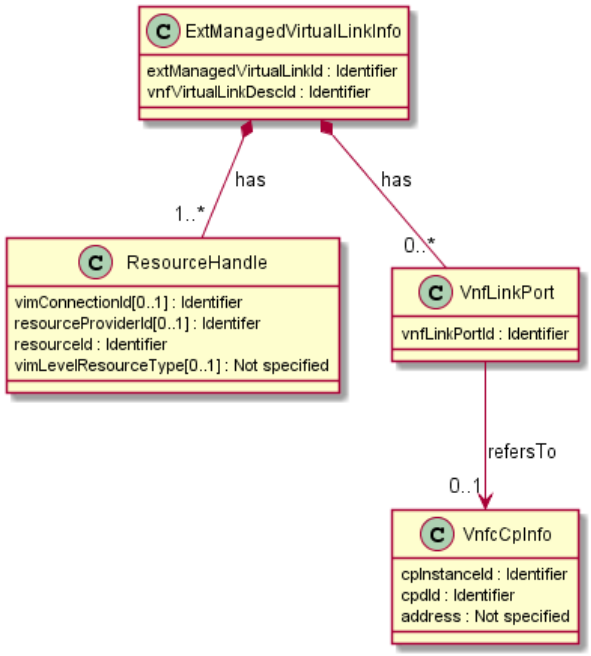

Figure 6.4.4.2.1-1: Extension to support multiple `ResourceHandle` to realize an `ExtManagedVirtualLinkInfo`

6.4.4.2.2 Identified gaps and/or extensions

Following are a list of identified gaps and/or needed extensions:

1) Extending the `ExtManagedVirtualLinkInfo` maintained by the NFVO to include multiple `ResourceHandle`, i.e. updating the cardinality of the `ResourceHandle` in the `ExtManagedVirtualLinkInfo` from "1" to "1..*".

6.4.5 Gap analysis and extensions to virtualised network resource runtime information

6.4.5.1 Current connectivity model related to virtual network and NFVI-PoP connectivity (ETSI GS NFV-IFA 005)

Figure 6.4.5.1-1 illustrates the current information modelling available in the VirtualNetwork information element. The figure only shows the most relevant information elements used to define connectivity aspects such as virtual network ports, network subnets and virtual network interfaces.

NOTE: The purpose of the modeling illustrated on the Figure 6.4.5.1-1 and Figure 6.4.5.1-2 is to provide an indication of the type of information relevant to connectivity and it should not be understood as an alternative to the already available NFV Information Model of ETSI GR NFV-IFA 015 [i.13].

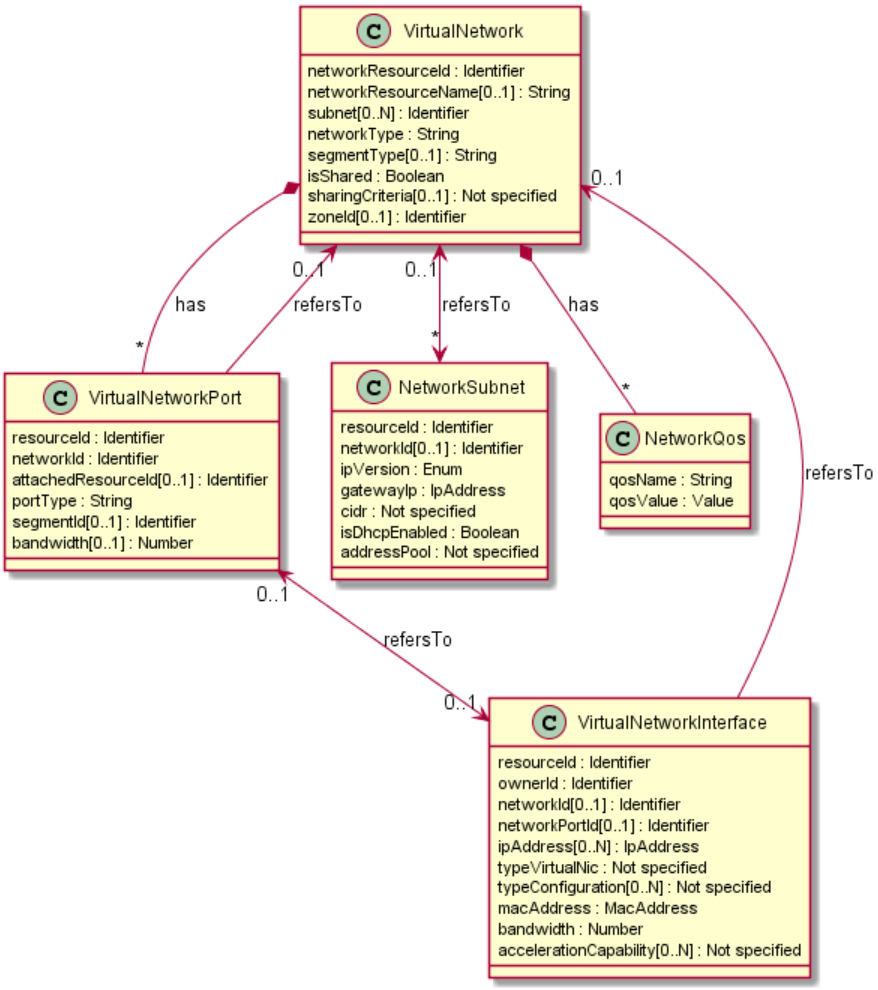

Figure 6.4.5.1-1: Current `VirtualNetwork` information model from ETSI GS NFV-IFA 005 [i.7]

Figure 6.4.5.1-2 illustrates the current information modeling available in the `NfviPop` information element specified in clause 8.10.3 of ETSI GS NFV-IFA 005 [i.7]. The `NfviPop` information element contains basic data to identify an NFVI-PoP in a VIM, and it helps consumer functional blocks build topological information relative to NFVI-PoP connectivity to other NFVI-PoP.

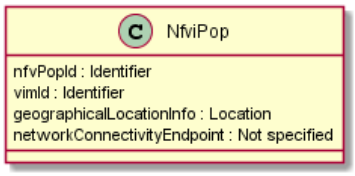

Figure 6.4.5.1-2: Current `NfviPop` information model from ETSI GS NFV-IFA 005 [i.7]

6.4.5.2 Virtual network runtime deployment view

6.4.5.2.1 Description

The `VirtualNetwork` information element, as specified in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7] (for the Or-Vi reference point), provides runtime information of a virtual network as managed by a VIM and therefore, is a representation of the available resources provided by the NFVI within a Site.

With respect to the runtime information of a virtual network, and as derived from the use cases, the following items are relevant:

1) Virtual network runtime information for virtualised network resources in the WAN.

   A WAN connecting between sites or between a site and an access network does not provide direct connectivity to terminal endpoints. Therefore, certain information available for virtual network resources on the WAN might not be necessary, since such an information is not determining the direct connectivity of the VNF/PNF within the NS VL forwarding graph.

   On the one hand, examples of unnecessary information on virtualised network resources for WAN include:

   - The `NetworkSubnet` information element as there is not exposure of L3 network as a consumable resource.
   - The `VirtualNetworkPort` information element, as there is not direct attachment of virtualised container's vNIC to a WAN port.
   - The `zoneId` attribute of `VirtualNetwork` information element. Such information is more relevant to grouping and partitioning of resource pools in an NFVI-PoP, rather than on WAN.

   On the other hand, additional information on virtualised network resources for WAN includes:

   - Identification of the WAN over which the virtualised network resource is instantiated.
   - The list of NFVI-PoPs to which a particular virtualised network resource for WAN establishes connectivity to.
   - Connectivity properties of the virtualised network resource on the WAN enabling the inter NFVI-PoP connectivity. Part of this information may be technology dependent (see also step 6 in Table 5.2.6-1), hence requiring some generic key-value-pair definition. This information identifies also the different types of network connectivity involved in the multi-site scenario, including:
     - Network type information related to the connectivity provided by the virtualised network resource (see attribute `wanNetworkType` in the example of Figure 6.4.5.2.1-1). Examples: IP, IP/MPLS, Ethernet.
     - Network connectivity type of the virtualised network resource (see attribute `interNfviPopNetworkType` in the example of Figure 6.4.5.2.1-1). Examples: virtual private LAN service (VPLS), Ethernet over MPLS (EoMPLS), EVPN over Network Virtualisation Overlay (NVO) tunnels (VXLAN, NVGRE, MPLS over Generic Routing Encapsulation (GRE)).
     - Network segment information, according to the network type, of the virtualised network resource (see attribute `interNfviPopNetworkSegment` in the example of Figure 6.4.5.2.1-1). Examples: VLAN Identifier (VID), VXLAN Network Identifier (VNI), RD.

  - Connectivity topology information of the virtualised network resource (see attribute `interNfviPopNetworkTopology` in the example of Figure 6.4.5.2.1-1). Examples: point-to-point, mesh, tree.

- Information for connecting the virtualised network resource to the NFVI-PoPs endpoints. See also step 14 in Table 5.2.6-2.

Figure 6.4.5.2.1-1 illustrates an example of the relevant information for virtualised network resources for WAN.

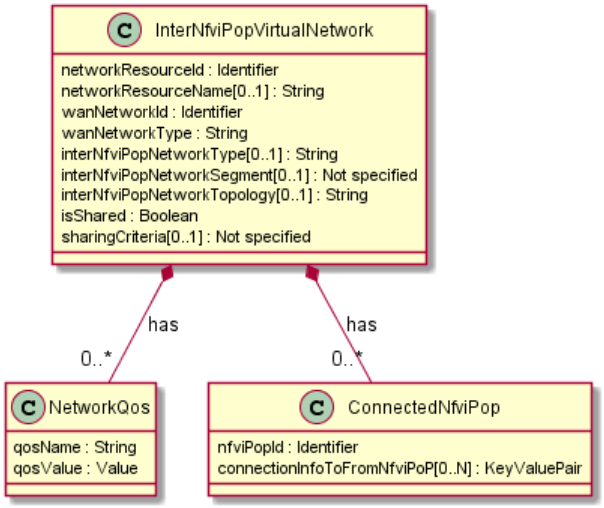

Figure 6.4.5.2.1-1: Example of new `InterNfviPopVirtualNetwork`

2) Virtual network runtime information for virtualised network resources in the NFVI-PoP.

   As introduced in clause 6.4.5.1, the `VirtualNetwork` information element contains information about a virtualised network resource. In the context of ETSI GS NFV-IFA 005 [i.7], this corresponds to a virtualised network resource instantiated within an NFVI-PoP.

   When the virtualised network resource is part of a multi-site VL (either of an NS or internal to a VNF), the connectivity in between the different virtualised network resource segments within the NFVI-PoP and external NFVI-PoP needs to be enabled. To realize this, the VIM needs to handle and manage the stitching of the virtualised network resources within and outside the NFVI-PoP. The stitching can either be performed by translating/routing between internal and external network, or by tunneling the virtualised network of the NFVI-PoP into the virtualised network on the WAN. The VIM makes use and mantains necessary information to configure the network gateways.

   The necessary information, in addition to the `VirtualNetwork`, enabling the association of the virtual network resource within the NFVI-PoP with the internal-to-external NFVI-PoP interconnection includes:

   - Identification of the virtualised network resource.

   - Connectivity to virtualised network resource external to the NFVI-PoP, further including:

     - Identification of the internal-to-external NFVI-PoP interconnection.

     - Type of internal-to-external NFVI-PoP interconnection. Examples: routed, tunnelled.

     - Network connectivity type of the virtualised network resource on the WAN enabling the inter NFVI-PoP connectivity. Examples: VPLS, EoMPLS, VXLAN, NVGRE, MPLS over GRE.

     - Network segment information, according to the network type, of the virtualised network resource on the WAN enabling the inter NFVI-PoP connectivity.

6.4.5.2.2 Identified gaps and/or extensions

Following is a summary list of identified gaps and/or needed extensions:

1) A new information element for virtualised network resources on WAN or a description in the available `VirtualNetwork` identifying the conditions to reuse the `VirtualNetwork` information element for such type of resources.

2) Additional information relevant to virtualised network resource on WAN as described in clause 6.4.5.2.1 point 1).

3) Specify new information elements to detail the association of the virtualised network resource within the NFVI-PoP with the internal-to-external NFVI-PoP interconnection, as introduced in clause 6.4.5.2.1 point 2).

6.4.5.3 NFVI-PoP and WAN connectivity views

6.4.5.3.1 Description

The `NfviPop` information element, as specified in clause 8.10.3 of ETSI GS NFV-IFA 005 [i.7], provides runtime information to help identify an NFVI-PoP in a VIM, and it allows consumer functional blocks build topological information relative to NFVI-PoP connectivity to other NFVI-PoP.

With respect to the runtime information related to NFVI-PoP and inter NFVI-PoP connectivity over WAN, and as derived from the use cases, the following items are relevant:

1) The information about the connectivity endpoints of the NFVI-PoP.

   The NFVI-PoP are assumed to have network gateways that forward traffic in and out of the NFVI-PoP to the WAN or other networks. An example of such a network gateway is a customer edge router between the NFVI-PoP and WAN. Such network gateways are assumed to be under control of the VIM. Information about such gateways is exposed currently as part of the `NfviPoP` information element (see clause 8.10.3 of ETSI GS NFV-IFA 005 [i.7]). The `NfviPop` provides rather static information about the connectivity capabilities, and currently it contains one attribute, `networkConnectivityEndpoint`, that provides information about network connectivity endpoints to the NFVI-PoP. Details of the `networkConnectivityEndpoint` attribute are not specified in the ETSI GS NFV-IFA 005 [i.7].

   To enable the use cases in the present document, additional information is needed, which can include:

   - Network layering capabilities of the gateway. Examples: Layer 2 (L2), Layer 3 (L3).
   - Network type to interconnect to external network. Examples: IP, IP/MPLS,
   - Port/interface addresses to external network(s).
   - QoS support and bitrate of interfaces to external network(s).
   - Network connectivity types supported. Examples: VPLS, EoMPLS, VXLAN, NVGRE, MPLS over GRE.

2) The information about the connectivity support on the WAN.

   Similarly as with the NFVI-PoP, connectivity information and network capabilities of the WAN. An equivalent information element for WAN, herein further referred as `WanPop`, could provide such information, which can include:

   - Identification information, including:
     - Identification of the WAN.
     - Identification of the management entity (e.g. the WIM).

- Network connectivity information, including:
  - Network layering of the network. Examples: L2, L3.
  - Network type. Examples: Ethernet, IP, IP/MPLS,
  - QoS and bitrate support, QoS characteristics (latency, delay, etc.).
  - Information about the network connectivity types supported. Examples: VPLS, EoMPLS, VXLAN, NVGRE, MPLS over GRE.
  - Information about reachability of and among NFVI-PoPs. Example: endpoint port/interface addresses attached to the network.
  - Support of traffic/data flows differentiation.

6.4.5.3.2 Identified gaps and/or extensions

Following is a summary list of identified gaps and/or needed extensions:

1) Additional attributes or information elements to provide connectivity information of the NFVI-PoP to/from external networks as introduced in clause 6.4.5.3.1 point 1).

2) Specify new information elements to detail connectivity information on the WAN interconnecting the different NFVI-PoPs as introduced in clause 6.4.5.3.1 point 2).

7 Recommendations

7.1 Overview

Clause 7 provides recommendations resulting from the analysis performed from the use cases and the analysis in clause 6. Recommendations encompass the identification of potential new requirements, i.e. to describe that a requirement is needed to cover certain aspect or required functionality.

Recommendations are categorized in and elaborated as follows:

- General (refer to clause 7.2);
- Functional (refer to clause 7.3);
- Reference points and/or interfaces (refer to clause 7.4); and
- Descriptors and other information/data model artefacts (refer to clause 7.5).

7.2 General recommendations

The present clause provides recommendations focusing on higher-level and framework aspects.

Table 7.2-1 provides the recommendations related to general aspects of management of connectivity for multi-site services.

Table 7.2-1: General recommendations related to management of connectivity for multi-site services

Identifier	Recommendation description	Comments and/or traceability
Gen.Oam.001	It is recommended that a high-level requirement be specified for the NFV Architectural Framework to support management of connectivity for deployment of Network Services and VNFs on multiple sites.	Refer to clause 6.1
Gen.Oam.002	It is recommended that a requirement set be specified for the WAN infrastructure management.	Refer to clauses 6.1 and 6.2.
Gen.Oam.003	It is recommended that the NFV Information Model and descriptors contain the required information elements related to multi-site NS and VNF connectivity.	Refer to clauses 6.1 and 6.4.

7.3 Functional recommendations

The present clause provides recommendations focusing on functional aspects of functional blocks identified in the NFV Architectural Framework.

Table 7.3-1 provides the recommendations related to functional aspects of NFVO.

Table 7.3-1: Recommendations related to functional aspects of NFVO

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the NFVO to support:		
Nfvo.Oam.001	Lifecycle management of NS across multiple NFVI-PoPs.	Refer to clause 6.1.
Nfvo.Oam.002	Management of NS Virtual Link aggregation over a determined WAN virtualised network resource based on diverse operational policies. See note 1.	Refer to the analysis in clauses 5.5.8 and 6.1. This recommendation also includes necessary extensions for handling NS VL aggregation information (refer to clause 6.4.3.2.2).
Nfvo.Oam.003	Query and acquisition of information about the virtual network resources in the WAN.	Refer to the analysis in clauses 5.6.8 and 6.1. Related to Wim.Im.02.
Nfvo.Oam.004	Handling of alarm notifications about faulty virtualised network resources in the WAN. See note 3 and note 4.	Refer to the analysis in clauses 5.7.8, 5.8.8 and 6.1.
Nfvo.Oam.005	Preparing and requesting the allocation of virtualised network resources in the WAN in advance to their usage. See note 3 and note 4.	Refer to the analysis in clauses 5.8.8, 5.7.8 and 6.1.
Nfvo.Oam.006	Determining the required virtualised network resources in the WAN to meet the requirements for the NS Virtual Links based on the information provided in the NSD. See note 2.	Refer to the analysis in clauses 5.8.8 and 6.1.
Nfvo.Oam.007	Orchestration of actions related to virtualised network resources among multiple NFVI-PoPs managed by one or more VIMs and/or WIMs.	Refer to clause 6.1.
Nfvo.Oam.008	Update of NS Virtual Links to be assigned a specific virtualised network resource in the WAN.	Refer to the analysis in clauses 5.8.8 and 6.1.
Nfvo.Oam.009	Informing/notifying to the VNFM about changes/failures of connectivity on an NS Virtual Link impacting the connectivity of a VNF constituent of the NS and managed by the VNFM. See note 3.	Refer to the analysis in clauses 5.7.8 and 6.1.
Nfvo.Oam.010	Requesting the VNFM to connect/disconnect a specific external connection point of a VNF. See note 3.	Refer to the analysis in clauses 5.7.8 and 6.1.

Identifier	Recommendation description	Comments and/or traceability
Nfvo.Oam.011	Determining the required virtualised network resources in the WAN to meet the requirements for the multi-site deployment of a VNF based on the information provided in the VNFD and/or received via interfaces.	Refer to the analysis in clauses 5.7.8 and 6.1.
Nfvo.Oam.012	Query and acquisition of information about the connectivity support on the WAN.	Refer to analysis in clause 6.4.5.3.2. Related to Wim.Im.01.
Nfvo.Oam.013	Management of VNF internal VL when the VL spans virtualised network resources different NFVI-PoPs and across WAN.	Refer to the analysis in clause 6.4.4.2.2.
Nfvo.Oam.014	Orchestrating the acquisition and provision of information produced by a VIM/WIM about managed virtualised network resources for connecting to the virtualised network resource managed by other VIMs/WIMs.	Refer to clause 5.2.8.
NOTE 1: Operational policies can take different rules or criteria to determine reusing an existing virtualised network resource for the aggregation, such as: - tenancy of the new VL with respect to the already assigned VL; - the (group of) Network Service(s) or VNF(s) to which the new VL to be instantiated belongs to; - the (group of) connectivity types of the VL; - the QoS class of the VL; - the throughput requirements of the VL; and - affinity/anti-affinity rules specified in the NSD. NOTE 2: An example of a requirement is an affinity/anti-affinity constraint to ensure that NS VL are anti-affine in terms of physical WAN resources to fulfil certain redundancy requirements. NOTE 3: This is in support of management of Virtual Link redundancy among NFVI-PoPs. NOTE 4: This is in support of management of Virtual Link healing among NFVI-PoPs.		

Table 7.3-2 provides the recommendations related to functional aspects of VNFM.

Table 7.3-2: Recommendations related to functional aspects of VNFM

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the VNFM to support:		
Vnfm.Oam.001	Multi-site VNF deployment.	Refer to clause 6.1
Vnfm.Oam.002	Connect/disconnect a specific external connection point of a VNF.	Refer to the analysis in clauses 5.7.8 and 6.1.

Table 7.3-3 provides the recommendations related to functional aspects of management of VIM.

Table 7.3-3: Recommendations related to functional aspects of VIM

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the VIM to support:		
Vim.Oam.001	Management of virtualised network resources for connectivity of the NFVI-PoP to / from WAN.	Refer to clause 6.1.
Vim.Oam.002	Update existing virtualised network resources within the NFVI-PoP to connect to a WAN virtualised network resource enabling connectivity to/from the WAN.	Refer to the analysis in clauses 5.4.8 and 6.1.
Vim.Oam.003	Update existing virtualised network resource within the NFVI-PoP to reconnect from a WAN virtualised network resource to another WAN virtualised network resource.	Refer to the analysis in clauses 5.8.8 and 6.1.
Vim.Oam.004	Management of virtualised network resources for overlay or inter-AS connections to/from other NFVI-PoPs.	Refer to the analysis in clauses 5.2.8 and 6.1.
Vim.Oam.005	Providing information about the connectivity of the NFVI-PoP to/from external networks (e.g. WAN).	Refer to the analysis in clause 6.4.5.3.2. Related to Vim.Im.001.
Vim.Oam.006	Providing information about the association of the virtualised network resource within the NFVI-PoP with the internal-to-external NFVI-PoP interconnection.	Refer to the analysis in clause 6.4.5.2.2. Related to Vim.Im.002.

Table 7.3-4 provides the recommendations related to functional aspects of WIM.

Table 7.3-4: Recommendations related to functional aspects of WIM

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the WIM to support:		
Wim.Oam.001	Management of virtualised network resources for connectivity amongst NFVI-PoP over WAN infrastructure.	Refer to clauses 6.1 and 6.2.
Wim.Oam.002	Management of QoS for virtualised network resources of WAN	Refer to clauses 6.1 and 6.2.
Wim.Oam.003	Providing information about the virtual network resources on the WAN.	Refer to the analysis in clauses 5.6.8, 6.1, 6.2 and 6.4.5.2.2. Related to Wim.Im.002.
Wim.Oam.004	Reporting of alarms about faulty virtualised network resources in the WAN.	Refer to the analysis in clauses 5.7.8, 5.8.8, 6.1 and 6.2.
Wim.Oam.005	Providing information about the connectivity support on the WAN.	Refer to analysis in clauses 6.1, 6.2 and 6.4.5.3.2. Related to Wim.Im.001.
Wim.Oam.006	An alarm needs to be provided by the WIM to the NFVO using the Notification mechanism whenever the NFVO should be involved in the healing process for multi-site Virtual Link process.	Refer to the analysis in clauses 5.8.8 and 6.2.

7.4 Reference points and/or interfaces

7.4.1 Reference point between OSS/BSS and NFVO (Os-Ma-nfvo)

The present clause provides recommendations focusing on the definition and specification of interfaces on the Os-Ma-nfvo reference point for the management and connectivity of a multi-site service.

Table 7.4.1-1 provides the recommendations related to interface for life cycle management on the Os-Ma-nfvo reference point.

Table 7.4.1-1: Recommendations related to interface for life cycle management on Os-Ma-nfvo

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the life cycle management interface on Os-Ma-nfvo to support:		
Osmanfvoif.Lcm.001	Lifecycle management of NS across multiple NFVI-PoPs.	Refer to clause 6.1.
Osmanfvoif.Lcm.002	Constraints specified as part for selection of connectivity parameters for Virtual Links that are to be instantiated as part of NS instantiation. For example, to declare whether the Virtual Links should be deployed in the same or different WAN infrastructures.	Refer to clause 5.3.8. The constraints are analysed in "Network Service Descriptor Parsing".
Osmanfvoi.Lcm.003	Providing to the NFVO information about WAN connectivity across multiple NFVI-PoPs available to fulfil the lifecycle management of NS across multiple NFVI-PoPs.	Refer to clauses 5.6.8, 6.3 and 6.4.5.

7.4.2 Reference point between NFVO and VNFM (Or-Vnfm)

The present clause provides recommendations focusing on the definition and specification of interfaces on the Or-Vnfm reference point related to the management and connectivity of a multi-site service.

Table 7.4.2-1 provides the recommendations related to the VNF lifecycle management interface on the Or-Vnfm reference point.

Table 7.4.2-1: Recommendations related to VNF lifecycle management interface on the Or-Vnfm

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the VNF life cycle management interface on Or-Vnfm to support:		
Orvnfm.Lcm.001	Connecting/disconnecting a specific external connection point of a VNF instance to external Virtual Link.	Refer to the analysis in clauses 5.7.8 and 6.1. Related to Vnfm.Oam.002.
Orvnfm.Lcm.002	Informing/notifying about changes/failures of connectivity impacting the connectivity of the external connection points of a VNF instance to external Virtual Links.	Refer to the analysis in clauses 5.7.8 and 6.1. Related to Nfvo.Oam.009.

7.4.3 Reference point between NFVO and VIM (Or-Vi)

The present clause provides recommendations focusing on the definition and specification of interfaces on the Or-Vi reference point related to the management and connectivity of a multi-site service.

Table 7.4.3-1 provides the recommendations related to the virtualised network resource management interfaces on the Or-Vi reference point.

Table 7.4.3-1: Recommendations related to virtualised network resource management interface on the Or-Vi

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the virtualised network resource management interface on Or-Vi to support:		
Orvi.Vrm.001	Management of virtualised network resources for connectivity of the NFVI-PoP to / from WAN.	Refer to clause 6.1. Related to Vim.0am.001.
Orvi.Vrm.002	Update existing virtualised network resources within the NFVI-PoP to connect to a WAN virtualised network resource enabling connectivity to/from the WAN.	Refer to the analysis in clauses 5.4.8 and 6.1. Related to Vim.Oam.002.
Orvi.Vrm.003	Update existing virtualised network resource within the NFVI-PoP to reconnect from a WAN virtualised network resource to another WAN virtualised network resource	Refer to the analysis in clauses 5.8.8 and 6.1. Related to Vim.Oam.003.
Orvi.Vrm.004	Querying information about the association of the virtualised network resource within the NFVI-PoP with the internal-to-external NFVI-PoP interconnection.	Refer to the analysis in clause 6.4.5.2.2. Related to Vim.Oam.006.
Orvi.Vrm.005	Management of virtualised network resources for overlay or inter-AS connections to/from other NFVI-PoPs.	Refer to the analysis in clauses 5.2.8 and 6.1. Related to Vim.Oam.004.

Table 7.4.3-2 provides the recommendations related to the virtualised network resource capacity management interfaces on the Or-Vi reference point.

Table 7.4.3-2: Recommendations related to virtualised network resource capacity management interface on the Or-Vi

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the virtualised network resource capacity management interface on Or-Vi to support:		
Orvi.Vrcm.001	Providing information for the connectivity of the NFVI-PoP to/from external networks (e.g. WAN). See note.	Refer to the analysis in clause 6.4.5.3.2. Refer to Vim.Oam.005.
NOTE: This type of information is not typically associated with capacity, but currently the QueryNfviPoP operation is part of "virtualised network resource capacity management" interface in ETSI GS NFV-IFA 005 [i.7]. The recommendation is expected to be specified in the appropriate interface if enhancements are performed to ETSI GS NFV-IFA 005 [i.7].		

7.4.4 Reference point between NFVO and WIM

Table 7.4.4-1 provides the recommendations related to interface for virtualised resources management on the reference point between NFVO and WIM.

Table 7.4.4-1: Recommendations related to interface for virtualised network resource management on the reference point between NFVO and WIM

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the NFV-MANO virtualised resources management interface on the reference point between NFVO and WIM to support:		
Nfvowimif.Vnrm.001	Allocating virtualised network resources for WAN connectivity.	Refer to clauses 5.2.8 and 6.2.
Nfvowimif.Vnrm.002	Terminating virtualised network resources for WAN connectivity.	Refer to clauses 5.2.8 and 6.2.
Nfvowimif.Vnrm.003	Querying virtualised network resources for WAN connectivity.	Refer to clauses 5.2.8, 5.6 and 6.2.
Nfvowimif.Vnrm.004	Updating virtualised network resources for WAN connectivity.	Refer to clauses 5.12 and 6.2.

Table 7.4.4-2 provides the recommendations related to interface for fault management on the reference point between NFVO and WIM.

Table 7.4.4-2: Recommendations related to interface for fault management on the reference point between NFVO and WIM

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the NFV-MANO fault management interface on the reference point between NFVO and WIM to support:		
Nfvowimif.Fm.001	Notification of an alarm resulting from a connectivity fault.	Refer to clauses 5.7 and 6.2.
Nfvowimif.Fm.002	Notification of status change of an alarm.	Refer to clauses 5.7 and 6.2.

Table 7.4.4-3 provides the recommendations related to the virtualised network resource capacity management on the reference point between NFVO and WIM.

Table 7.4.4-3: Recommendations related to virtualised network resource capacity management on the reference point between NFVO and WIM

Identifier	Recommendation description	Comments and/or traceability
It is recommended that a requirement set be specified for the virtualised network resource capacity management interface on the reference point between NFVO and WIM to support:		
Nfvowimif.Vrcm.001	Querying information about the connectivity support on the WAN. See note.	Refer to analysis in clauses 6.2 and 6.4.5.3.2. Related to Wim.Oam.005.
NOTE: This type of information is not typically associated with capacity. The recommendation is expected to be specified in the appropriate interface should reuse of the enhancements made to NFV-IFA 005 occur.		

7.5 Descriptors and other information/data model artefacts

The present clause provides recommendations focusing on the definition and specification of descriptors and information model elements related to management and connectivity for multi-site services.

Table 7.5-1 provides the recommendations related to descriptors and other information/data model artefacts related to management and connectivity for multi-site services.

Table 7.5-1: Recommendations related to descriptors and information model aspects of management and connectivity for multi-site services

Identifier	Recommendation description	Comments and/or traceability
Nsd.001	It is recommended that a requirement is specified for the NSD to support description of the affinity/anti-affinity constraints for the NS VL to be instantiated across WAN.	Refer to analysis in clause 6.4.2.2.2. See note 1.
Nsd.002	It is recommended that a requirement is specified for the NSD to support the description of service availability level information for the NS VL to be instantiated across WAN.	Refer to analysis in clause 6.4.2.3.2. See note 1.
Vnfd.001	It is recommended that a requirement is specified for the VNFD to support the description of service availability level information for the internal VNF VL.	Refer to the analysis in clause 6.4.2.3.2. See note 2.
Vim.Im.001	It is recommended that a requirement is specified to support managing information about the connectivity of the NFVI-PoP to/from external networks (e.g. WAN). See note 3.	Refer to the analysis in clause 6.4.5.3.2. Related to Vim.Oam.005.
Vim.Im.002	It is recommended that a requirement is specified to support managing information about the association of the virtualised network resource within the NFVI-PoP with the internal-to-external NFVI-PoP interconnection. See note 4.	Refer to the analysis in clause 6.4.5.2.2. Related to Vim.Oam.006.
Wim.Im.001	It is recommended that a requirement is specified to support managing information about the connectivity support across the WAN. See note 5.	Refer to the analysis in clauses 5.7.8, 5.8.8, 6.1 and 6.4.5.2.2. Related to Wim.Oam.003.
Wim.Im.002	It is recommended that a requirement is specified to support managing information about the virtualised network resources on WAN. See note 6.	Refer to the analysis in clause 6.4.5.2.2. Related to Wim.Oam.003.
Nsd.Oam.001	Distinction between primary and secondary virtual links	Refer to clause 5.7.8.

NOTE 1: Existing requirements in the ETSI GS NFV-IFA 014 [i.12] might already fulfil the requirement, in which case the recommendation is to address the necessary extensions to the appropriate information elements.

NOTE 2: Existing requirements in the ETSI GS NFV-IFA 011 [i.10] might already fulfil the requirement, in which case the recommendation is to address the necessary extensions to the appropriate information elements.

NOTE 3: The various types of information include:
- network layering capabilities of the gateway;
- network type, port and interfaces to interconnect to external network;
- QoS support and bitrate of interfaces to external network; and
- network connectivity types supported.

NOTE 4: The existing VirtualNetwork information element can be extended including:
- Identification of the virtualised network resource.
- Connectivity to virtualised network resource external to the NFVI-PoP, further including:
  - Identification of the internal-to-external NFVI-PoP interconnection.
  - Type of internal-to-external NFVI-PoP interconnection.
  - Network connectivity type of the virtualised network resource on the WAN.
  - Network segment information of the virtualised network resource on the WAN.

NOTE 5: The various types of information include:
- the NFVI-PoP reachability over the WAN;
- network layering capabilities;
- the connectivity type(s) supported by the WAN;
- the support of differentiation of data flows from different VL;
- the QoS and bitrate supported by the WAN;
- support for traffic/data flows differentiation; and
- the capacity information of the WAN.

NOTE 6: The various types of information include:
- Identification of the WAN over which the virtualised network resource is instantiated.
- List of NFVI-PoP endpoints to which the virtualised network resource on the WAN connects to.
- Information for connecting the virtualised network resource to the NFVI-PoP endpoint.
- Connectivity properties of the virtualised network resource on the WAN, further including:
  - Network type;
  - Network connectivity type;
  - Network segment information; and
  - Connectivity topology information.

NOTE: Future enhancements to service availability level related functionality in NFV-MANO might create additional capabilities that may be beneficial to the management and connectivity for multi-site services. Utilization of such new capabilities is not addressed in the present document.

7.6 Recommendations related to Security

ETSI GS NFV-SEC 012 [i.37] defines requirements for host system elements on which sensitive workloads are to be run. It also defines requirements to ensure isolation of sensitive workloads from non-sensitive workloads sharing a platform. Moreover, it discusses a wide range of different technologies which aim to increase the security of a host system for the workloads which will be executing on it.

The present clause provides recommendations focusing on security aspects in alignment with Annex C of the present document. Table 7.6-1 provides the recommendations related to security. The present clause on recommendations related to security assumes that all entities are within one administrative domain.

Table 7.6-1: Recommendations related to Security

Identifier	Recommendation description	Comments and/or traceability
SEC.001	It is recommended that a requirement be defined for the system to provide means to ensure data integrity of any message (e.g. query, request, notification, fault information report).	See clause 7.3
SEC.002	It is recommended that a requirement be defined for the system to provide means to verify the identity and authenticity of the source of any message (e.g. query, request, notification, fault information report and resource information).	See clause 7.3
SEC.003	It is recommended that a requirement be defined for the system to provide means to verify the identity and authenticity of the consumer of any message (e.g. query, request, notification, fault information report and resource information).	See clause 7.3
SEC.004	It is recommended that a requirement be defined for the system to provide means to ensure that requests sent by unauthorized entities are discarded and that only requests sent by authorized entities are processed. Examples are a) request to deploy an NS instance across multiple sites, b) request to use an NS instance, c) request for LCM of an NS instance, d) request to access and receive the NSD.	
SEC.005	It is recommended that a requirement be defined for the system to raise an appropriate alarm in reaction to unauthorized access attempts.	
SEC.006	It is recommended that a requirement be defined to ensure the authenticity of the provider of an interface, e.g. the NS lifecycle operation granting interface.	
SEC.007	It is recommended that a requirement be specified to verify the identity and authenticity of the hosts/gateways associated with the desired sites (i.e. NFVI-PoP) across which the NS is to be deployed.	See clause 7.3
SEC.008	It is recommended that a requirement be specified to verify the identity and authenticity of the VNFC instances in multiple sites that will be part of the NS across multiple sites.	See clause 7.3
SEC.009	It is recommended that a requirement be defined for the system to provide means to ensure the confidentiality of any system message (e.g. query, request, notification, fault information report and resource information), i.e. to ensure it is not made available or disclosed to unauthorized entities.	See clause 7.3
SEC.010	It is recommended that a requirement be defined for the system to provide means to ensure that only authorized entities can take any action on the system (e.g. post queries, send requests, subscribe to receive notifications, provide and consume fault information report and resource information).	
SEC.011	It is recommended that a requirement be defined for the system to provide means to ensure non-repudiation of the act of having sent a message by a sender.	See clause 7.3
SEC.012	It is recommended that a requirement be defined for the system to provide means to prevent replay of any queries, requests, notification, fault information report or resource information.	See clause 7.3
SEC.013	It is recommended that a requirement be defined for timestamps to be issued by a trusted source of time.	

Identifier	Recommendation description	Comments and/or traceability
SEC.014	It is recommended that a requirement be defined for the system to ensure against the unauthorized access to connectivity control, and control over any resources and the related information.	See clause 7.3
SEC.015	It is recommended that a requirement be defined for the credentials used in the proof of identity (such as passwords, cryptographic keys, or key material) be properly secured by the sender and the receiver	
SEC.016	It is recommended that a requirement be defined for using a specific set of security best practices to be followed for all operations.	

8 Conclusion

The present document presents 13 use cases in the context of provisioning and managing of network services across multiple sites (i.e. NFVI-PoP) and WAN infrastructure. Based on the detailed analysis of these use cases, gaps have been identified with reference to the existing specifications and relevant recommendations have been proposed. These recommendations highlight the need to perform additional normative specification work and to update existing normative specification documents. The scope of analysis cover the following aspects:

1) Analysis of the role of the WIM to establish connectivity between different NFVI-PoPs.

2) Potential architectural options for the placement of WIM functional entity within the NFV-MANO architecture highlighting the need to enhancing the NFV-MANO descriptors, reference points and functional blocks.

3) Information modeling analysis to highlight the gaps with respect to the NFV information model, including design time information, i.e. NS and VNF descriptors, as well as runtime information, e.g. virtualised resource information.

Based on the above scope of analysis, recommendations have been derived that are grouped in the following four categories:

1) General recommendations focusing on higher-level and framework aspects.

2) Recommendations focusing on functional aspects of functional blocks identified in the NFV Architectural Framework.

3) Recommendations focusing on the definition and specification of interfaces on the Os-Ma-nfvo, Or-Vnfm, Or-Vi reference points and the reference point between WIM and NFVO for the management and connectivity of a multi-site service.

4) Recommendations focusing on the definition and specification of descriptors and information model elements related to management and connectivity for multi-site services.

The proposed recommendations encompass the identification of potential new requirements, which should form the basis of the developing a new normative specification, while filling the gaps in the existing ones.

Finally a set of recommendations related to security aspects were derived from the analysis and included in Annex C.

Annex A:
A collection of variants of multi-site NS deployment

A.1 Introduction

Use case #1 in clause 5.2 describes multi-site NS deployment, and shows two possible base flows. Multi-Site NS deployment can be realized by various forms of underlying network technologies. In order to derive appropriate potential requirements for the NFV-MANO to interact with the underlying network technologies in a common manner, this annex provides concrete examples of such technologies, and illustrates how they would work with the NFV-MANO to deploy an NS between sites across WAN.

A.2 L2 WAN connectivity

A.2.1 Case 1: Extending a VLAN network across WAN

A.2.1.1 Overview

In this case, WIM provides L2 connectivity service which connects two or more sites transparently. There are several technologies to establish L2 WAN connectivity (e.g. L2-VPN using MPLS), and this case is not limited to a particular technology. However, this case assumes that VLAN (IEEE 802.1q [i.39]) is used for interfaces between the WAN and an NFVI-PoP to establish NFVI-PoP connectivity shown in clause 5.2.8.

Figure A.2.1.1-1 shows an overview of extending a VLAN network across WAN. The WIM allocates a virtualised network resource #2 which the WAN connectivity is mapped to. In this case, VLAN ID=$\boldsymbol{id_2}$ is assigned to access the WAN connectivity, that is, Ethernet frames transferred between a network gateway and a PE node are tagged with the VLAN ID= $\boldsymbol{id_2}$. The VIMs allocate virtualised network resources within a NFVI-PoP. The virtualised network resources are also mapped to a VLAN network, which in this case VLAN ID= $\boldsymbol{id_1}$ for NFVI-PoP#1 and VLAN ID= $\boldsymbol{id_3}$ for NFVI-PoP#2. To properly interconnect the virtualised network resource at the WAN and the virtualised network resources at the NFVI-PoPs, the VIMs configure the network gateways such that the network gateways can translate the VLAN ID of incoming/outgoing Ethernet frames. For example, the network gateway at NFVI-PoP#1 translates the VLAN ID of incoming traffic from $\boldsymbol{id_2}$ to $\boldsymbol{id_1}$. Similarly, the network gateway at NFVI-PoP#1 translates the VLAN ID of outgoing traffic from $\boldsymbol{id_1}$ to $\boldsymbol{id_2}$.

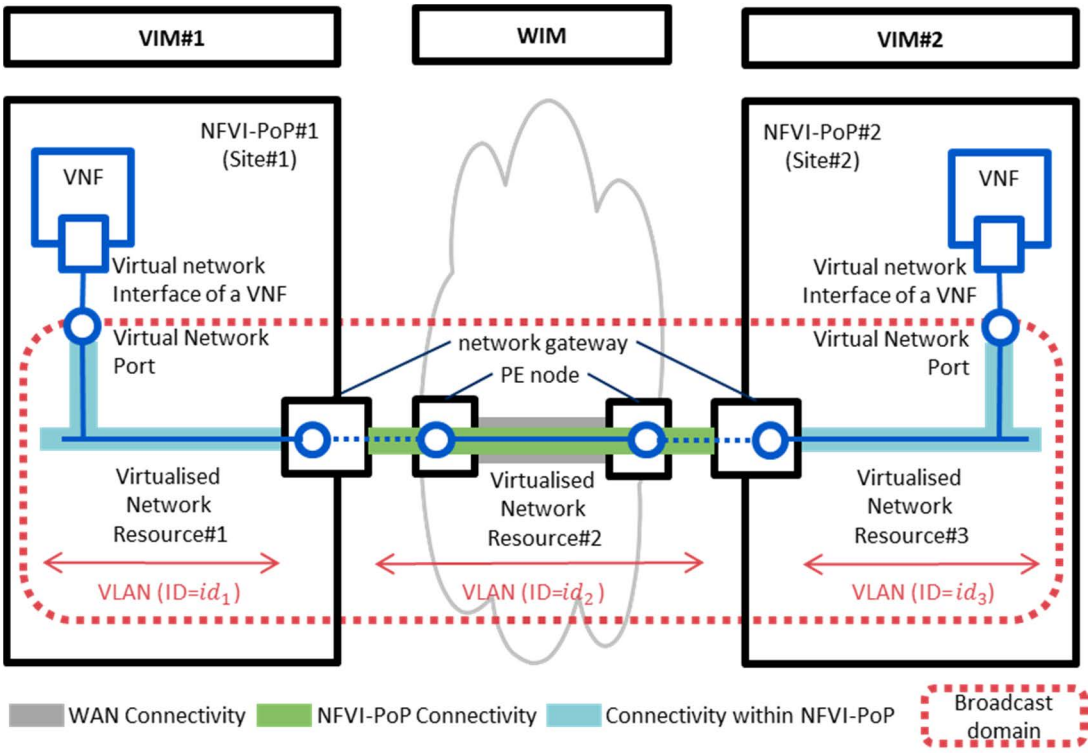

Figure A.2.1.1-1: Overview of extending a VLAN network across WAN

A.2.1.2 Properties of virtual network resources

The virtualised network resources at WAN, NFVI-PoP#1 and NFVI-PoP#2 are characterized as shown in Table A.2.1.2-1. These properties are exchanged between NFVO and WIM/VIM through the Or-Vi reference point.

Table A.2.1.2-1: Properties of virtualised network resources

Virtualised Network Resource	Attribute	Example Value	Description
@WAN	Connectivity type	Ethernet and Mesh	See ConnectivityType information element in clause 6.5.3 in ETSI GS NFV-IFA 014 [i.12].
	Network type of WAN connectivity	l2-vpn	The type of network of the WAN connectivity that maps to the virtualised network. In this case, it is L2-VPN using MPLS. See also attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].
	Network type of NFVI-PoP connectivity	vlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].
	Segment type	***id₂***	vlan identifier. See also attribute segmentType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].
	Is shared	False	This attribute represents whether the network is shareable (for aggregation). In this case, the network is not shareable. See also attribute isShared of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].

Virtualised Network Resource	Attribute	Example Value	Description
@NFVI-PoP#1	Network type	vlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].
	Segment type	***id₁***	vlan identifier. See also attribute segmentType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].
@NFVI-PoP#2	Network type	vlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].
	Segment type	***id₃***	vlan identifier. See also attribute segmentType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].

A.2.1.3 Operational flow

Table A.2.1.3-1 shows the operational flow for this case. It follows BF#1.1 of use case #1 in clause 5.2, so Table A.2.1.3-1 shows only additional description specific for this case.

Table A.2.1.3-1: Operational flow (based on BF#1.1 of use case #1)

#	Flow	Description
1	OSS/BSS -> NFVO	See step 1 of BF#1.1 of use case #1 in clause 5.2.
2	NFVO	See step 2 of BF#1.1 of use case #1 in clause 5.2.
3	NFVO ->WIM	See step 3 of BF#1.1 of use case #1 in clause 5.2. In this case, the following information is passed to the WIM; • NFVI-PoPs to be connected: NFVI-PoP#1 and NFVI-PoP#2; • Connectivity type: Ethernet and Mesh; • Is shared: False; and • QoS and bandwidth information.
4	WIM -> Network Controller	See step 4 to 6 of BF#1.1 of use case #1 in clause 5.2. L2 WAN connectivity between the PE nodes at WAN is established for the virtualised network resource#2. Then, NFVI-PoP connectivity is prepared so that the L2 WAN network connectivity is accessible with VLAN ID= ***id₂*** from the NFVI-PoPs.
5	Network Controller	
6	Network Controller -> WIM	
7	WIM -> NFVO	See step 7 of BF#1.1 of use case #1 in clause 5.2. The WIM returns an indication of the network port of the WAN and VLAN ID= ***id₂*** as information for connecting to the WAN.
8	NFVO -> VIM at Site#1	See step 8 of BF#1.1 of use case #1 in clause 5.2. In this case, the following information is passed to the VIM: • Information for connecting to the WAN: an indication of the network port of the WAN and VLAN ID= ***id₂***; and • QoS and bandwidth information.
9	VIM at Site#1	See step 9 of BF#1.1 of use case #1 in clause 5.2. According to the input parameters at step 8, the VIM creates the virtualised network resource#1. A VLAN network is established for the virtualised network resource#1. The VLAN ID of the network is ***id₁***. The network gateway is configured for VLAN ID translation, i.e. the VLAN ID of incoming traffic is translated from ***id₂*** to ***id₁***, and the VLAN ID of outgoing traffic is translated from ***id₁*** to ***id₂***.
10	VIM at Site#1 -> NFVO	See step 10 of BF#1.1 of use case #1 in clause 5.2. The VIM returns the identifier of the virtualised network resource. The identifier will be used to attach virtual network ports to be connected with a virtual network interface of a VNF.
11	NFVO -> VIM at Site#2	See step 11 of BF#1.1 of use case #1 in clause 5.2. In this case, the following information is passed to the VIM: • Information for connecting to the WAN: an indication of the network port of the WAN and VLAN ID= ***id₂***; and • QoS and bandwidth information.

#	Flow	Description
12	VIM at Site#2	See step 12 of BF#1.1 of use case #1 in clause 5.2. According to the input parameters at step 11, The VIM creates the virtualised network resource#3. A VLAN network is established for the virtualised network resource#3. The VLAN ID of the network is ***id₃***. The network gateway is configured for VLAN ID translation, i.e. the VLAN ID of incoming traffic is translated from ***id₂*** to ***id₃***, and the VLAN ID of outgoing traffic is translated from ***id₃*** to ***id₂***.
13	VIM at Site#2 -> NFVO	See step 13 of BF#1.1 of use case #1 in clause 5.2. The VIM returns the identifier of the virtualised network resource. The identifier will be used to attach virtual network ports to be connected with a virtual network interface of a VNF.
14	NFVO	See step 14 of BF#1.1 of use case #1 in clause 5.2.
15	NFVO -> OSS/BSS	See step 15 of BF#1.1 of use case #1 in clause 5.2.

A.2.1.4 Considerations

A.2.1.4.1 Distributed control and centralized control in VLAN ID assignment

In this case, each of the VIMs and the WIM independently assigns VLAN ID to virtualised network resources. As a result, VLAN IDs of the virtualised network resources for a Virtual Link can be different from each other. Alternatively, it is also possible that NFVO manages a pool of VLAN IDs which are commonly used among multiple NFVI-PoPs and a WAN, and assigns a single VLAN ID to the virtual network resources for a Virtual Link. In that case, the NFVO sends the VLAN ID selected by the NFVO for a Virtual Link to the WIM and the VIMs at step 3, 8 and 11 in Table A.2.1.3-1 respectively.

A.2.1.4.2 Supporting L3 connectivity services

It is possible to enable L3 connectivity services such as DHCP on a Virtual Link which is instantiated according to the operational flow shown in Table A.2.1.3-1 in clause A.2.1.3. To enable it, additional steps are necessary for VIM#1 and VIM#2 to create a virtualised sub-network and associate it with the virtualised network resource created at step 9 or 12 of the operational flow. As described in clause 8.4.5.3 in ETSI GS NFV-IFA 005 [i.7], the virtualised sub-network is used to specify properties for L3 connectivity services. Since the virtualised network resources at VIM#1 and VIM#2 belong to the same broadcast domain, the L3 related parameters of the virtualised sub-networks need to be the same between VIM#1 and VIM#2.

If DHCP is enabled, it needs to assign IP addresses without overlapping between the two sites. It is FFS how to achieve it.

A.2.2 Case 2: EVPN connection with Inter-AS among NFVI-PoPs

A.2.2.1 Overview

In this use case, the network of NFVI-PoP and WAN provide EVPN-VXLAN- and EVPN-MPLS (Ethernet VPN), respectively. The NFVI-PoPs and WAN are connected by the Inter-AS option B as described in the IETF RFC 4364 [i.14] and are managed by independent domains. The EVPN, which is standardized in IETF RFC 7432 [i.20], can advertise information of L2 (MAC) and L3 (IP) through Multiprotocol BGP (MP-BGP). The EVPN has many benefits for efficiency, reliability, scalability, etc. on network operations. In addition, The MPLS-based network provides standard-based management tools and technologies, namely MPLS Operations, Administration and Maintenance (MPLS-OAM), traffic management, and QoS. By using the EVPN connection, the VNFs can communicate to each other within the same L2 broadcast domain across WAN.

Figure A.2.2.1-1 shows an overview of EVPN connection with Inter-AS option B among the NFVI-PoPs across WAN. In this case, The NFVI-PoP#1, NFVI-PoP#2 and WAN belong to different administrative domains. The network gateway#1 and #2 show ASBR for connecting ASes. The Ethernet frames which are sent from VNF#1 are labelled by RD which is part of destination network address, namely ***id₁***, and encapsulated by VXLAN header, namely ***id₄*** to isolate from other networks within NFVI-PoP#1. At the network gateway at NFVI-PoP#1, VPN information are exchanged from NFVI-PoP#1 domain to WAN domain by using external BGP (e-BGP). Then RD is re-labelled from ***id₁*** to ***id₂*** and re-encapsulated by MPLS header. Then VPN packets are transferred to NFVI-PoP#2 domain following target RT information at WAN. And at the network gateway at NFVI-PoP#2, VPN-information are distributed from WAN to NFVI-PoP#2 by using e-BGP. Then RD is re-labelled from ***id₂*** to ***id₃***, and re-encapsulated by VXLAN header, namely ***id₅***. As a result, VNF#1 of NFVI-PoP#1 and VNF#2 of NFVI-PoP#2 can communicate with each other.

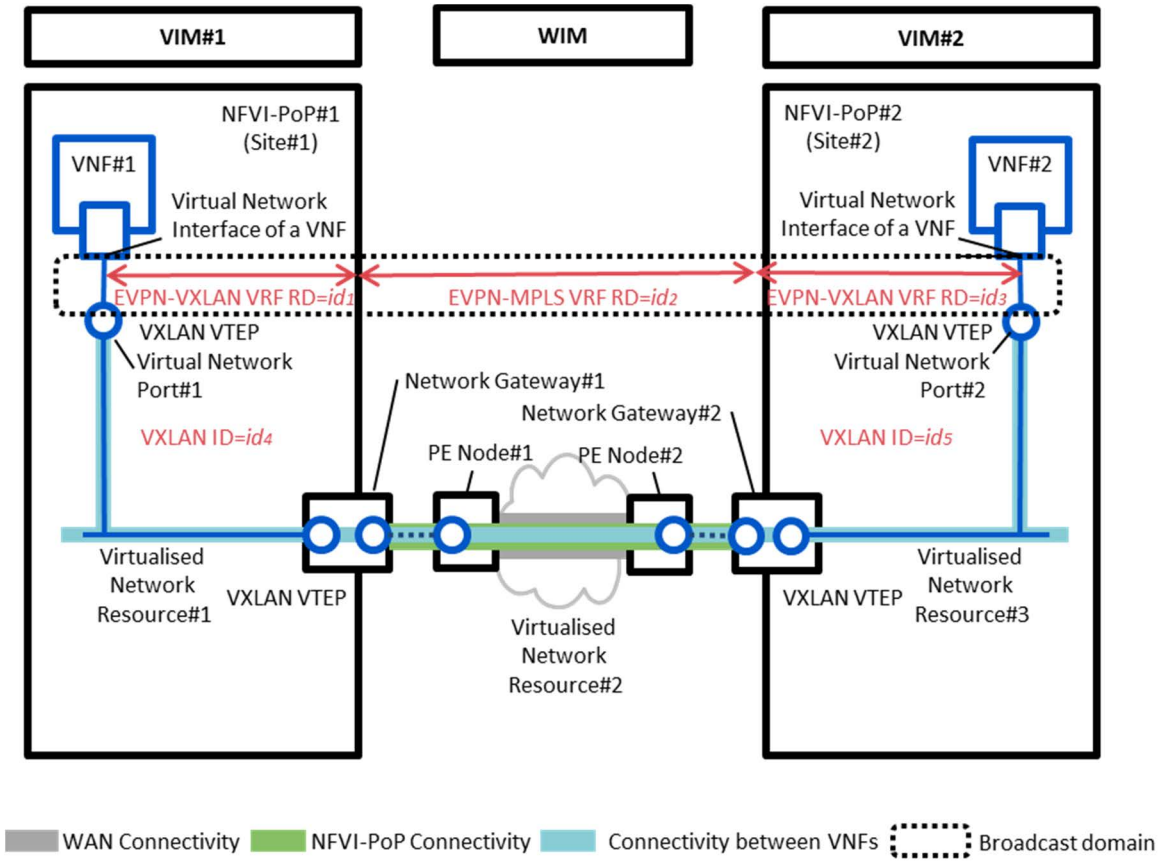

Figure A.2.2.1-1: Overview of EVPN connection with Inter-AS among NFVI-PoPs

A.2.2.2 Properties of virtual network resources

The virtualised network resources at WAN, NFVI-PoP#1 and NFVI-PoP#2 are characterized as shown in the Table A.2.2.2-1. These properties are exchanged between NFVO and WIM/VIM through the Or-Vi reference point.

Table A.2.2.2-1: Properties of virtualised network resources

Virtualised Network Resource	Attribute	Example Value	Description
@WAN	Connectivity type	MPLS and Mesh	See connectivityType information element of the Network Service Virtual Link Descriptor in clause 6.5.3 of ETSI GS NFV-IFA 014 [i.12].
	Network type (for WAN connectivity)	l2-vpn	The type of network for the WAN connectivity that maps to the virtualised network. In this example, it is Ethernet over MPLS. For details, see attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].

Virtualised Network Resource	Attribute	Example Value	Description
	Network type (for NFVI-PoP connectivity)	evpn-mpls	The type of network for the NFVI-PoP connectivity that maps to the virtualised network. In this example, it is EVPN-MPLS. See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Segment type (for NFVI-PoP connectivity)	***id₂***	This attribute indicates VRF RD for EVPN-MPLS at WAN. This attributes provided by WIM and is unchangeable from NFVO. IP packets through MPLS-VPN are encapsulated by VRF-RD. See also attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Is shared	True	This attribute indicates whether the network is shareable (for aggregation among Virtual Links) or not. In this use case, the network is shareable. See also the attribute isShared of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
@NFVI-PoP#1	Network type (for connectivity within NFVI-PoP)	vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Segment type (for connectivity within NFVI-PoP)	***id₄***	This attribute indicates VXLAN ID within NFVI-PoP #1. This attributes provided by VIM#1 and is unchangeable from NFVO. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].
	Network type (for NFVI-PoP connectivity)	evpn-vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Segment type (for NFVI-PoP connectivity)	***id₁***	This attribute indicates VRF RD for EVPN-VXLAN at Site#1. This attributes provided by VIM and is unchangeable from NFVO. IP packets through VXLAN-VPN are encapsulated by VRF-RD. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].
@NFVI-PoP#2	Network type (for connectivity within NFVI-PoP)	vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Segment type (for connectivity within NFVI-PoP)	***id₅***	This attribute indicates VXLAN ID within NFVI-PoP #2. This attributes provided by VIM#2 and is unchangeable from NFVO. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Network type (for NFVI-PoP connectivity)	evpn-vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Segment type (for NFVI-PoP connectivity)	***id₃***	This attribute indicates VRF RD for EVPN-VXLAN at Site#2. This attributes provided by VIM and is unchangeable from NFVO. See attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].

A.2.2.3 Operational flow

Table A.2.2.3-1 shows the operational flow for this case. It follows BF#1.2 of use case #1 in clause 5.2, so that Table A.2.2.3-1 shows only additional descriptions specific to this use case.

Table A.2.2.3-1: Operational flow (based on BF#1.2 of use case #1)

#	Flow	Description
1	OSS/BSS -> NFVO	See step 1 of BF#1.2 for use case #1 in clause 5.2.
2	NFVO	See step 2 of BF#1.2 for use case #1 in clause 5.2.
3	NFVO ->WIM	See step 3 of BF#1.2 for use case #1 in clause 5.2. See note. In this case, the following attributes are provided to the WIM: • Connectivity type: MPLS and Mesh; • NFVI-PoPs to be connected: NFVI-PoP#1 and NFVI-PoP#2; • Network type for WAN connectivity: l2-vpn; • Network type for NFVI-PoP connectivity: evpn-mpls; • Is shared: True; and • QoS and bandwidth information.
4	WIM -> Network Controller	See step 4 to 6 of BF#1.2 for use case #1 in clause 5.2. See note. EVPN-MPLS between the PE node#1 and PE node#2 is established as virtualised network resource#2.The WIM allocates VRF RD for the EVPN-MPLS, namely ***id₂*** to itself.
5	Network Controller	
6	Network Controller -> WIM	
7	WIM -> NFVO	See step 7 of BF#1.2 of use case #1 in clause 5.2. The WIM returns an identifier of virtualised network resource#2 and VRF RD, namely ***id₂***.
8	NFVO -> VIM#1	See step 8 of BF#1.2 for use case #1 in clause 5.2. In this case, the following attributes are provided to the VIM#1: • Network type for connectivity within NFVI-PoP: vxlan; • Network type for NFVI-PoP connectivity: evpn-vxlan.
9	VIM#1	See step 9 of BF#1.2 for use case #1 in clause 5.2. According to the attributes of step 8, the VIM#1 creates EVPN-VXLAN as the virtualised network resource#1. The VIM#1 configures ***id₁*** to its own VRF RD.
10	VIM#1 -> NFVO	See step 10 of BF#1.2 for use case #1 in clause 5.2. The VIM#1 returns identifiers of the virtualised network resource #1 and VRF RD, namely ***id₁***.
11	NFVO -> VIM#2	See step 11 of BF#1.2 for use case #1 in clause 5.2. In this case, the following attributes are provided to the VIM#2: • Network type for connectivity within NFVI-PoP: vxlan; • Network type for NFVI-PoP connectivity: evpn-vxlan.
12	VIM#2	See step 12 of BF#1.2 for use case #1 in clause 5.2. According to the attributes of step 11, the VIM#2 creates EVPN-VXLAN as the virtualised network resource#3. The VIM#2 configures ***id₃*** to its own VRF RD.
13	VIM#2 -> NFVO	See step 13 of BF#1.2 for use case #1 in clause 5.2. The VIM#2 returns identifiers of the virtualised network resource#3 and VRF RD, namely ***id₃***.
14	NFVO ->WIM	See step 14 of BF#1.2 for use case #1 in clause 5.2. In this case, the following attributes are provided to the WIM; • Information for connecting to virtualised network resource #1: ***id₁;*** and • Information for connecting to virtualised network resource #3: ***id₃***.
15	WIM -> Network Controller	See step 15 of BF#1.2 for use case #1 in clause 5.2.
16	Network Controller	See step 16 of BF#1.2 for use case #1 in clause 5.2. The WIM adds ***id₁*** and ***id₃*** to the import RT list at the PE node#1 and the PE node#2.
17	Network Controller -> WIM	See step 17 of BF#1.2 for use case #1 in clause 5.2.
18	WIM -> NFVO	See step 18 of BF#1.2 for use case #1 in clause 5.2.
19	NFVO -> VIM #1	See step 19 of BF#1.2 for use case #1 in clause 5.2. In this case, the following attributes are provided to the VIM#1: • Information for connecting to virtualised network resource #3: ***id₃.***
20	VIM #1	See step 20 of BF#1.2 for use case #1 in clause 5.2. The VIM#1 adds ***id₃*** to the import RT list at the network gateway#1.
21	VIM #1 -> NFVO	See step 21 of BF#1.2 for use case #1 in clause 5.2.
22	NFVO -> VIM#2	See step 22 of BF#1.2 for use case #1 in clause 5.2. In this case, the following attributes are provided to the VIM#2: • Information for connecting to virtualised network resource #1: ***id₁.***
23	VIM #2	See step 23 of BF#1.2 for use case #1 in clause 5.2. The VIM#2 adds ***id₁*** to the import RT list at the network gateway#2.
24	VIM #2 -> NFVO	See step 24 of BF#1.2 for use case #1 in clause 5.2.
25	NFVO	See step 25 of BF#1.2 for use case #1 in clause 5.2.
26	NFVO -> OSS/BSS	See step 26 of BF#1.2 for use case #1 in clause 5.2.
NOTE: Once a L2-VPN is established, the establishment of a virtualised network resource and allocation of VRF RD at steps from step 3 to step 7 can be skipped when allocating other Virtual Links between the NFVI-PoPs.		

A.3 L3 WAN connectivity

A.3.1 Case 1: VXLAN connection over L3 WAN connectivity between NFVI-PoPs

A.3.1.1 Overview

In this case, L3-VPN at WAN is used to provide an IP based underlying network among two or more NFVI-PoPs, and overlay tunnels with VXLAN are created over the underlying network to provide L2 connectivity for Virtual Links. It is supposed that the L3-VPN autonomously manages traffic engineering according to QoS and bandwidth requirements from the NFV-MANO, and exchanges the routing information of each NFVI-PoP by using BGP or Open Shortest Path First (OSPF).

The VXLAN creates L2-based broadcast domains for Virtual Links and allows NFV-MANO to specify IP addresses to the VNFs independently from the address spaces of the underlying network. There are several options in terms of end points of VXLAN based overlay networks; i.e. the location of VTEPs. In this case, the VTEPs are placed on vSwitches on hosts and VXLAN based overlay networks are terminated at virtual network ports connected to the virtual network interfaces of the VNFs.

Figure A.3.1.1-1 shows an overview of a VXLAN connection over L3 WAN connectivity between two NFVI-PoPs.

The WIM creates an L3-VPN between NFVI-PoP#1 and NFVI-PoP#2. In this case, the WIM is responsible for IP address assignment for the network between the network gateway of NFVI-PoP and a PE node of the WAN. That is, when establishing an L3-VPN, the WIM generates IP addresses for external ports of the network gateways and the PE nodes and then passes these IP addresses to the VIM#1 and the VIM#2 to properly configure the addresses and routing information (i.e. next-hop) of the network gateways. In this specific example, the WIM assigns 172.16.1.2/24 and 172.16.2.2/24 to the external ports of the network gateways #1 and #2 and 172.16.1.1/24 and 172.16.2.1/24 to the PE nodes #1 and #2, respectively. In the NFVI-PoPs, 192.168.1.1/24 and 192.168.2.1/24 are statically allocated to the internal ports of the network gateways respectively. When establishing a VXLAN connection, the VIMs assign IP addresses to virtual network ports for VXLAN VTEPs. In this specific example, the VIMs assign 192.168.1.2/24 and 192.168.2.2/24 to the virtual network ports #1 and #2, respectively. Then the VIM#1 and VIM#2 configure VXLAN VTEPs on virtual network port#1 and #2 to provide L2 connectivity (ID= $\boldsymbol{id_1}$) for VNFs in NFVI-PoP#1 and NFVI-PoP#2. As a result, NFV-MANO can assign the IP addresses to virtual network interfaces of the VNFs according to the NSD, in this specific example, 10.10.0.1/24 and 10.10.0.2/24 are assigned to virtual network interafaces#1 and #2 respectively.

When the VNF#1 sends Ethernet frames to the VNF#2, these frames are encapsulated with the VXLAN headers and outer IP/UDP headers by virtual network port#1. The destination address of the outer IP header is set to the IP address of peered virtual network port#2 (i.e. 192.168.2.2). Then the IP packets are delivered to virtual network port#2 over the IP based underlying network. The VXLAN header and outer IP/UDP headers of the IP packets are removed by virtual network port#2 and then the unwrapped Ethernet frames are forwarded to the VNF#2.

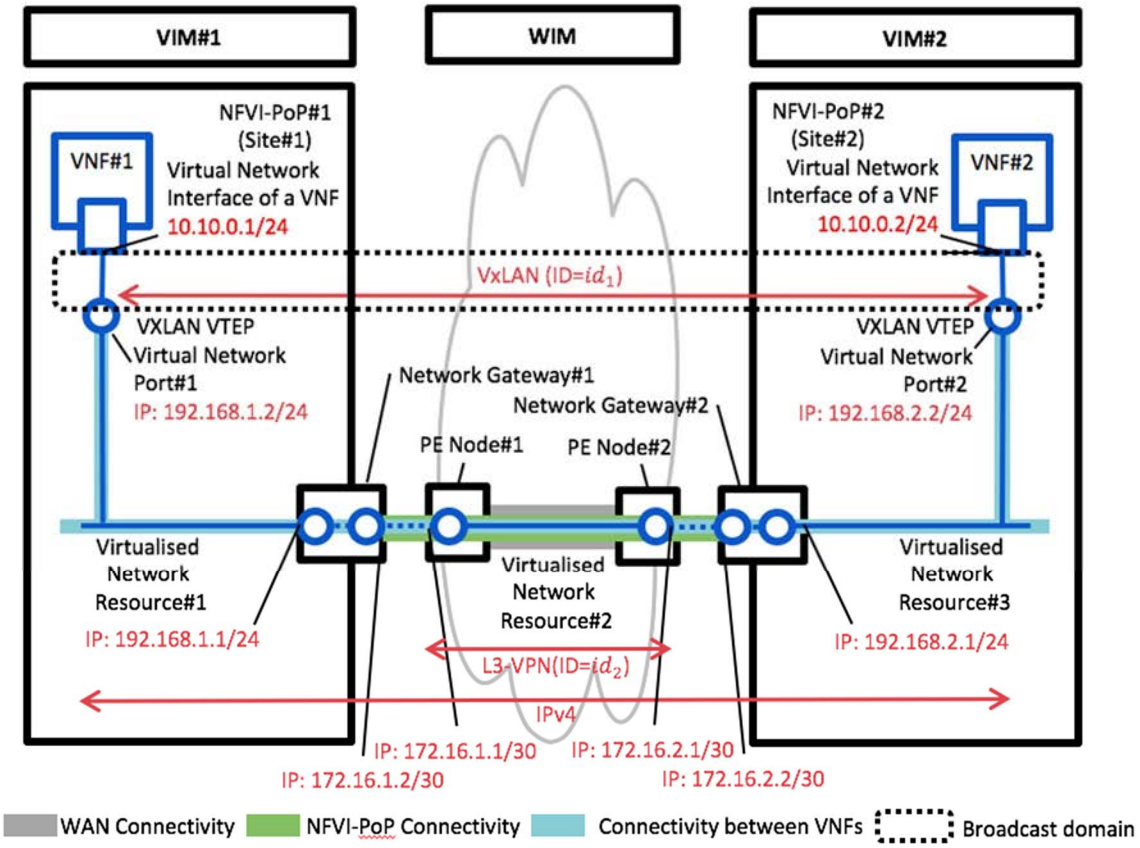

Figure A.3.1.1-1: Overview of VXLAN connection between NFVI-PoPs over L3 WAN connectivity

A.3.1.2 Properties of virtual network resources

The virtualised network resources at WAN, NFVI-PoP#1 and NFVI-PoP#2 are characterized as shown in Table A.3.1.2-1. These properties are exchanged between NFVO and WIM/VIM through the Or-Vi reference point.

Table A.3.1.2-1: Properties of virtualised network resources

Virtualised Network Resource	Attribute	Example Value	Description
@WAN	Connectivity type	IPv4 and Mesh	See connectivityType information element of the Network Service Virtual Link Descriptor in clause 6.5.3 of ETSI GS NFV-IFA 014 [i.12].
	Network type (for WAN connectivity)	l3-vpn	The type of network for the WAN connectivity maps to the virtualised network. In this example, it is L3-VPN using MPLS. For details, see attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Network type (for NFVI-PoP connectivity)	IPv4	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Segment type (for NFVI-PoP connectivity)	none	See also attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Is shared	True	This attribute indicates whether the network is shareable (for aggregation among Virtual Links) or not. In this use case, the network is shareable. See also the attribute isShared of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].

Virtualised Network Resource	Attribute	Example Value	Description
@NFVI-PoP#1	Network type	vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Segment type	id_1	VXLAN network Identifier. See also attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 in ETSI GS NFV-IFA 005 [i.7].
	scope	multi-site	The scope of the area which the network covered. "multi-site" means this network is extended to other sites.
@NFVI-PoP#2	Network type	vxlan	See attribute networkType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	Segment type	id_1	VXLAN network Identifier. See also attribute segmenetType of the VirtualNetwork information element in clause 8.4.5.2 of ETSI GS NFV-IFA 005 [i.7].
	scope	multi-site	The scope of the area which the network covered. "multi-site" means this network is extended to other sites.

A.3.1.3 Operational flow

Table A.3.1.3-1 shows the operational flow for this case. It follows BF#1.3 of use case #1 in clause 5.2, so Table A.3.1.3-1 shows only additional description specific for this case.

Table A.3.1.3-1: Operational flow (based on BF#1.3 of use case #1)

#	Flow	Description
1	OSS/BSS -> NFVO	See step 1 of BF#1.3 for use case #1 in clause 5.2.
2	NFVO	See step 2 of BF#1.3 for use case #1 in clause 5.2. NFVO decides to create the VXLAN and selects an identifier of VXLAN (ID= ***id₁***) for connecting VNFs at NFVI-PoP#1 and NFVI-PoP#2.
3	NFVO ->WIM	See step 3 of BF#1.3 for use case #1 in clause 5.2. See note 1. In this case, the following attributes are provided to the WIM: • Connectivity type: IPv4 and Mesh; • NFVI-PoPs to be connected: NFVI-PoP#1 and NFVI-PoP#2; • Network type for WAN connectivity: l3-vpn; • Network type for NFVI-PoP connectivity: IPv4; • Is shared: True; and • QoS and bandwidth information.
4	WIM -> Network Controller	See step 4 to 6 of BF#1.3 for use case #1 in clause 5.2. See note 1. L3-VPN between the PE node#1 and PE node#2 is established as virtualised network resource#2. The WIM allocates IP addresses, namely 172.16.1.1/24 and 172.16.2.1/24 to the PE node#1 and PE node#2. It also selects IP addresses, namely 172.16.1.2/24 and 172.16.2.2/24 to be assigned to the external port of the network gateways of NFVI-PoP#1 and NFVI-PoP#2, respectively.
5	Network Controller	
6	Network Controller -> WIM	
7	WIM -> NFVO	See step 7 of BF#1.3 for use case #1 in clause 5.2. See note 1. The WIM replies an identifier of virtual network resource#2 and IP addresses, namely 172.16.1.2/24 and 172.16.2.2/24, to be assigned to the external ports of the network gateways. It also replies IP addresses of the PE nodes, namely 172.16.1.1/24 and 172.16.2.1/24.
8	NFVO -> VIM#1	See step 8 of BF#1.3 for use case #1 in clause 5.2. In this case, the following attributes are provided to the VIM#1: • Information for connecting to the WAN: 172.16.1.2/24 to be assigned to the external port of the network gateway#1 and 172.16.1.1/24 of the PE node#1 for configuring a next-hop of the network gateway#1; • Network type for NFVI-PoP: vxlan; • Scope: multi-site; and • QoS and bandwidth information.
9	VIM#1	See step 9 of BF#1.3 for use case #1 in clause 5.2. According to the attributes of step 8, the VIM#1 creates the virtualised network resource#1. The VIM#1 allocates the specified IP address, namely 172.16.1.2/24 to the external port of the network gateway#1 and adds a next hop (i.e. 172.16.1.1/24) to the routing table of the network gateway#1. The VIM#1 also allocates an IP address, namely 192.168.1.2/24 to the virtual network port#1 for VXLAN VTEP.

#	Flow	Description
10	VIM#1 -> NFVO	See step 10 of BF#1.3 for use case #1 in clause 5.2. The VIM#1 returns identifiers of the virtualised network resource#1 and IP address of the virtual network port#1, namely 192.168.1.2/24.
11	NFVO -> VIM#2	See step 11 of BF#1.3 for use case #1 in clause 5.2. In this case, the following attributes are provided to the VIM#2: • Information for connecting to the WAN: 172.16.2.2/24 to be assigned to the external port of the network gateway#2 and 172.16.2.1/24 of the PE node#2 for configuring a next-hop of the network gateway#2; • Network type for NFVI-PoP: vxlan; • Scope: multi-site; and • QoS and bandwidth information.
12	VIM#2	See step 12 of BF#1.3 for use case #1 in clause 5.2. According to the attributes of step 11, the VIM#2 creates the virtualised network resource#2. The VIM#2 allocates the specified IP address, namely 172.16.2.2/24 to the external port of the network gateway#2 and adds a next hop (i.e. 172.16.2.1/24) to the routing table of the network gateway#2. The VIM#2 also allocates an IP address, namely 192.168.2.2/24 to the virtual network port#2 for VXLAN VTEP.
13	VIM#2 -> NFVO	See step 13 of BF#1.3 for use case #1 in clause 5.2. The VIM#2 returns identifiers of the virtualised network resource and IP address of virtual network port#2, namely 192.168.2.2/24.
14	NFVO -> VIM#1	See step 14 of BF#1.3 for use case #1 in clause 5.2. In this case, the following attributes are provided to the VIM#1: • Segment type for NFVI-PoP: id_1; and • VTEP address of NFVI-PoP#2 obtained at step 13: 192.168.2.2/24. See note 2.
15	VIM#1	See step 15 of BF#1.3 for use case #1 in clause 5.2. According to the attributes of step 14, the VIM#1 configures VTEP at the virtual network port#1 (ID = id_1 and the destination address= 192.168.2.2/24).
16	VIM#1 -> NFVO	See step 16 of BF#1.3 for use case #1 in clause 5.2.
17	NFVO -> VIM#2	See step 17 of BF#1.3 for use case #1 in clause 5.2. In this case, the following attributes are provided to the VIM#2: • Segment type for NFVI-PoP: id_1; and • VTEP address of NFVI-PoP#1 obtained at step 10: 192.168.1.2/24. See note 2.
18	VIM#2	See step 18 of BF#1.3 for use case #1 in clause 5.2. According to the attributes of step 17, the VIM#2 configures VTEP at the virtual network port#2 (ID = id_1 and the destination address = 192.168.1.2/24).
19	VIM at Site#2 -> NFVO	See step 19 of BF#1.3 for use case #1 in clause 5.2.
20	NFVO	See step 20 of BF#1.3 for use case #1 in clause 5.2.
21	NFVO -> OSS/BSS	See step 21 of BF#1.3 for use case #1 in clause 5.2.
NOTE 1: Once a L3-VPN is established, the steps from step 3 to step 7 can be skipped when allocating other Virtual Links between the NFVI-PoPs. NOTE 2: The VXLAN has several options like unicast mode/multicast mode/ BGP control plane to exchange addresses of VTEPs. In this case, it is assumed that the VXLAN uses unicast mode.		

Annex B:
Gap analysis between WIM and Network Controller

B.1 Introduction

This annex is presented to analyse the gaps between WIM and Network Controller. In view of the liaison relationship of ETSI-NFV with ONF and OIF, this annex will highlight the gaps with reference to the Transport SDN as defined in ONF and OIF and use it as an example of Network Controller for the gap analysis. Note that a particular type of network infrastructure and the detail of the fulfilment are out of scope in the scope of the present document and of ETSI-NFV.

B.2 Recap on Analysis of SDN across multiple VIMs

"Report on SDN Usage in NFV Architectural Framework" [i.3] discussed deployment option of a Network Controller with SDN features across multiple VIMs. In the context, "SDN across multiple VIMs in different NFVI-PoPs" in the clause 5.3.4.2 of [i.3] showed multiple options about how NFVO and WAN infrastructure are interfaced with each other.

The simplest case is a static model where a pre-allocated static WAN connectivity service (e.g. E-Line, E-LAN, IP/MPLS VPN) is established between multiple termination points located at geographically remote NFVI-PoPs. The model is analysed that it does not require coordination between NFVI-PoP and WAN resources, but also limited in the sense that the WAN resources do not follow agility and dynamism of the NFVI-PoP network environment.

Another case is an on-demand model where VNFs are deployed across at multiple NFVI-PoP locations - NFVI-PoP and WAN belong to a common trust domain. The WIM implements the application-control interface and uses directly the services exposed by the northbound interface of the WAN SDN controller.

The third model is an extension derived from the previous model where the WAN infrastructure is operated by another service provider. In the model, SDN controllers are hierarchically introduced. WAN resources are virtually exposed to multiple client environment by the WAN (=lower) controller. Each WAN resources exposed are controlled by the upper SDN controllers interfacing with their WIM.

In the present document, the use cases have basically been considered within a context of single service provider. Therefore, the simplest and the second model could be leveraged but the third model is out of the scope.

B.3 SDN Architecture for Transport Networks

Transport SDN is a type of SDN which is applied to WAN infrastructure [i.33], and the scope is quoted:

"Transport networks need to accommodate growing bandwidth demand from data centers, support rapid service deployment by service providers, and provide real-time responsiveness to capacity/QoS changes. Application and service providers want the ability to request and provision edge-to-edge connections with guaranteed SLA (in terms of e.g. bandwidth, delay, availability, error performance) over multiple types of transport infrastructures, including OTN, MPLS-TP and Carrier Ethernet."

According to the functional requirements [i.25], the transport SDN controller supports the following multiple services, which is also illustrated in Figure B.3-1.

- *Topology service* allows an API client to retrieve topological information (e.g. network topology, nodes, links, ports…) that is within its shared Context.
- *Connectivity service* allows an API client to retrieve connectivity information and request connectivity service within its shared Context.
- *Path Computation service* allows an API client to ask to compute a path from an entry point to exit point.

- *Virtual Network service* allows an API client to manage virtual network deployed in the transport network infrastructure.
- *Notification service* allows an API client to be notified about events, for example, alarms, performance monitoring (PM) threshold crossings, object creation/deletion, attribute value change (AVC), state change, etc.

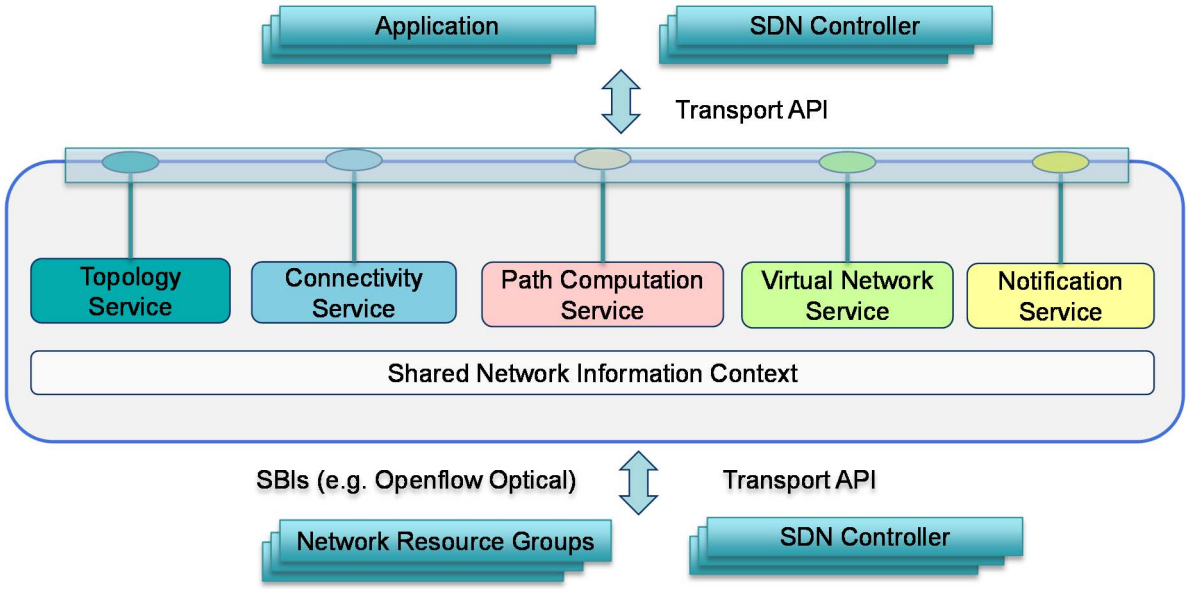

Figure B.3-1: Transport SDN Controller services and APIs (ONFTR-527 Functional Requirements for Transport API)

B.4 Interoperability test and demonstration by ONF/ OIF in 2016

In 2016, OIF SDN Transport API Interoperability Demonstration was held by the OIF and ONF. The interoperability test, mainly managed by the OIF, reported multi-layer and multi-domain environments in global carrier labs located in Asia, Europe and North America. In the context, Topology and connectivity services are tested in their network infrastructure configured by multiple vendors' equipment.

Since the transport networks generally reside at the lower layers of the networking infrastructure hierarchy, actually a particular type of network infrastructure area is out of scope of the present document. The Transport SDN use cases needs to be more relevant when considered in the context of a larger service and user ecosystem. For this interoperability demonstration, the use cases were framed in the context of the ETSI-NFV architecture.

B.5 ETSI-NFV PoC#42 Mapping ETSI-NFV onto Multi-Vendor, Multi-Domain Transport SDN

In ETSI-NFV, the present document studies connectivity service instantiations and management between different NFVI-PoPs in the context of end-to-end NS Life Cycle Management. The use cases are based on scenarios involving multiple sites, hosting NFVI-POPs, which are interconnected over a Wide Area Network (WAN) infrastructure [i.5]. In view of the above considerations, the objective of this PoC is to demonstrate a connectivity life cycle management with SDN-based Network Controllers over WAN interconnections that are interfaced with the WIM. As shown in Figure B.5-1, the PoC is architecturally configured by a network controller, interfacing with WIM, and Wide Area Network (WAN) infrastructure. The WAN interconnects multiple ETSI-NFV sites. In the present document, an NFVI-PoP is considered as a site. Based on this PoC, it is expected to gain valuable experiences that will enable us to not only derive the requirements on WIM towards the Network controller but also derive requirements on WIM from/towards the NFV-MANO functional components. By learning a specific SDN controller implementation in this PoC, the capability differences between WIM and Network Controller will be clearer. For the implementation of the PoC a Transport API [i.33], [i.25], [i.26], called T-API, implements a set of northbound application interfaces of the network controller. In the proposed PoC, a network infrastructure is configured by multiple networks of individual vendors. A domain (=lower) controller is responsible for the individual a network infrastructure. A multi-domain (=higher) controller is responsible for end-to-end connectivity of the multi-domain network infrastructure. The multi-domain controller implements the TAPI interface to WIM.

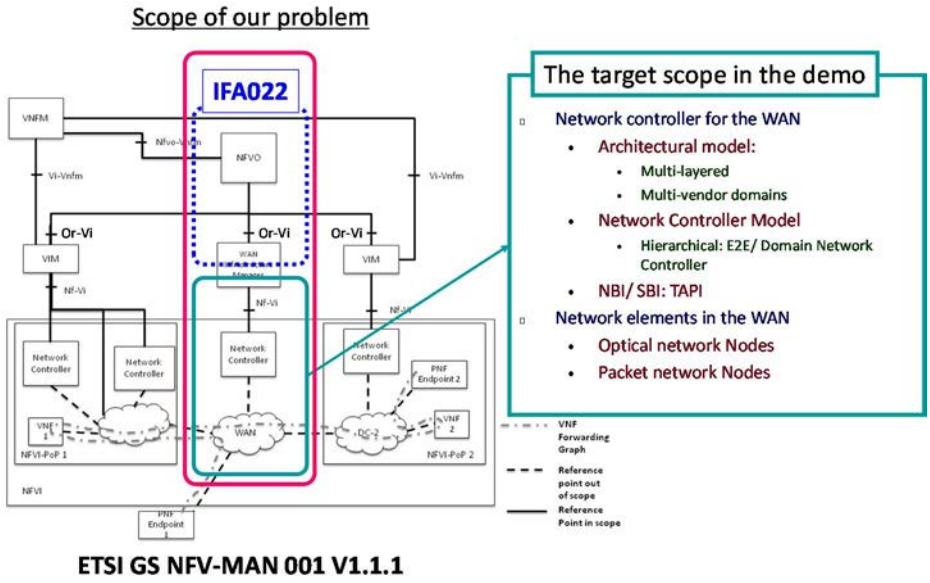

Figure B.5-1: Scope of our demonstration in the PoC

B.6 Analysis

In ETSI-NFV, an SDN controller has been considered as an example of a Network Controller. Within an NFVI-PoP, the Network Controller is considered as a centralized function which provides an abstract view of its network domain to the NFVI Network Control functions of the VIM [i.4]. The Network Controller is also considered as a function which is responsible for providing the programmable network interfaces that enable the establishment of connectivity within the domain [i.5]. As introduced, it is considered that the Transport SDN is newly introduced by ONF/OIF in ETSI-NFV, and the Transport SDN controller is another type of Network Controller, but for the WAN resources.

As for connectivity service aspect, it is considered that WIM is responsible for the following aspects related to the NFVI connectivity services [i.5]:

- Path computation based on quality assurance factors such as jitter, RTT, delay & bandwidth calendaring.
- Establish connectivity over the physical network (e.g. set of MPLS tunnels).

- Provide a northbound interface to the higher layers, e.g. NFVO, to provide connectivity services between NFVI-PoPs or to physical network functions.
- Invoke the underlying NFVI network southbound interfaces, whether they are Network Controllers or Network Functions, to construct the service within the domain.

However, a few overlaps were found in the references in ETSI-NFV, ONF and OIF. For instance, the path computation capability is considered in the WIM and the Transport SDN Controller. Another overlap is that a fulfilment for the network connectivity is also discussed as a part of the WIM and the Transport SDN Controller. Since the use case study in the present document notes that WIM is able to utilize services defined in Network Controller, so the path computation service and connectivity services may not be mandatory for WIM if Transport SDN is applied. Moreover, the topology service within Network Controller may also be utilized when WIM exposes network topology information to NFVO, But appropriate level of abstraction needs to be considered.

The minimum capabilities expected of the WIM, if Transport SDN is applied, are:

- Provide a northbound interface to the higher layer, e.g. NFVO, to provide WAN topology information between NFVI-PoPs.
- Provide a northbound interface to the higher layers, e.g. NFVO, to provide connectivity services between NFVI-PoPs or to physical network functions.
- Provide a northbound interface to the higher layers, e.g. NFVO, to provide alarm notifications that it may receive related to connectivity faults of the virtualised network resources in the WAN infrastructure (see clause 5.8).
- Invoke the underlying NFVI network southbound interfaces, whether they are Network Controllers or Network Functions, to construct the service within the domain.

Multiple Network Controller can be defined in NFVI-PoP and WAN. For example, in the environment defined by the Transport SDN, lower layer controllers for OTN, MPLS-TP and Carrier Ethernet are assumed. In ETSI-NFV, a particular type of network infrastructure and the detail of the fulfilment are out of scope. The northbound interface of the WIM needs to be managed by ETSI-NFV.

It is noted that the southbound interfaces are out of scope of the present document.

Annex C:
Security and Regulatory Concerns

C.1 Risk analysis and assessment

Table C.1-1 is the output of the Threat, Risk, Vulnerability Analysis according to ETSI GS NFV-SEC 006 [i.35].

Table C.1-1: Threat, Risk, Vulnerability Analysis

A Security Environment		
a.1	**Assumptions**	
a.1.1	An extended set of capabilities to the NFV MANO system that allows the establishment of NS traversing multiple NFVI-PoPs over the WAN infrastructure.	See clause 4.1
a.1.24	A specific NFV MANO functional block, i.e. a WIM, is one that leverages on the Or-Vi interfaces to deploy and manage NS across multiple NFVI-PoPs.	See clause 6.2.1
a.1.3	The WIM functional block produces interfaces that are consumed by other NFV-MANO functional entities, e.g. NFVO to enable multi-site connectivity of NFs (and VNFC).	See clause 4.1
a.2	**Assets**	
a.2.1	NFVO: it has two main responsibilities: • The orchestration of NFVI resources across multiple VIM instances, and the WAN resources in order to fulfil the Resource Orchestration functions within the NFVI-PoP and WAN; and • The lifecycle management of NS, fulfilling the Network Service Orchestration functions.	See clause 5.2
a.2.2	VNFM: it is responsible for the lifecycle management of VNF instances within the respective NFVI-PoPs.	See clause 5.2
a.2.3	VIM: it is responsible for controlling and managing NFVI compute, storage and network resources within one operator's Infrastructure Domain (e.g. NFVI-PoP). The VIM manages the association of the virtualised resources to the physical compute, storage and networking resources within the respective NFVI-PoPs.	See clause 5.2
a.2.4	WIM: it is responsible for assisting in the deployment and management of NS across multiple NFVI-PoPs.	
a.2.5	NFVI-PoP: N-PoP where a Network Function is or could be deployed as Virtual Network Function (VNF)	
a.2.6	Interfaces for management of WAN resources and connectivity of VNFs across multiple NFVI-PoPs..	See clause 5.2
a.2.7	Fault alarm: fault information reported to a consumer including information to identify the object on which the fault occurred, the type of fault that was identified, the cause of the fault, the timestamp information about when the event causing the fault was observed, as well as timing information about the alarm that is raised.	See clause 5.7
a.2.8	Performance metrics: performance information that need to be reported/acquired.	See clause 5
a.3	**Threat agents**	
a.3.1	Unauthorized user of assets (e.g. reports, notifications, queries, fault information, resource information)	
a.3.2	(Industrial) espionage agent	
a.3.3	Sabotage agent	
a.3.4	Internal threat agent, e.g. corrupt employee	

a.4	**Threats**	
a.4.1	Unauthorized viewing/copying/consuming of data and interfaces	Refer to all threat agents a.3. Refer to all assets in a.2.
a.4.2	Manipulation	Refer to all threat agents a.3. Refer to all assets in a.2.
a.4.2.1	- Unauthorized access	Refer to threat agents a.3.1, a.3.2 and a.3.3. Refer to all assets in a.2.
a.4.2.2	- Masquerade ("spoofing")	
a.4.2.3	- Forgery	
a.4.2.4	- Loss or corruption of information	
a.4.3	Repudiation	Refer to threat agent a.4.2. Refer to all assets a.2.
a.4.4	Denial of service	Refer to threat agents a.3.1, a.3.2 and a.3.3. Refer to all assets in a.2.
	B Security Objectives	
b.1	**Security objectives for the asset**	
b.1.1	The assets should ensure that only authorized and authenticated entities can access (read or write) the provided interfaces and that data is exchanged in a confidential manner. Therefore, requirements for access controls and communications security (see clauses 8.5 and 8.6 in [i.37]) should be followed.	
b.1.2	The assets should ensure the authenticity and integrity of all data exchanged on the interfaces and should prevent replay of any data. Therefore, requirements for authentications controls (see clause 8.4 in [i.37]) should be followed.	
b.1.3	The assets should ensure the availability of data to be provided on the interfaces.	
b.1.4	The assets should be accountable for the data provided, that is why the assets should ensure collected data (e.g. fault data, connectivity data, timestamps) and its sources can be trusted.	
b.1.5	The assets should ensure that interception is possible where required to support regulatory requirements (such as Lawful Interception [i.34] and Retained Data [i.36]) and not possible otherwise.	
b.1.6	The assets should ensure that denial of service (e.g. by message storms) is not possible.	
b.1.7	The assets should ensure that NS instances across multiple sites can only be deployed by authorized users and entities.	
b.1.8	The assets should ensure that NS instances can only be used by authorized users	
b.1.9	The assets should ensure that LCM of NS instances can only be requested by authorized users/entities	
b.1.10	The assets should ensure that NSDs can only be retrieved by authorized users/entities	
b.1.11	The assets should ensure that interception is possible where required to support regulatory requirements (such as Lawful Interception [i.34] and Retained Data [i.36]) and not possible otherwise.	
b.1.12	The assets should ensure the authenticity of the provider of the NS lifecycle operation granting interface.	
b.1.13	The assets should ensure the authenticity of the NFVI-PoPs.	

Annex D:
Authors & contributors

People have contributed to the present document:

Rapporteur:

Zarrar Yousaf, NEC

Previous Rapporteur:

Andrew Veitch, Netcracker

Other contributors:

Hiroshi Dempo, NEC

Zarrar Yousaf, NEC

Atsushi Taniguchi, NTT Corporation

Takeshi Kinoshita, NTT Corporation

Joan Triay, DOCOMO Communications Lab

Kazuaki Obana, DOCOMO Communications Lab

Koji Tsubouchi, DOCOMO Communications Lab

Ryosuke Kurebayashi, DOCOMO Communications Lab

Ashiq Khan, DOCOMO Communications Lab

Gerald Kunzmann, DOCOMO Communications Lab

Bertrand Souville, DOCOMO Communications Lab

Yuya Kuno, DOCOMO Communications Lab

Bhumip Khasnabish, ZTE Corporation

Nicola Santinelli, Telecom Italia S.p.A.

Anatoly Andrianov, Nokia

Catalin Meirosu, Ericsson LM

Arturo Martin De Nicolas, Ericsson LM

Cristina Badulescu, Ericsson LM

Stephen Fratini, Ericsson LM

Maria Toeroe, Ericsson LM

Aijuan Feng, Huawei

Haitao Xia, Huawei

Shaoji Ni, Huawei

Yannan Yuan, China Mobile

Rongwei Ren, China Mobile

Ran Duan, China Mobile

Changming Bai, China Mobile

Xiang Li, China Mobile

Rafael L. da Silva, Telefonica

Rafael Cantó, Telefonica

Diego López, Telefonica

Jesús Folgueira, Telefonica

Marc Flauw, Hewlett-Packard Enterprise

Jeremy Fuller, GENBAND Ireland Ltd.

History

Document history		
V3.1.1	April 2018	Publication