ETSI GR NFV-EVE 016 V1.1.1 (2020-09)

GROUP REPORT

Network Functions Virtualisation (NFV); Evolution and Ecosystem; Report on Connection-based Virtual Services

Reference

DGR/NFV-EVE016

Keywords

NFV, service, virtual services, virtualisation

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 prevailing version of an ETSI
deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

ETSI

Contents

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 scope of the present document is to:

- describe use cases and identify gaps within the NFV Architecture Framework to support Connection-based Virtual Services; identify recommendations for interfaces of service user and virtual resources (e.g. VM, Containers), and interfaces between Cloud Service Providers (Cloud SPs) to support the Connection-based Virtual Services; identify recommendations for connection and connection end points to support the Connection-based Virtual Services; and

- identify recommendations for MANO to support Connection-based Virtual Services.

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]   OCC 1.0 Reference Architecture, December 2014.

NOTE: Available at
https://wiki.mef.net/pages/viewpageattachments.action?pageId=63185562&highlight=OCC+1.0+Reference+Architecture.pdf#OCC+Specifications-attachment-OCC+1.0+Reference+Architecture.pdf.

[i.2]   OCC 1.0 Reference Architecture with SDN and NFV Constructs, August 2015.

NOTE: Available at
https://wiki.mef.net/pages/viewpageattachments.action?pageId=63185562&highlight=OCC+1.0+Reference+Architecture.pdf#OCC+Specifications-attachment-OCC+1.0+Reference+Architecture.pdf.

[i.3]   ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.4]   MEF 6.2: "EVC Ethernet Services Definitions Phase 3", August 2014.

[i.5]   MEF 61.1: "IP Service Attributes", May 2019.

[i.6]   MEF Whitepaper: "Understanding SD-WAN Managed Services", July 2017.

[i.7]   MEF 70: "SD-WAN Service Attributes and Service Definitions", May 2019.

[i.8]   ETSI GR NFV-IFA 022: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on Management and Connectivity for Multi-Site Services".

[i.9]   ETSI GS NFV 001: "Network Functions Virtualisation (NFV); Use Cases".

[i.10]   ETSI GS NFV-IFA 014: "Network Functions Virtualisation (NFV); Management and Orchestration; Network Service Templates Specification".

[i.11]   ETSI GS NFV-MAN 001: "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.12]   ETSI GS NFV-SWA 001: "Network Functions Virtualisation (NFV); Virtual Network Functions Architecture".

[i.13]   ETSI GS NFV-INF 004: "Network Functions Virtualisation (NFV); Infrastructure; Hypervisor Domain".

[i.14]   ETSI GS NFV-INF 001: "Network Functions Virtualisation (NFV); Infrastructure Overview".

[i.15]   ETSI GR NFV-IFA 029: "Network Functions Virtualisation (NFV) Release 3; Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"".

[i.16]   ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

3   Definition of terms, symbols and abbreviations

3.1   Terms

For the purposes of the present document, the following terms apply:

Cloud Application: self-contained or a group of programs or a software package that performs a specific function directly for an end user or, in some cases, for another application that may be owned by a Cloud User or Cloud SP or Cloud Operator (i.e. cloud service components that are not associated with connectivity)

Cloud Application UNI: Cloud Application interface between User and Cloud Service Provider

Cloud Application ENNI: Cloud Application interface between two Operators

Cloud Connectivity UNI: Connectivity interface between an User and Cloud Service Provider

Cloud Connectivity ENNI: Connectivity interface between two Operators

Cloud Operator: entity that is responsible for making Cloud Applications available to Cloud Service Providers and/or Cloud Operators

Cloud Operator-Operator Interface: interface between two Operators which is composed of Cloud Connectivity ENNI and Cloud Application ENNI

Cloud Service: service comprising one or more of platform components such as compute and storage, applications, and connectivity among them, that may be accessed by the Subscriber from one or more locations

Cloud Service Packet: packet that is exchanged at Cloud Subscriber Interface or Cloud Operator-Operator Interface among parties involved in a Cloud Service

Cloud Service Provider: entity that is responsible for the creation, delivery and billing of cloud services, and negotiates relationships among Connectivity Operators, Cloud Operators, and Cloud Users

Cloud User: end-user (i.e. a person or organization) that maintains a business relationship with and uses services from a Cloud Service Provider

Cloud User Interface: interface between a Cloud User and Cloud Service Provider which is composed of Cloud Connectivity UNI and Cloud Application UNI

Cloud Virtual Connection: association of two or more Cloud VC End Points (Cloud VC EPs)

Cloud Virtual Connection End Point: construct at a Cloud User Interface that selects a subset of the Cloud Service Packets that pass over the interface

Connectivity Operator: providing connectivity services between Cloud Operators, Connectivity Operators and Users

3.2   Symbols

Void.

3.3   Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 001 [i.9], ETSI GS NFV 003 [i.3] and the following apply:

CE	Carrier Ethernet
CMaaS	Communications as a Service
CPE	Customer Premises Equipment
CSUI	Cloud Service User Interface
EM	Element Management
ENNI	External Network Network Interface
EP	End Point
IaaS	Infrastructure as a Service
LAN	Local Area Network
MPLS	Multiprotocol Label Switching
NaaS	Network as a Service
PaaS	Platform as a Service
SD-WAN	Software Defined Wide Area Network
SECaaS	Security as a Service
SP	Service Provider
UNI	User Network Interface
VC	Virtual Connection
VPN	Virtual Private Network
WAN	Wide-area Network

4   Use Cases for Connection-based Virtual Services

4.1   Introduction

Connection-based Virtual Service term is used to describe Cloud Service given Cloud Service always has a connection between an application and a user, and virtual components. Therefore, both terms are used synonymously in the present document.

A Cloud Service can include application entities (e.g. VNFs), Cloud Virtual Connection (Cloud VC) and associated resources such as NFVI in ETSI GS NFV 003 [i.3]. For example, a connectivity service for an application can be a Cloud Service. Similarly, computing applications, computing resources and virtual network collectively can form a Cloud Computing service or just the computing applications together with computing resources form a Cloud Service where internet connection is used for the application access as depicted in Figure 4-1.

When a Cloud Service is an end-to-end service between external interfaces of a Cloud Service Provider (Cloud SP), it can include non-virtual and virtual resources such as VNFs and NSs or all virtual resources. For example, a user may use a non-cloud based network, cloud based network, or hybrid network to access cloud computing applications.

The services can be grouped under Network as a Service (NaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Communications as a Service (CMaaS) and Security as a Service (SECaaS). For example:

- SD-WAN providing application aware routing can be considered as NaaS;

- server, desktop, database, LAN and WAN can be categorized as IaaS;

- development environment and test environment can be categorized as PaaS;

- security services via virtualised firewalls and/or security services can be considered as SECaaS;

- WAN Optimization providing efficient utilization of network resources can be considered as SaaS;

- business, consumer, network and communication applications can be categorized as SaaS; and

- virtual PBX, audio and video conferencing and telepresence can be categorized as CMaaS.
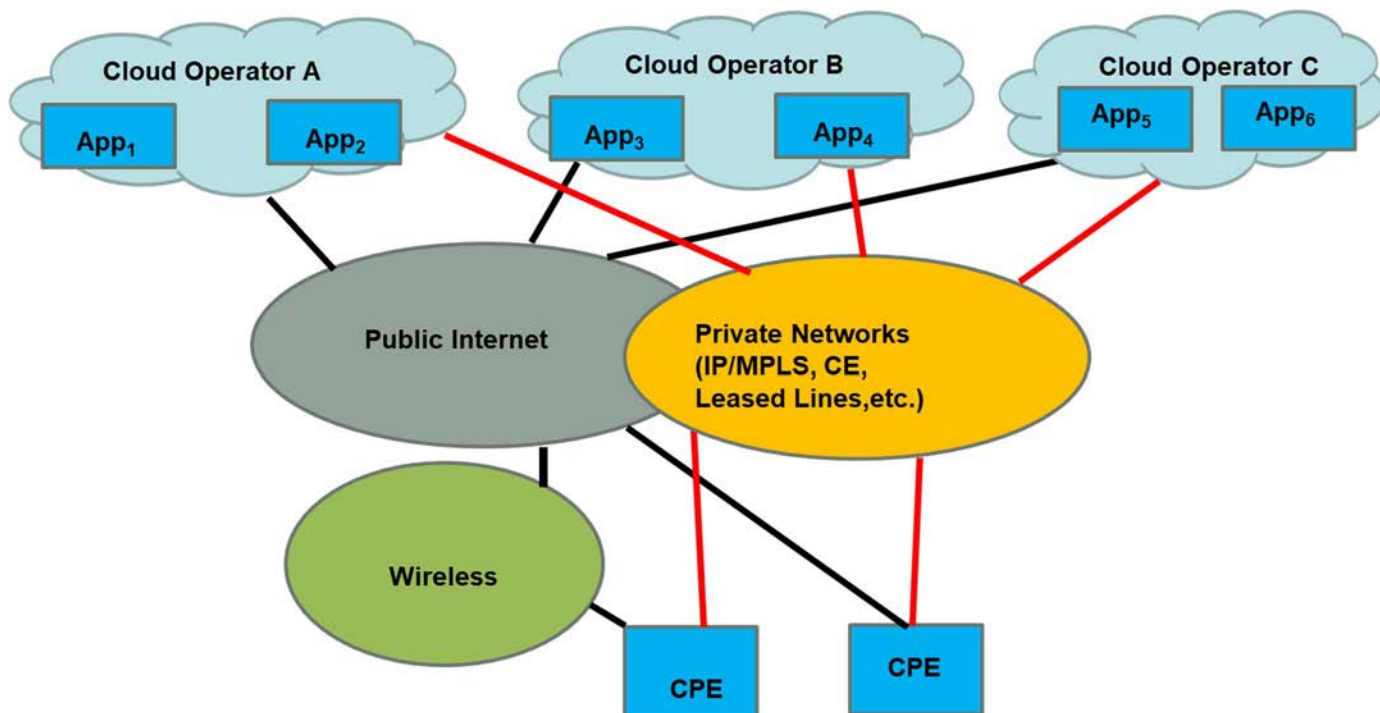
CE: Carrier Ethernet
CPE: Customer Premises Equipment
IP/MPLS: Internet Protocol/Multiprotocol Label Switching

Figure 4-1: Various access mechanisms for accessing Cloud Applications

In this clause, SD-WAN is described as an example.

4.2   SD-WAN

SD-WAN is a network connectivity service, NaaS, providing secure, IP-Based virtual overlay networks that typically uses IPsec tunnels over Internet or MPLS underlay networks. SD-WANs support any topology, e.g. full/partial mesh and hub and spoke. IP-Based SD-WAN implementations often use the public Internet as one of their WANs in which case they need to support firewall and Network Address Translation (NAT) capabilities.

The SD-WAN tunnel is initiated or terminated by the SD-WAN Edge which provides the SD-WAN service demarcation. The SD-WAN Edge creates and terminates encrypted tunnels over different types of wired or wireless underlay networks, such as T1s/E1s, broadband Internet (DSL, Cable, and PON), Wi-Fi™ and LTE™ wireless access networks, and IP (Internet) and MPLS core networks.

The SD-WAN Edge also performs application-based QoS and security policy enforcement, application forwarding over one or more WAN connections, and QoS performance measurements over each WAN to determine WAN path selection. The SD-WAN Edge may also perform WAN optimization functions such as packet buffering/reordering, data duplication, data compression, and forward error correction as described in MEF Whitepaper [i.6].

The SD-WAN Edge functionality may be implemented as a VNF which may run on a virtual CPE (vCPE) at the customer premises or in a data centre, which is managed by cSP. The SD-WAN Edge functionality can be also provided by a physical CPE device resident on the customer premises and managed by cSP.

The SD-WAN Controller provides physical or virtual device management for all SD-WAN Edges and SD-WAN Gateways (if used) to connect sites interconnected via alternative VPN technologies such as Carrier Ethernet. The management function includes configuration and activation, IP address management, and pushing down policies onto SD-WAN Edges and SD-WAN Gateways, and maintains connections to all SD-WAN Edges and SD-WAN Gateways.

The SD-WAN Controller communicates northbound with its Orchestrator. The Orchestrator provides the end-to-end SD-WAN management and interfaces to an OSS/BSS for service order and billing.

Two SD-WAN examples are depicted in Figures 4-2 and 4-3. These implementation examples do not follow ETSI-NFV standards.

In Figure 4-2, the SD-WAN configuration enables the user to use an encrypted SD-WAN tunnel over the Internet to augment their site-to-site MPLS VPN bandwidth and achieve higher resiliency using two WANs.
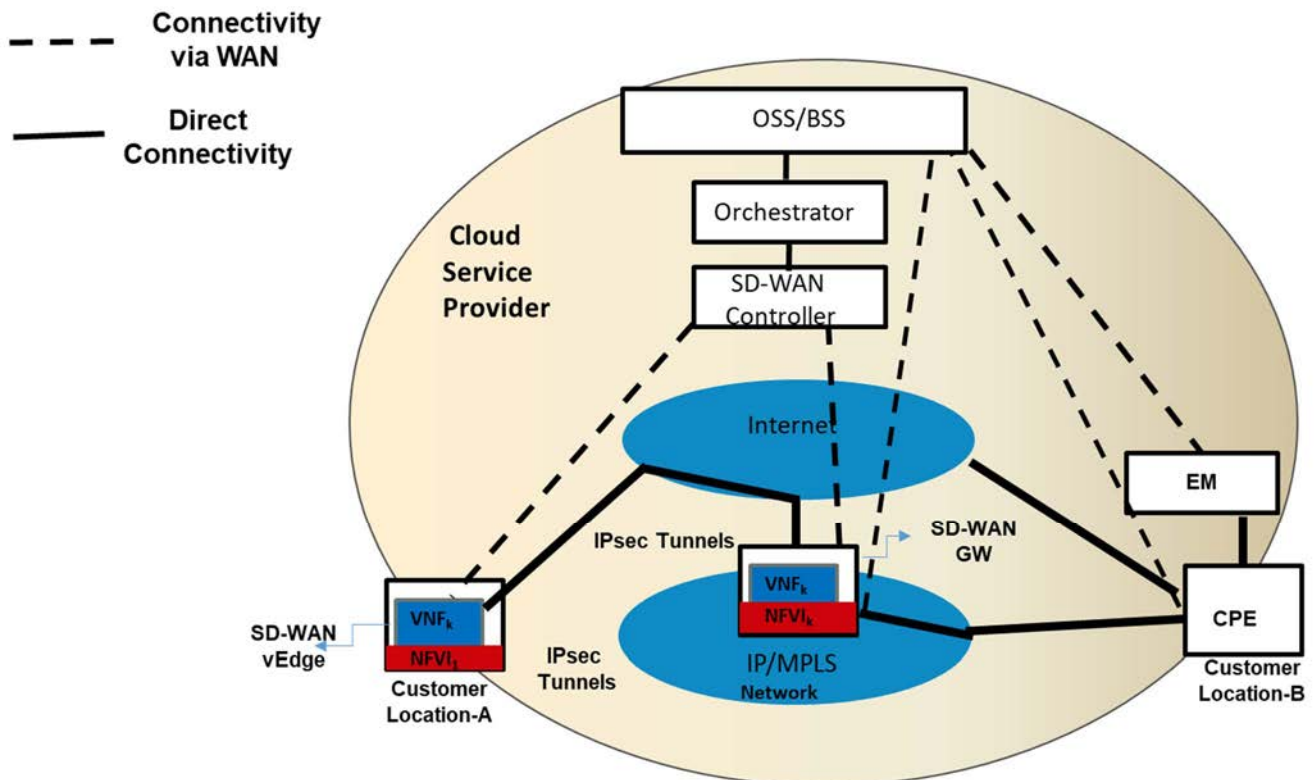

Figure 4-2: SD-WAN service tunnelled over Internet and MPLS WANs

Figure 4-3 illustrates an SD-WAN configuration where an SD-WAN Gateway interconnects sites connected via an SD-WAN over the Internet and sites connected via a MPLS VPN. An SD-WAN Gateway enables sites interconnected via the MPLS VPN to communicate with sites interconnected via SD-WAN tunnels over the Internet. The sites interconnected via MPLS VPN are expected to use legacy CPE which does not have virtualised components.
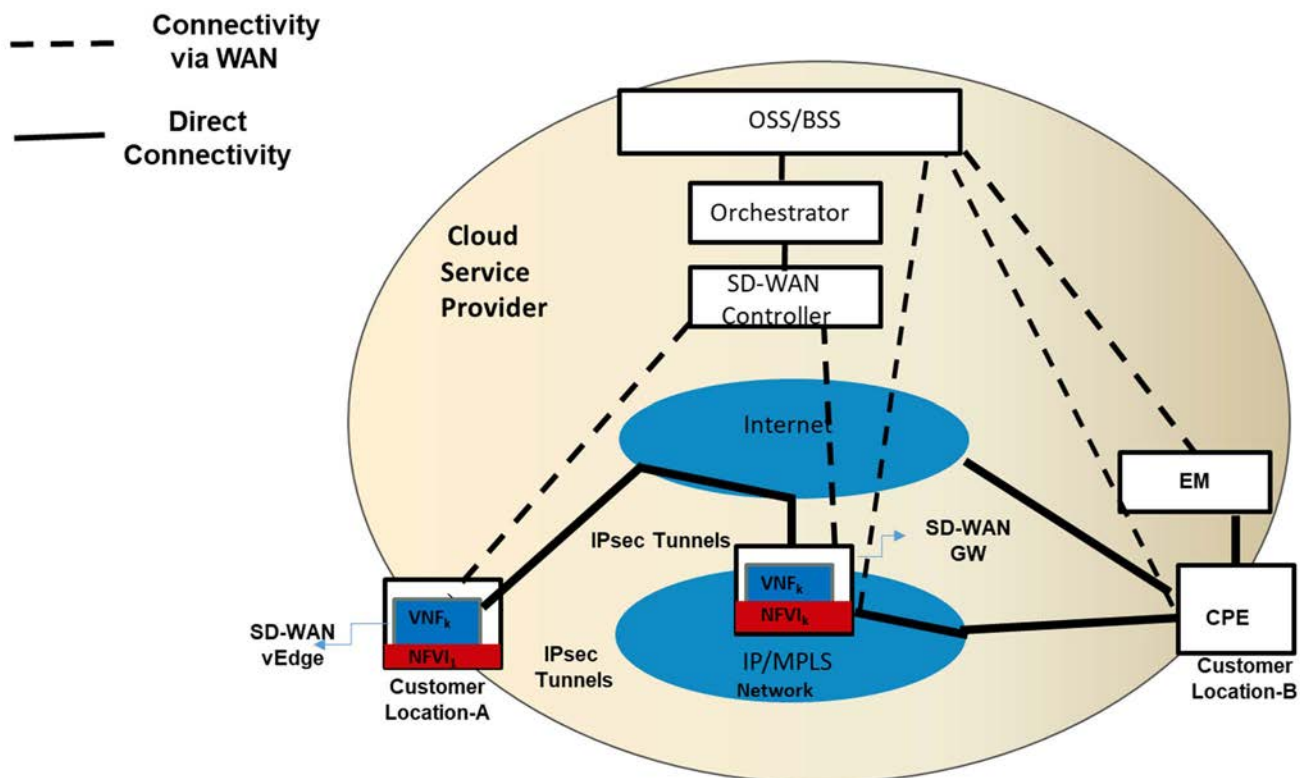
Figure 4-3: SD-WAN sites interconnecting with MPLS VPN sites

In Figures 4-2 and 4-3, the network that SD-WAN Edge units are connected to is managed by an Operations Support System (OSS) and various Element Managers (EMs). The OSS may consist of multiple systems. These systems along with EMs provide configuration management, fault management, performance management, security management and testing of network elements and facilities connecting these network elements.

The legacy CPE in Figure 4-3 is likely to be managed by an EM. Similarly, elements of the IP/MPLS network in Figures 4-3 and 4-4 are likely to be managed by EMs that are not shown in the figures.

Figure 4-4 redraws the network configuration similar to that in Figure 4-2 using ETSI NFV constructs. Per [i.8], [i.9], VNF represents vCPE. IPsec tunnel forming a Cloud Service Connection (or SD-WAN Connection) is mapped to a Virtual Link despite of the fact that there could be multiple connections in a given link.

SD-WAN vEdge VNFs are managed by VNFM. WIM provides the necessary multi-site connectivity to connect the SD-WAN vEdge islands that are instantiated over the NFVIs. The WIM may be responsible for underlying WAN.

In contrast to WIM, a VIM manages network resource as well as NFVI compute and storage resources within the domain of an NFVI-PoP where SD-WAN vEdge resides.
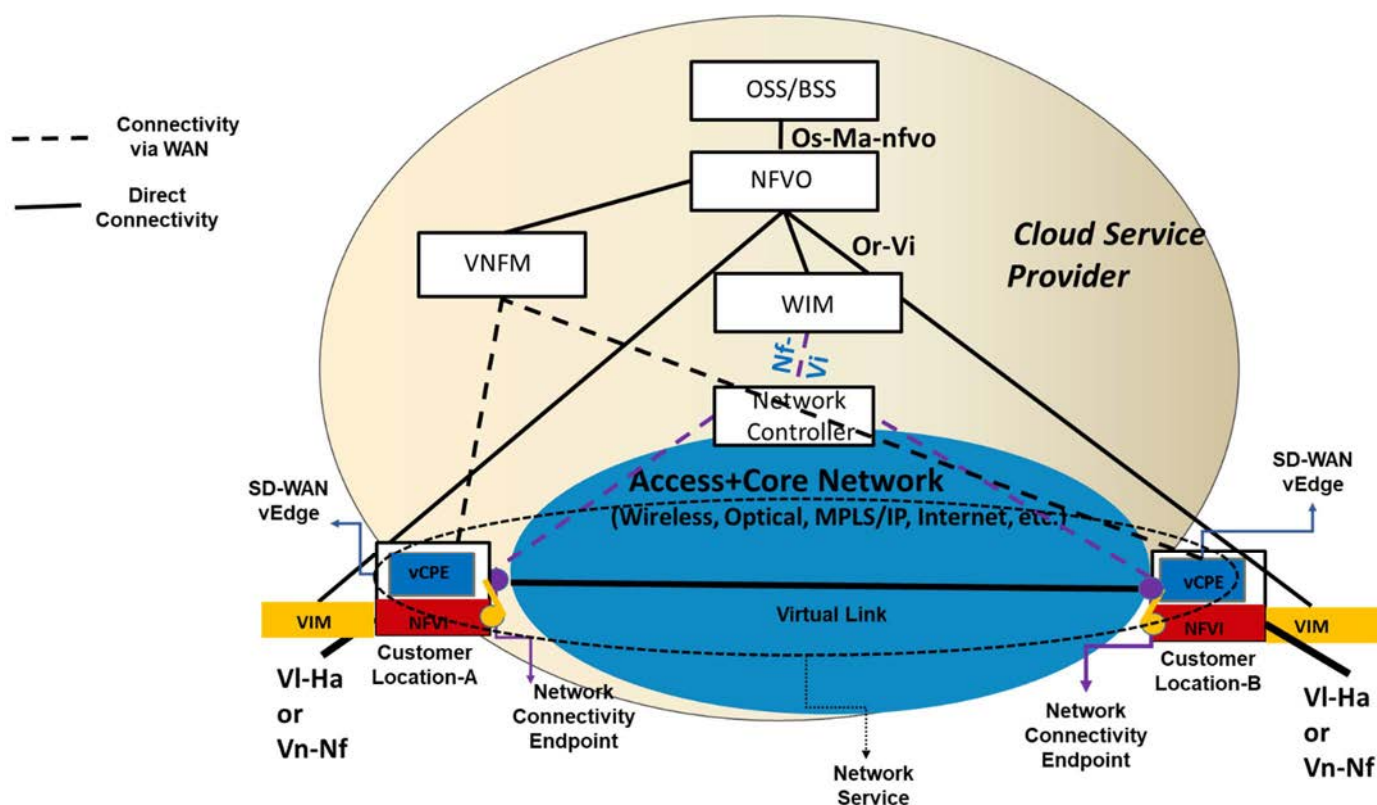
Figure 4-4: SD-WAN service components represented by ETSI NFV constructs

In Figure 4-4, a Network Service (NS) consisting of two VNFs (vCPE) is instantiated. These two VNFs are installed at two customer sites, Customer Location-A and Customer Location-B, and connected across the WAN infrastructure.

The virtualised network resources assigned to the vCPE 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 for Customer Location-A, Customer Location-B and WAN.

5   Actors of Connection-based Virtual Services

5.1   Introduction

The key actors of Connection-based Virtual Services (i.e. Cloud Services) are depicted in Figure 5-1 where a Cloud Service Provider (Cloud SP) is responsible for providing an end-to-end Connection-based Virtual Service to a Cloud User using resources of Connectivity Operator (s) and Cloud Operator (s) [i.1] and [i.2]. The connectivity can be provided by networks of Connectivity Operator (s) as well as by the Internet.
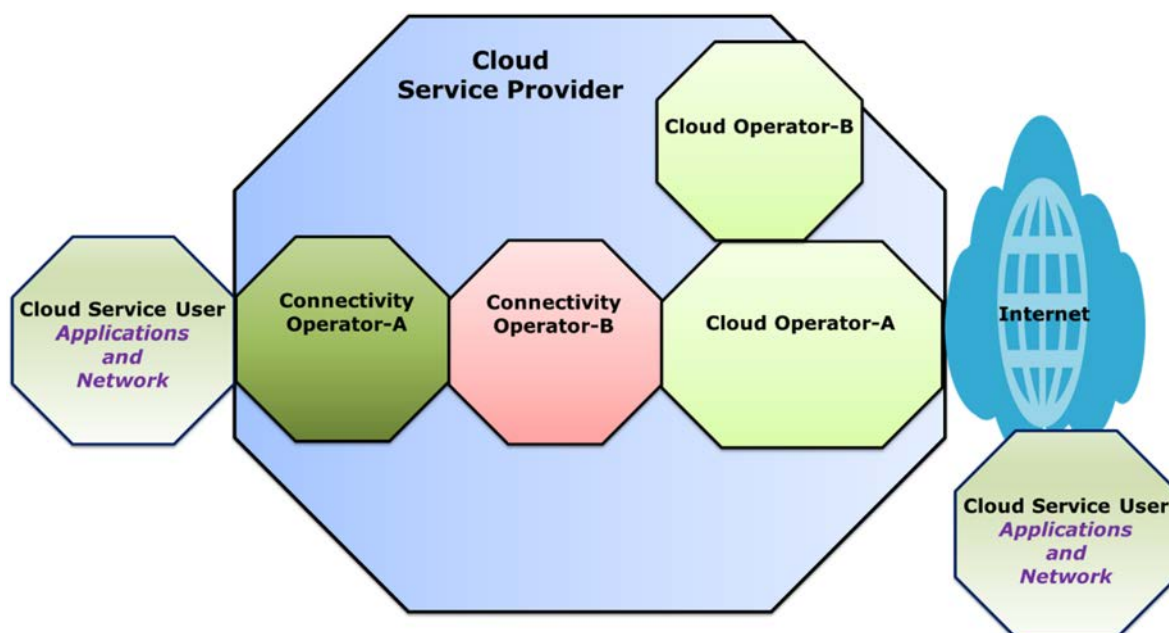
Figure 5-1: Cloud Service Actors

5.2 Cloud Service User

A Cloud Service User is the end-user (i.e. a person or organization) that maintains a business relationship with and uses services from a Cloud SP.

A Cloud Service User interfaces to a Cloud SP's facilities via a standards interface called Cloud Service User Interface (CSUI) (Figure 5-2) which is a demarcation point between the Cloud SP and the Cloud Service User.
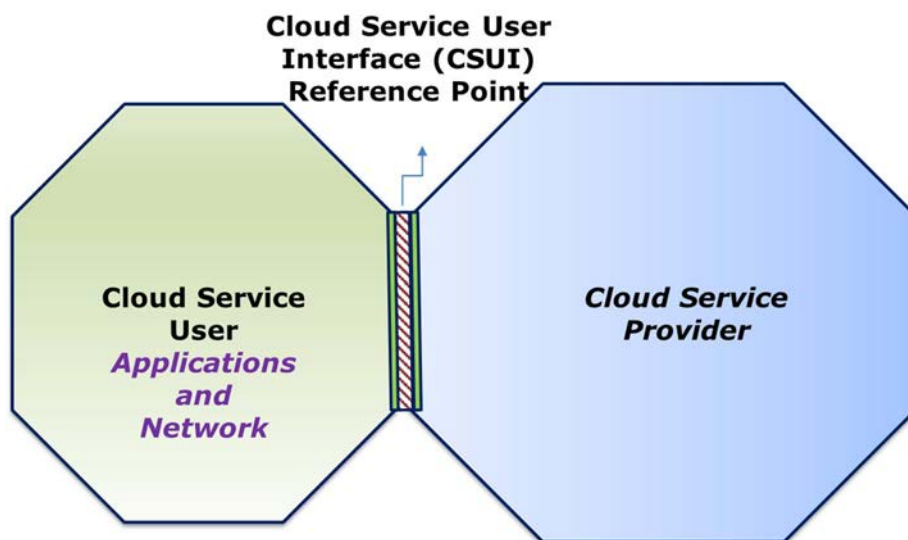

**Figure 5-2: CSUI Reference Point between Cloud Service User and Cloud SP**

The user in Figure 5-2 can be an enterprise with multiple users sharing the same Cloud User Interface. The user interface may consist of a physical equipment with an Internet browser, a VNF, a Virtual Machine (VM), a Container, or a collection of VNFs, VMs and Containers with a virtual switch.

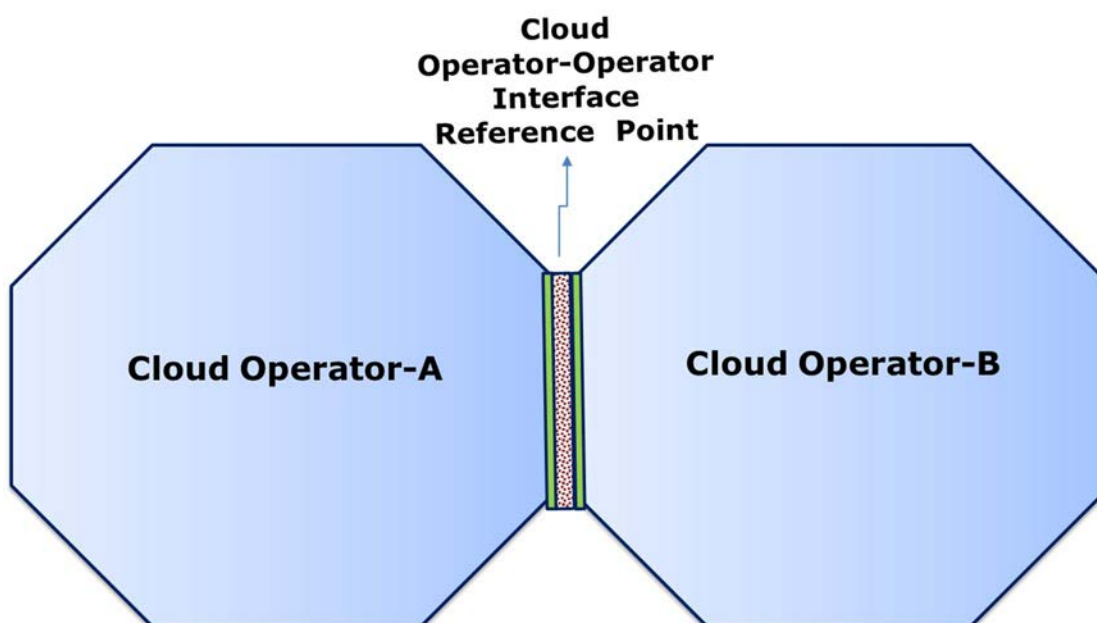## 5.3   Connectivity Operator and Cloud Operator

Connectivity Operator is an entity providing connectivity services between Cloud Operators, Connectivity Operators and Users. Cloud Operator is an entity that is responsible for making cloud applications available to Cloud Service Users.

A Cloud SP can implement the Cloud Service that they provide to the User by subcontracting with one or more Operators. Each Operator might provide a connectivity service (a Connectivity Operator) and/or an application(s) (a Cloud Operator).
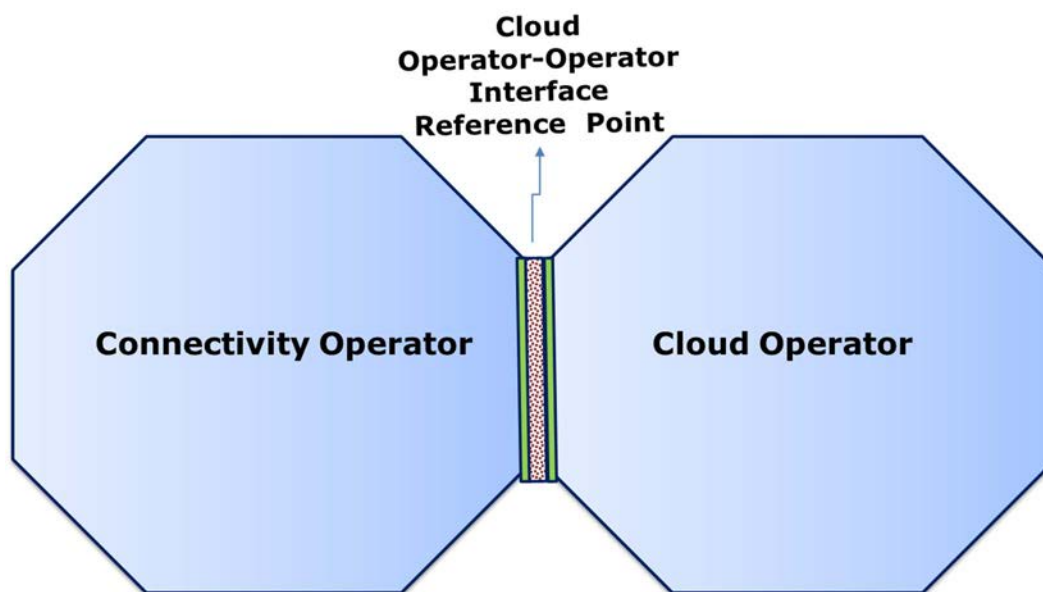
Two Operators interface each other via a Cloud Operator-Operator Interface as depicted in Figure 5-3.
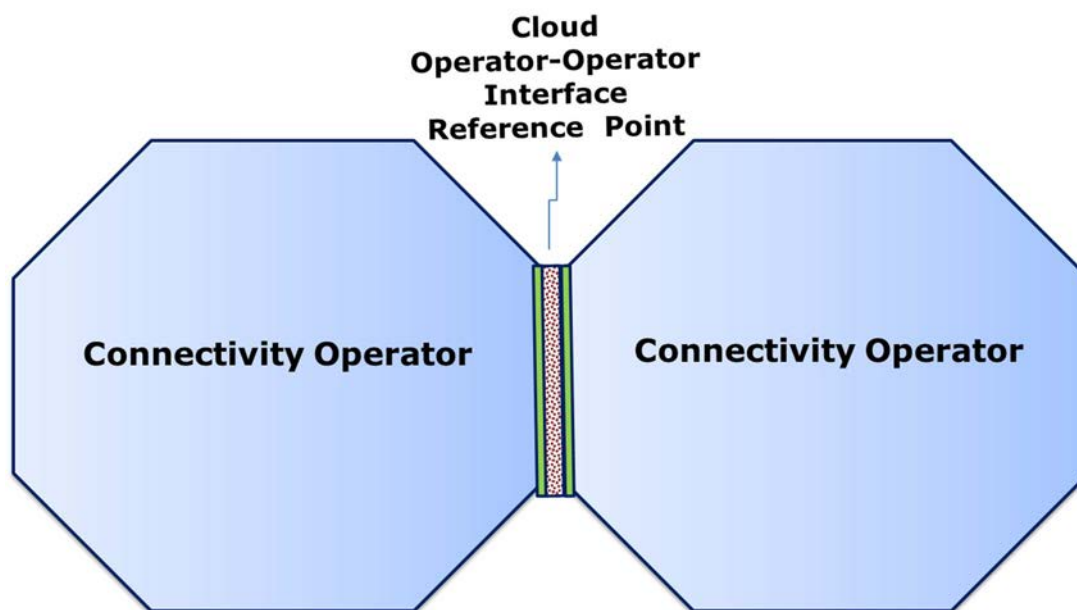
(a) Cloud Operator-Operator Interface between two Connectivity Operators

(b) Cloud Operator-Operator Interface between two Cloud Operators

(c) Cloud Operator-Operator Interface between Connectivity Operator and Cloud Operator

Figure 5-3: Cloud Operator-Operator Interface

5.4 Cloud Service Provider

Cloud Service Provider (Cloud SP) is an entity that is responsible for the creation, delivery and billing of cloud services, and negotiates relationships among Connectivity Operators, Cloud Operators, and Cloud Service Users. It is the single point of contact for the user.

For a given Cloud Service, the User contracts with a Cloud SP to be responsible for delivering Cloud Services at the User locations. The Service Provider, in turn, selects and contracts with various Connectivity Operators and Cloud Operators to deliver the services at requested locations. It is the responsibility of the Service Provider to ensure that service features purchased by the User are delivered.

6 Interfaces of Connection-based Virtual Services

6.1 Introduction

The interface between a Cloud Service User and a Cloud SP, the interface between Operators, and the interface of the Cloud Application or Cloud Platform are the key interfaces for using and delivering Cloud Services. They are described in the following clauses.

6.2 Cloud User interface

A Cloud User interfaces to a Cloud Service Provider's facilities via a Cloud User Interface. The Cloud User Interface is composed of Cloud Connectivity UNI (User Network Interface) and Cloud Application UNI (User Network Interface) as depicted in Figures 6-1 and 6-2. The Cloud Connectivity UNI demarcates domains under the responsibility of the Cloud Service Provider and domains under the responsibility of the Cloud User for connectivity. On the other hand, the Cloud Application UNI demarcates domains under the responsibility of the Cloud Service Provider and domains under the responsibility of the Cloud User for applications where an application is defined as the cloud service functionalities beyond connectivity.
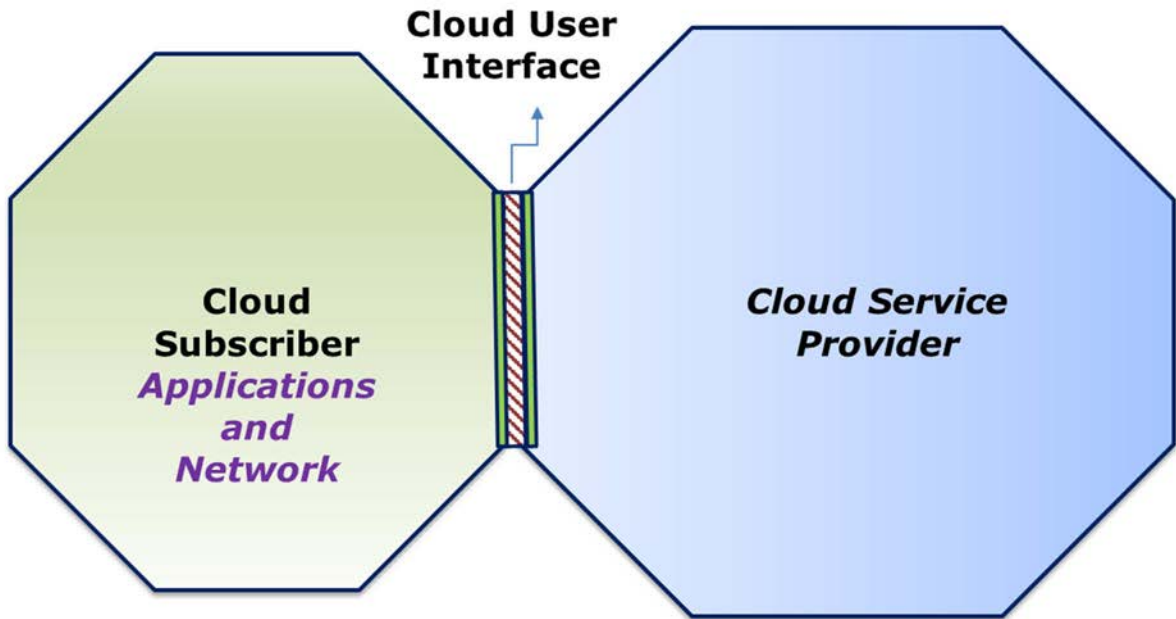
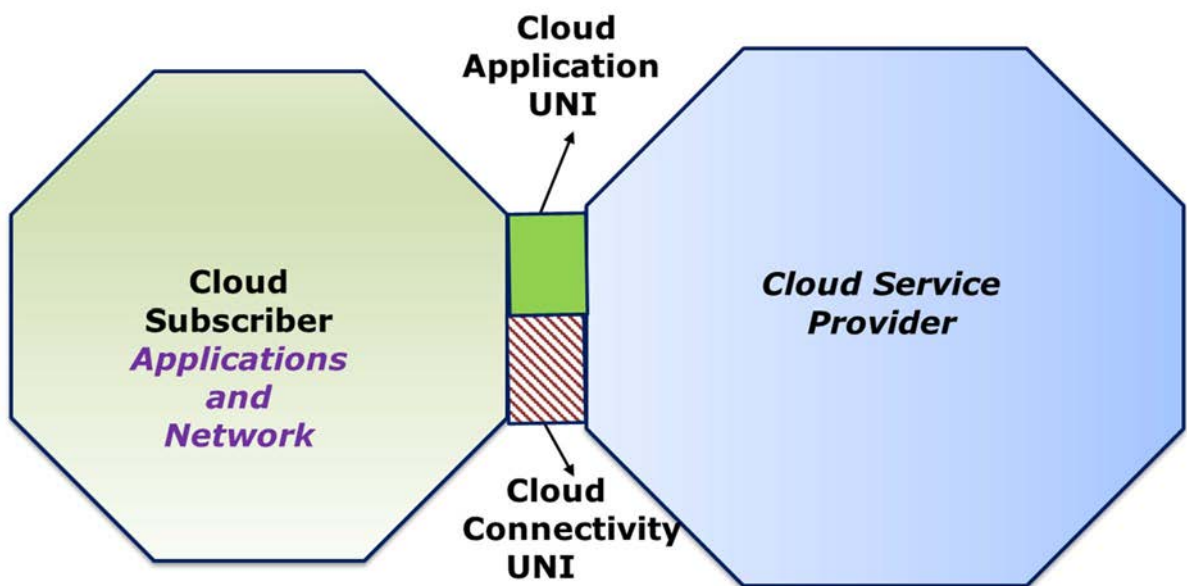**Figure 6-1: Cloud User Interface**

Figure 6-2: Cloud Connectivity UNI and Cloud Application UNI between User and Cloud SP

In cases where Cloud SP offers only connectivity services, the Cloud User Interface consists of only Cloud Connectivity UNI as illustrated in Figure 6-3.
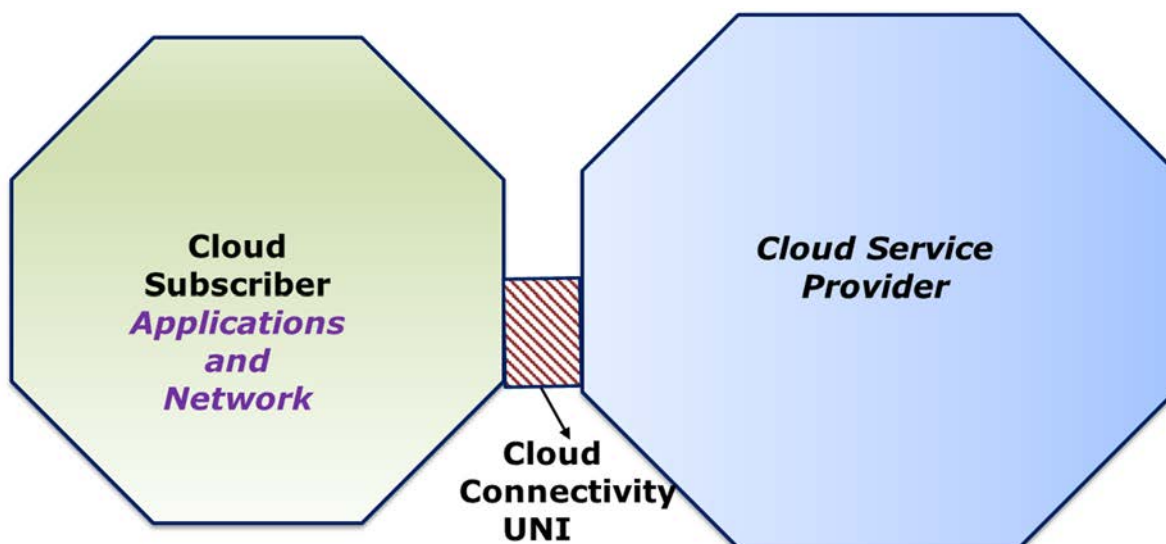
Figure 6-3: Cloud User Interface consists of only Cloud Connectivity UNI

The Cloud Application UNI may be at a different location than the Cloud Connectivity UNI. It is between the User application (s) and Cloud SP application (s) which is anywhere between User Application Location and Cloud SP Application Location. At the Cloud Application UNI, the User is responsible for the compatibility of Cloud Service Packets, that are originated within the User domain, with the Application UNI requirements. Similarly, the Cloud SP is responsible for the compatibility of cloud service packets, that are originated within the Cloud SP domain, with the Application UNI requirements.

Cloud User Interface is implemented over a bi-directional link that provides various data, control and management capabilities required by the Cloud Service Provider and dedicated to a single Cloud User such as an enterprise. Multiple flows can be multiplexed over this interface using logical connections.

The user in Figures 6-1 and 6-2 can be an enterprise with multiple users sharing the same Cloud User Interface. The user interface may consist of a physical equipment with an Internet browser, a VNF, a Virtual Machine (VM), a Container, or a collection of VNFs, VMs, and Containers with a virtual switch.

Across the Cloud User Interface, Cloud User establishes a connection, Cloud Virtual Connection (Cloud VC), with resources of Cloud SP such as virtual machines (VMs) and applications (i.e. VNFs), using connection resources of Cloud SP.

The user and Cloud SP exchange Cloud Service Packets across the Cloud User Interface. A Cloud Service Packet can be an L1 frame, Ethernet frame, an IP packet, an MPLS packet, or an application Protocol Data Unit (PDU).

The Cloud Service Packet transmitted across the Cloud User Interface toward the Cloud SP is called an ingress Cloud Service Packet. The Cloud Service Packet transmitted across the Cloud User Interface toward the Cloud User is called an egress Cloud Service Packet.

Cloud User Interface protocol stack is depicted in Figure 6-4 that may combine protocol stacks for Cloud Connectivity UNI and Cloud Application UNI as illustrated in Figure 6-5.
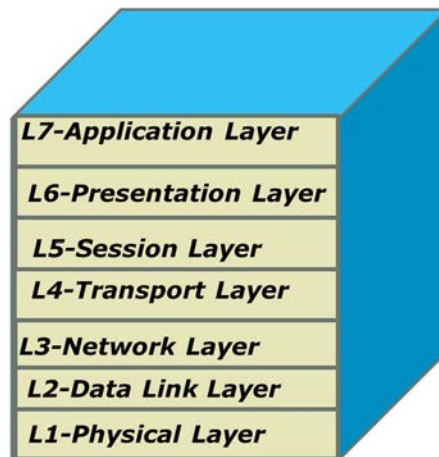
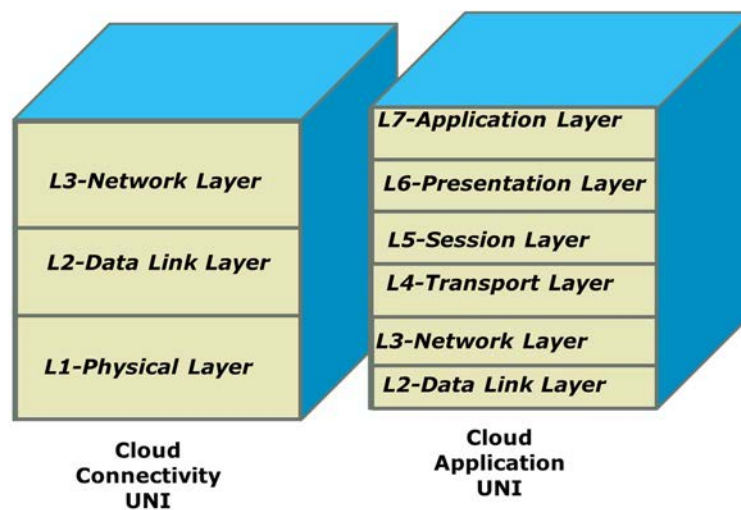**Figure 6-4: Cloud User Interface Protocol Stack**

Figure 6-5: Cloud Connectivity UNI and Application UNI Protocol Stacks

Depending on the cloud service offering, the protocol stack for Cloud Connectivity UNI can be L1, L2 or L3. For example, Cloud Connectivity UNI is an L2 interface for Carrier Ethernet Services and an L3 interface for IP services.

Depending on the service offering, the protocol stack for Cloud Application UNI can be L2 and above. For example, Cloud Application UNI is an L7 interface for multimedia applications.

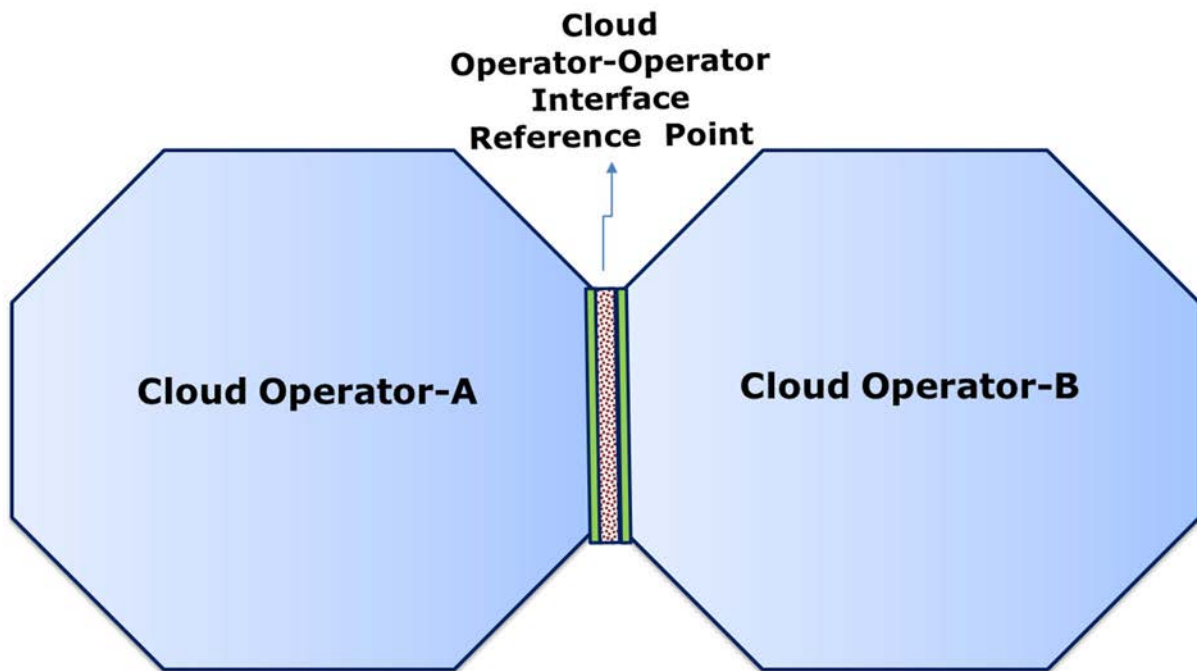## 6.3   Cloud Operator-Operator Interface

Applications and the connectivity to applications can be provided by one or more Connectivity Operators and Cloud Operators that are subcontracted by the Cloud SP, in providing a cloud service to a Cloud User.

A Cloud SP can implement the Cloud Service that they provide to the User by subcontracting with one or more Operators. Each Operator might provide a connectivity service (a Connectivity Operator) or a Cloud Service (a Cloud Operator).
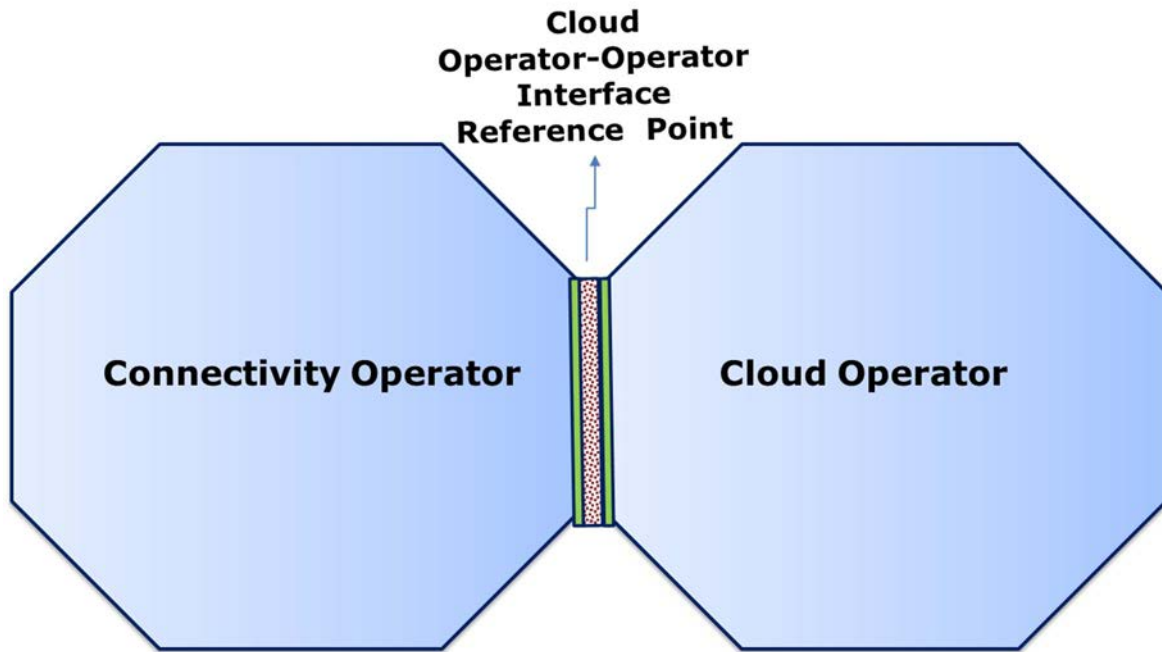
Two Operators interface each other via a Cloud Operator-Operator Interface as depicted in Figure 6-6. The Cloud Operator-Operator Interface is composed of Cloud Connectivity ENNI and Cloud Application ENNI as illustrated in Figure 6-7. There may not be a Cloud Application ENNI at the Cloud Operator-Operator Interface when only connectivity services are offered at this interface as illustrated in Figure 6-8. Cloud Application ENNI is between the applications of two Operators which is anywhere between applications locations. At the Cloud Application ENNI, both Operators are responsible from the compatibility of Cloud Service Packets originated within their domains with the Application ENNI requirements. Cloud Operator-Operator Interface demarcates domains under the responsibility of each Operator for cloud services.
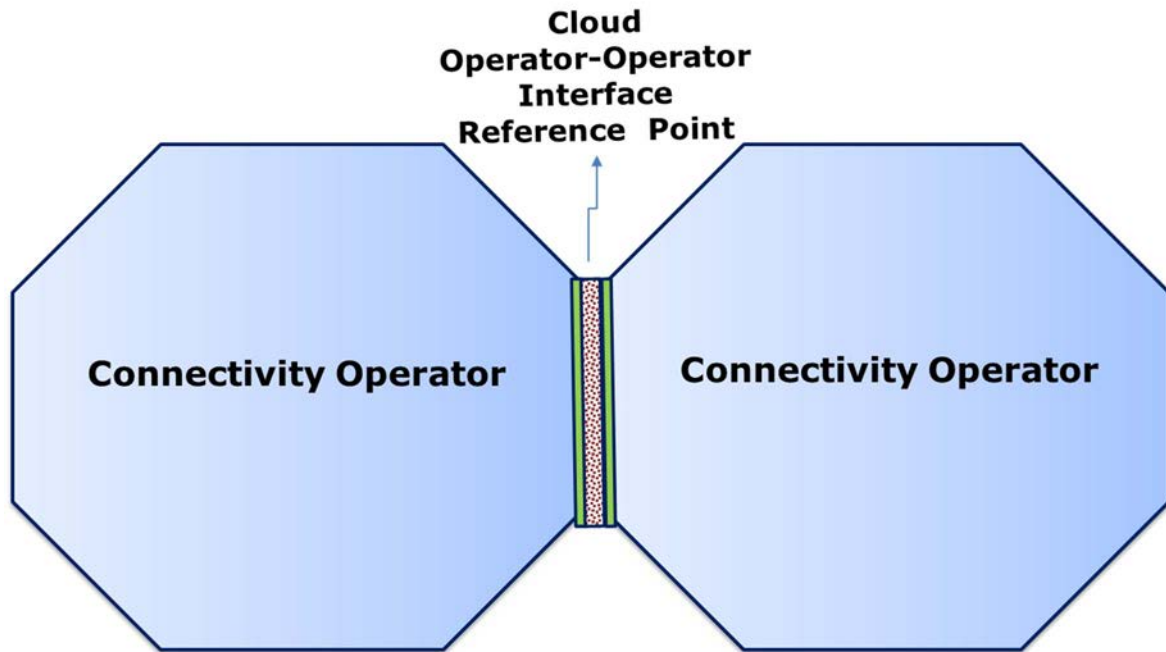
**Cloud
Operator-Operator
Interface
Reference Point**

Connectivity Operator

Connectivity Operator

(a) Cloud Operator-Operator Interface between two Connectivity Operators

**Cloud
Operator-Operator
Interface
Reference Point**

Cloud Operator-A

Cloud Operator-B

(b) Cloud Operator-Operator Interface between two Cloud Operators

(c) Cloud Operator-Operator Interface between Connectivity Operator and Cloud Operator

Figure 6-6: Cloud Operator-Operator Interface variations
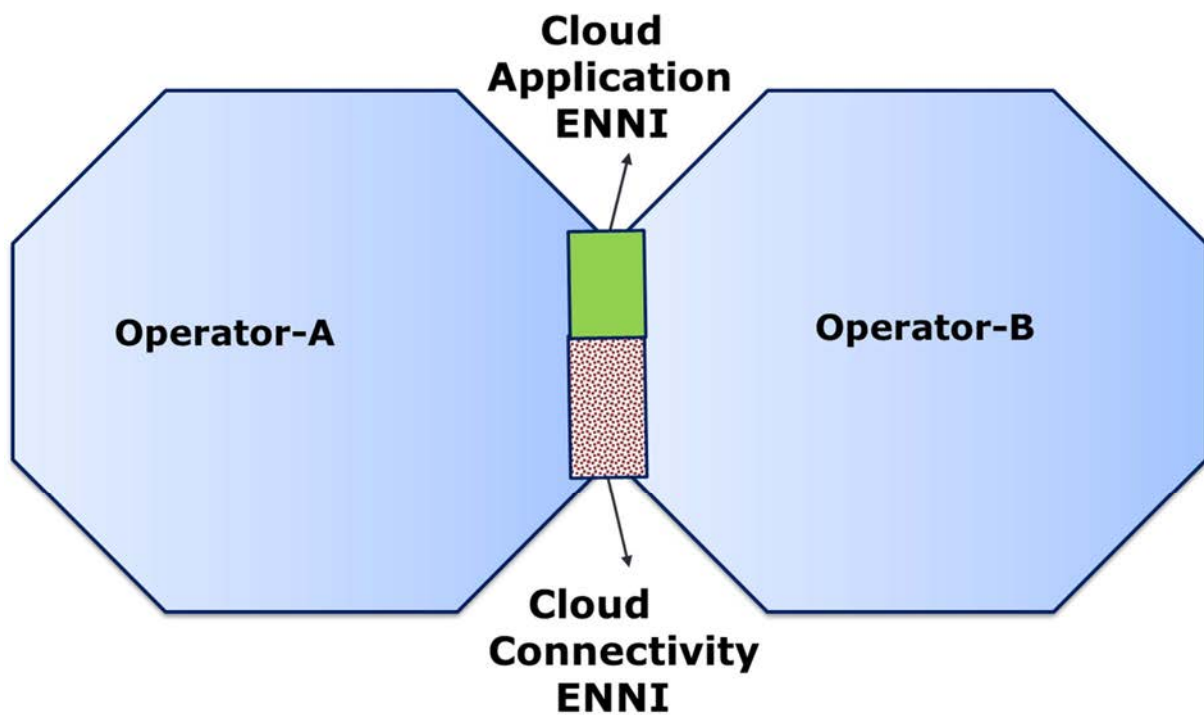

Figure 6-7: Cloud Connectivity ENNI and Cloud Application ENNI between two Cloud Operators
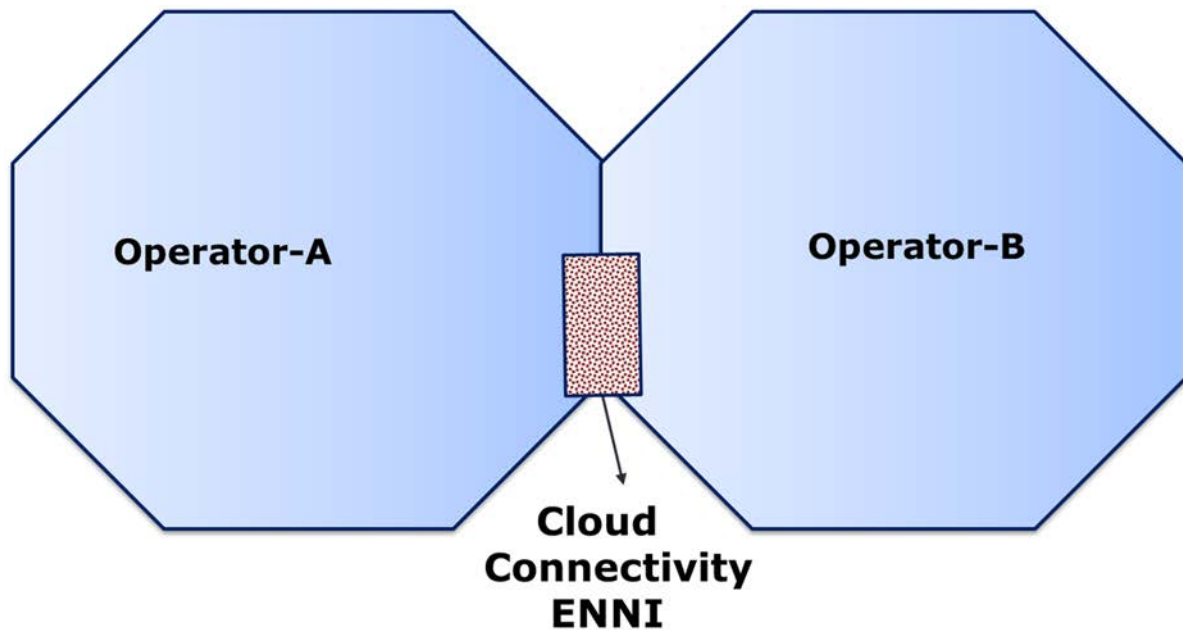
Figure 6-8: Cloud Connectivity ENNI is between two Connectivity Operators

Cloud Operator-Operator Interface protocol stack is depicted in Figure 6-9 that may combine the protocol stacks for Cloud Connectivity UNI and Cloud Application UNI as illustrated in Figure 6-10. Depending on the cloud service offering, the protocol stack for Cloud Connectivity ENNI can be L1, L2 or L3. Similarly, the protocol stack for Cloud Application ENNI can be L2 and above, depending on the service offering.

Figure 6-9: Cloud Operator-Operator Interface Protocol Stack
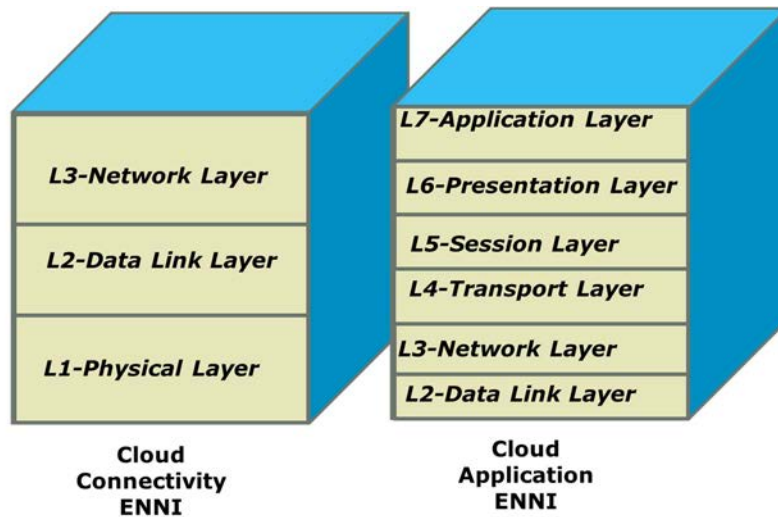
Figure 6-10: Cloud Connectivity ENNI and Application ENNI Protocol Stacks

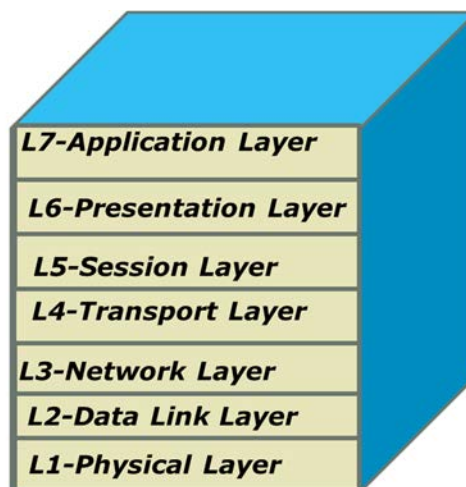# 6.4   Cloud Application interface

The Cloud Application Interface (i.e. Cloud Application UNI or Cloud Application ENNI) is the interface of a Cloud Service Application or Cloud Service Platform supported by a Cloud Operator or a Cloud Service Provider. Therefore, it can be an interface of a VNF, VM or Container, as depicted in Figure 6-11 and Figure 6-12.

NOTE: These are just examples for the Cloud Application Interface.
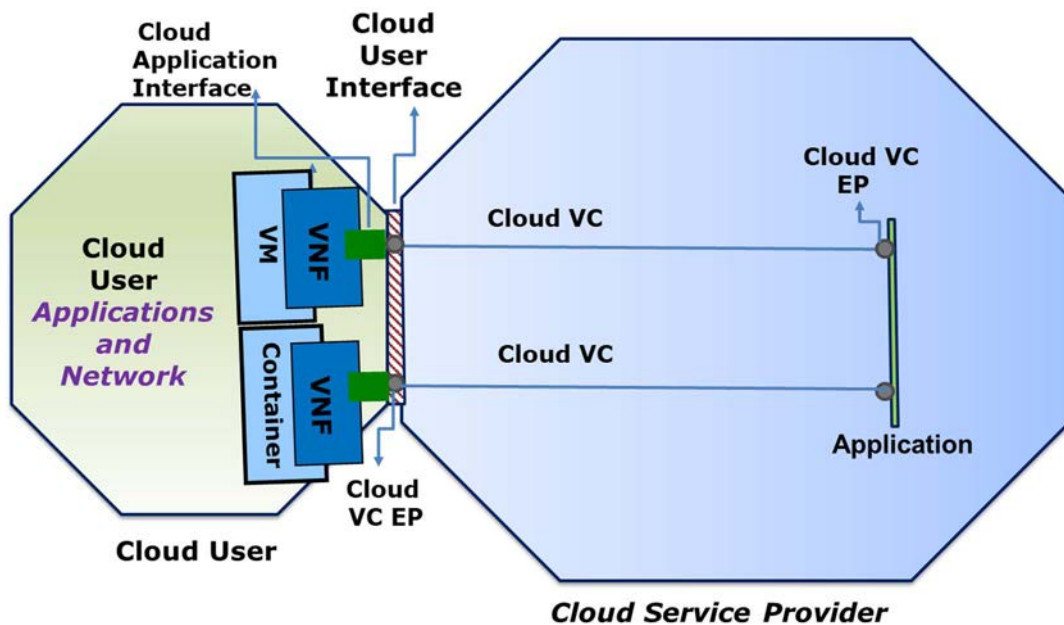
Cloud VC EP: Cloud Virtual Connection End Point.

Figure 6-11: Cloud Application Interface for VNF

In Figure 6-11, VNF can be a firewall as part of a Security as a Service (SECaaS) or SD-WAN Edge as part of a SD-WAN service.

Figure 6-12: Cloud Application Interface for VM or Container

Container and VM in Figure 6-12 can be a part of virtualisation platform supporting Platform as a Service (PaaS).

Depending on service offerings, the protocol stack for the Application Interface can be L2 and above. For example, Cloud Application In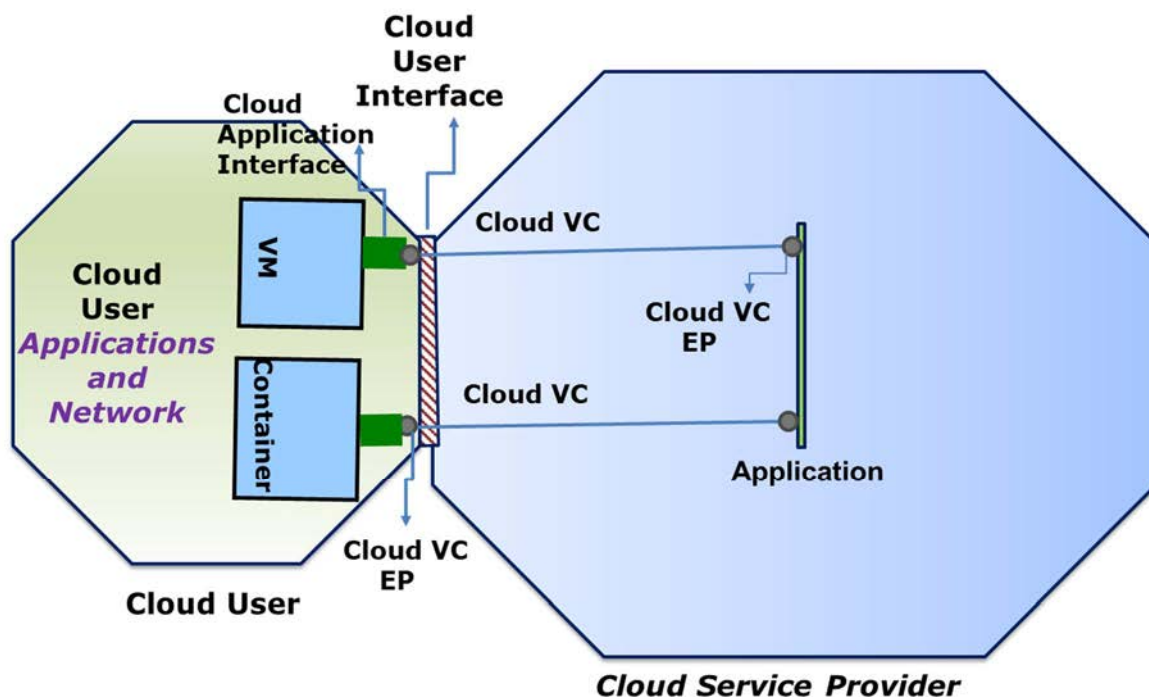terface is an L2 interface for WAN Optimization, L3 interface for SD-WAN and Virtual Router, and L7 interface for multimedia applications.

7 Connections and Connection End Points of Connection-based Virtual Services

7.1 Introduction

As described in clause 4 that Cloud Services consist of connectivity and application components. The connectivity can be between two cloud services users, between a cloud service user and application, and between two cloud applications.

Connection and connection end points providing cloud services are depicted in Figure 7-1 for a Cloud Virtual Connection (Cloud VC) crossing one or more administrative domains.

When a Cloud VC crosses multiple Operators, the components and their end points in each Operator are called Operator Cloud VC and Operator Cloud VC End Point (EP), respectively.

The following clauses will describe them in details.
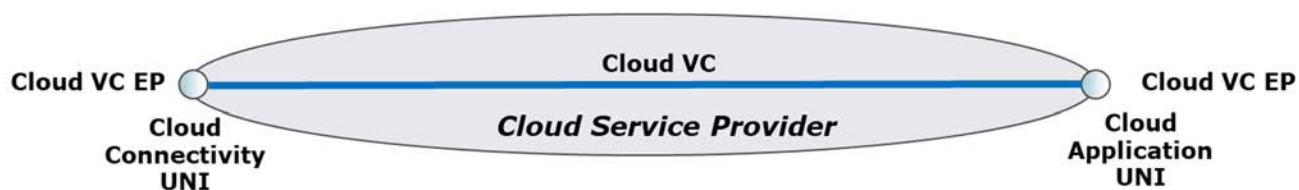
(a) Cloud VC between two end points residing on the resources of a Cloud SP

(b) Cloud VC between two end points residing on the resources of two different Operators

Figure 7-1: Cloud Virtual Connection Type

7.2   Cloud Virtual Connection

The Cloud VC is a cross connect between two or more Cloud VC EPs. The Cloud VC could be an EVC, LSP, IP VPN or SD-WAN connection. Identifiers of Cloud VC EPs associated with this Cloud VC, connection type, SLS, redundancy, connection start t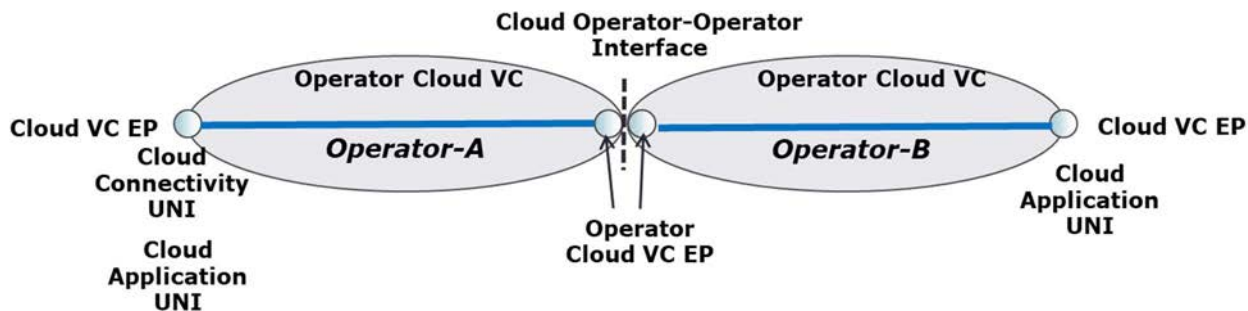ime, connection duration, connection period, billing options, maximum size of cloud service packets, administrative and operational states are among the attributes of Cloud VC.

As an example, a Cloud VC can terminate at a single VM with Cloud Application Interface as depicted in Figure 7-2 (a). Similarly, Cloud VC can connect multiple VMs via multiple sessions as depicted in Figure 7-2 (b) where a virtual switch routes traffic to destination VMs.

(a)

(b)
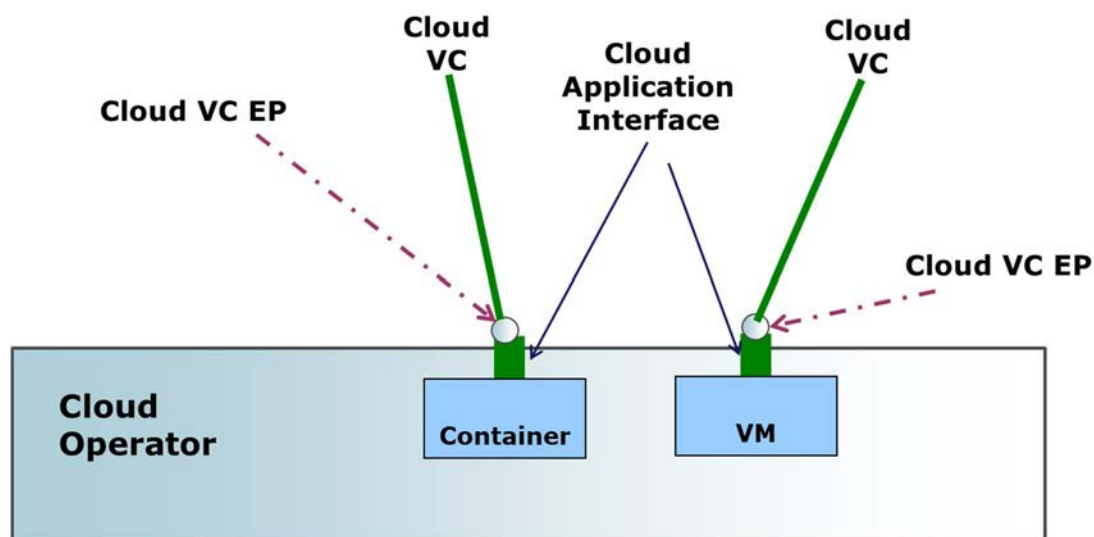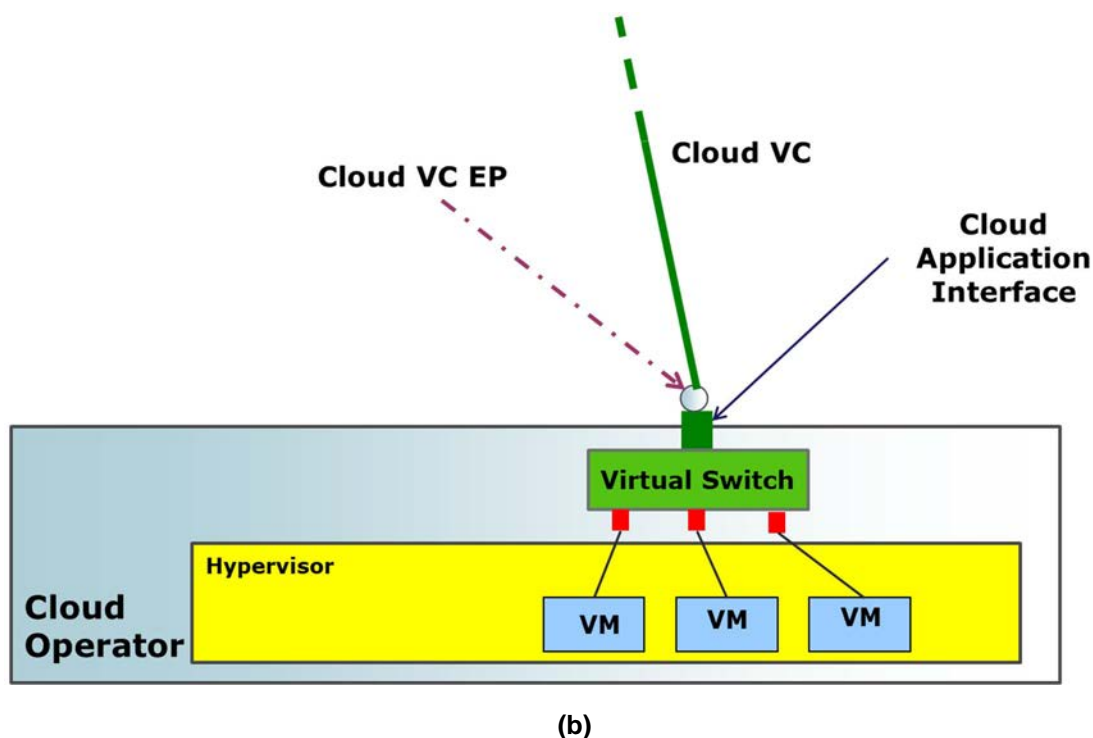
Figure 7-2: Cloud VC

Some or all of Cloud VC attributes can be modified on-demand, depending on the implementation.

7.3   Cloud Virtual Connection End Point

The Cloud VC is an association of two or more Cloud VC EPs. The Cloud VC could be, for example, an EVC [i.4], IP Virtual Connection [i.5] or SD-WAN Virtual Connection [i.7]. Identifiers of Cloud VC EPs associated with this Cloud VC, connection type, Service Level Specification (SLS), redundancy, connection start time, connection duration, connection period, billing options, maximum size of cloud service packets transmitted over Cloud VC, administrative and operational states are among the properties of Cloud VC.

The identifier of UNI or ENNI, bandwidth profile, parameters of security functionalities, administrative state and operational state are among the properties of Cloud VC EP.

Some or all of Cloud VC EP attributes can be modified on-demand, depending on the implementation.

7.4   Operator Cloud Virtual Connection

The Cloud VC may cross multiple Operator domains as depicted in Figure 7-3. Each domain will carry a component of the Cloud VC. The component in each Operator domain is called Operator Cloud VC.

Operator Cloud VC is another Cloud VC. It is called differently to identify the connection whether it is a component or an end-to-end connection.

Figure 7-3: Segments of Cloud VC crossing multiple Operators

The Operator Cloud VC is a cross connect between two Cloud VC EPs. The Operator Cloud VC could be an Operator Virtual Connection (OVC), LSP, IP VPN connection segment, or SD-WAN connection.

Identifiers of Operator Cloud VC EPs associated with this Operator Cloud VC, connection type, SLS, redundancy, connection start time, connection duration, connection period, billing options, maximum size of cloud service packets, administrative and operational states are among the attributes of Operator Cloud VC.
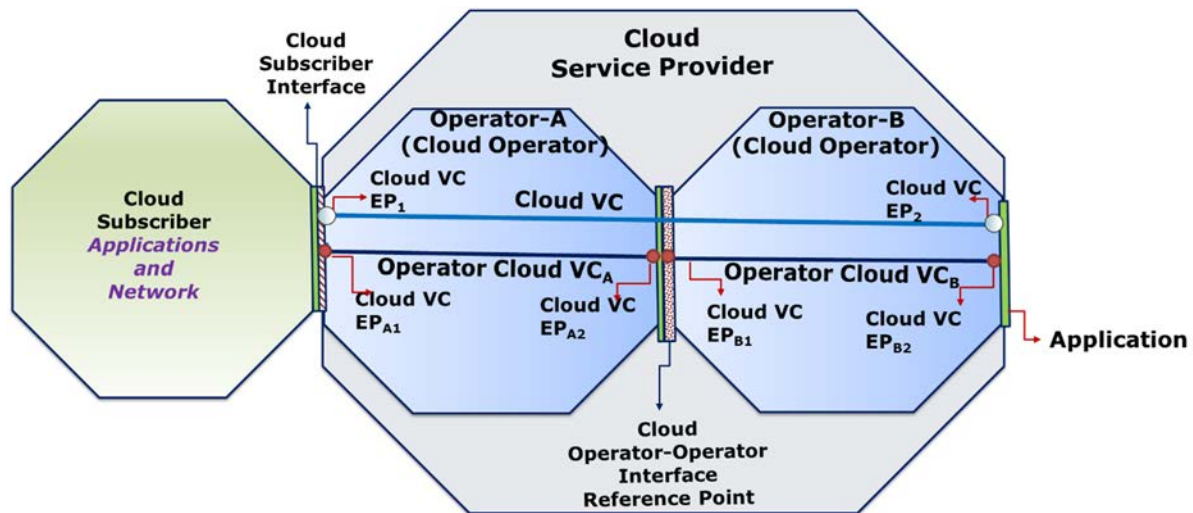
Some or all of Operator Cloud VC attributes can be modified on-demand, depending on the implementation.

7.5 Example for Cloud Virtual Connection and End Points

As an example, SD-WAN connection and connection end point attributes are described in Tables 2 and 5 of [i.7].

8 Overview of NFV Architecture

8.1 Introduction

This clause summarizes ETSI NFV architectural constructs, namely interfaces, link, and link end points; and maps them to Cloud Services Architecture constructs as described in clauses 6 and 7.

8.2 NF Forwarding Graph

ETSI GS NFV 002 [i.16] defines an NF Forwarding Graph (FG) consisting of NFs and logical links that connect them together as depicted in Figure 8-1. End points are connected to NFs via infrastructure resulting in a logical interface between end points and NFs.
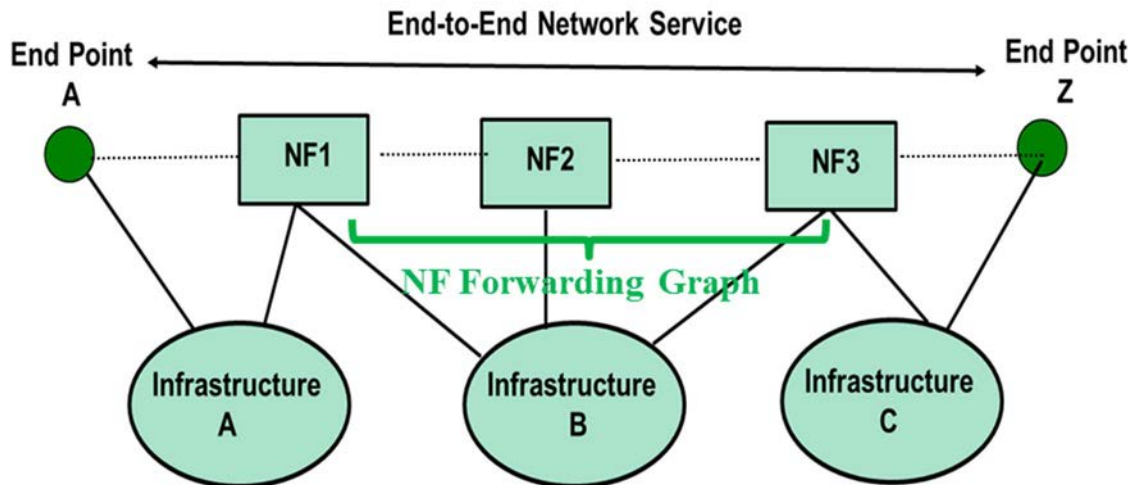
Figure 8-1: Forwarding Graph

The End-to-End Network Service with its End Points in Figure 8-1 may be mapped to a Cloud Virtual Connection and its End Points.

Virtual Link (VL) attributes defined in ETSI GS NFV-IFA 014 [i.10] are a subset of SD-WAN Connection (SWVC) and SD-WAN Connection (SWVC) End Point attributes as described in Tables 7-1 and 7-2. Similarly, the VL attributes are a subset of Cloud Service Connection (i.e. Cloud Virtual Connection) in OCC 1.0 Reference Architecture [i.1]. However, there could be multiple Cloud VCs between two VNFs or VNFCs while there is only one VL defined between two VNFs when there is no VL protection. When there is a VL protection, two links are terminated at each VNF where each VL is supported by a different network, as described in ETSI GS NFV-MAN 001 [i.11].

8.3   SWA Interfaces

ETSI GS NFV-SWA 001 [i.12] defines SWA-1 as the interface between two VNFs as illustrated in Figure 8-2.
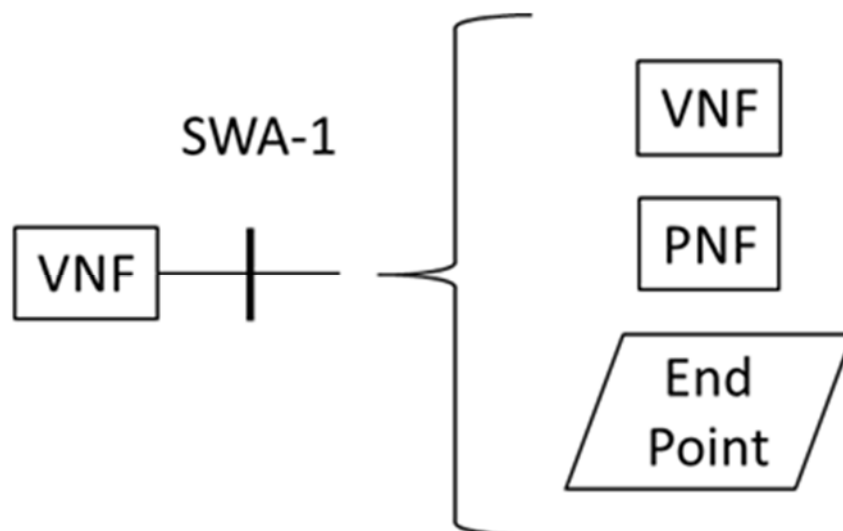
Figure 8-2: SWA-1 Interfaces [i.10]

SWA-1 interface enables communication between various network functions within the same or different network service. They may represent data and/or control plane interfaces of the network functions (VNF, PNF). The SWA-1 interface is between two VNFs, a VNF and a PNF, or between a VNF and an End Point. A VNF may support more than one SWA-1 interface.

Furthermore, ETSI GS NFV-SWA 001 [i.12] defines SWA-2 as the interface between two VNFCs, and SWA-5 (Vn-Nf) as the interface between VNFC and the NFVI hosted execution environment as depicted in Figures 8-3 and 8-4. These are internal interfaces of VNF.
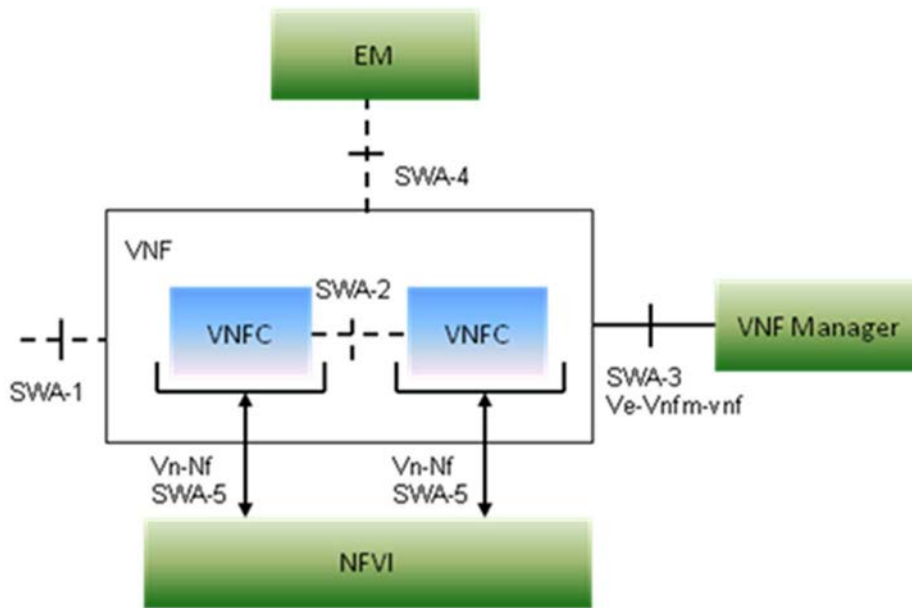
Figure 8-3: SWA-2 and SWA-5 Interfaces (ETSI GS NFV-IFA 014 [i.10])
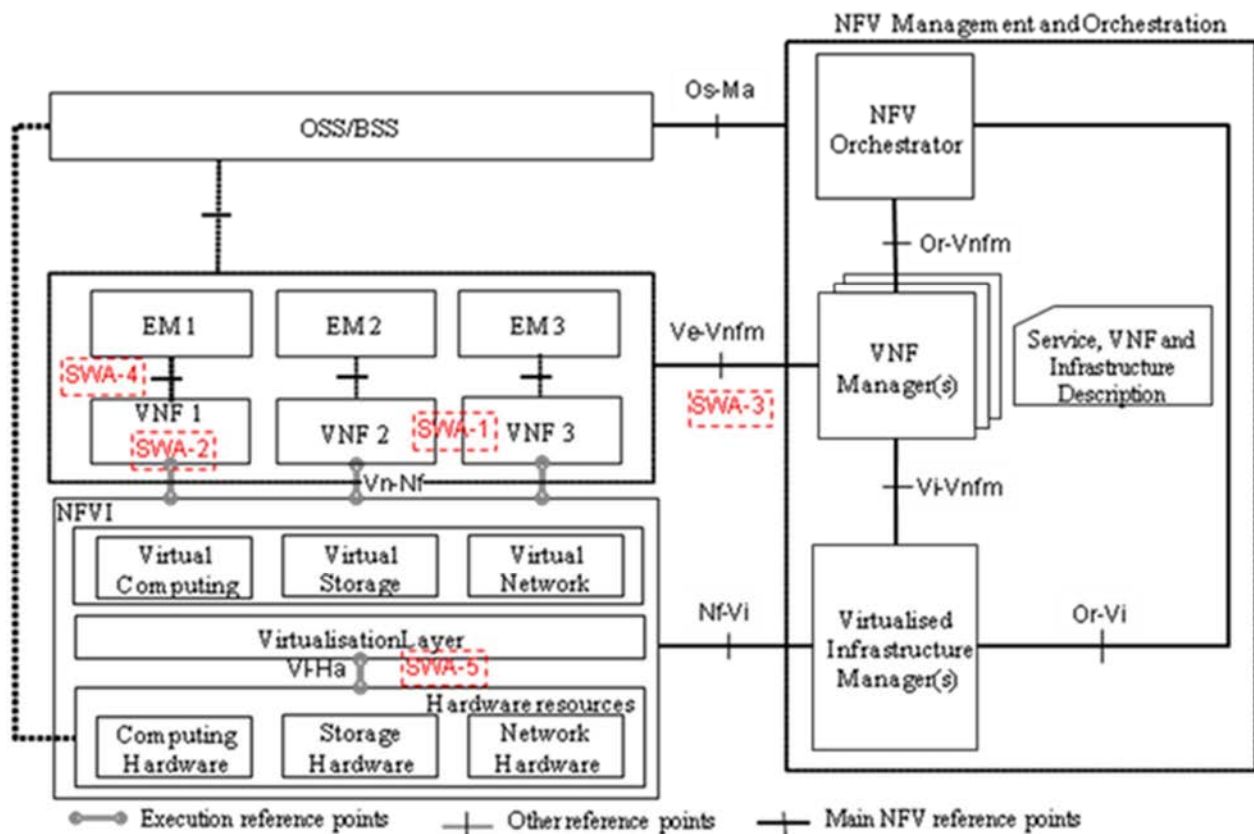
Figure 8-4: SWA Interfaces (ETSI GS NFV-SWA 001 [i.12])

ETSI GS NFV-SWA 001 [i.12] does not define SWA-1 attributes, but defines SWA-1 as the external VNF interface. Therefore, SWA-1 can be mapped to the Application Interface of Cloud Services. A VNF can have multiple SWA-1s. Similarly, a VNF can have multiple Application Interfaces. Cloud Service Interface (i.e. Application Interface) attributes are defined in OCC 1.0 Reference Architecture [i.1].

On the other hand, there are no corresponding Cloud Services Architecture constructs for SWA-2 and SWA-5 since these are internal interfaces.

8.4   NFV Framework Reference Points

ETSI GS NFV-INF 004 [i.13] defines NFV Framework Reference Points as in Table 8-1 and Figure 8-5.

Table 8-1: NFV Framework Reference Points

INF Ref point	Ref point type	Description and Comment
Ex-Nf	Traffic Interface	This is the reference point between the infrastructure network domain and any existing and/or non-virtualised network. This reference point also carries an implicit reference point between VNFs and any existing and/or non-virtualised network.
[Vl-Ha]/CSr	Execution Environment	The framework architecture shows a general reference point between the infrastructure 'hardware' and the virtualisation layer. This reference point is the aspect of this framework reference point presented to hypervisors by the servers and storage of the compute domain. It is the execution environment of the server/storage.
[Vi-Ha]/Nr	Execution Environment	This is a general reference point between the infrastructure 'hardware' and the virtualisation layer. While the infrastructure network has 'hardware', it is often the case that networks are already layered (and therefore virtualised) and that the exact choice of network layering may vary without a direct impact on NFV. The infrastructure architecture treats this aspect of the Vi-Ha reference point as internal to the infrastructure network domain.
Ha/CSr-Ha/Nr	Traffic Interface	This is the reference point between the infrastructure network domain and the servers/storage of the compute domain.

The interfaces in Table 8-1 are internal interfaces for the Cloud Services Architecture. Ex-Nf can become an external interface of a Cloud Operator if the infrastructure network domain is provided by one Operator and an existing and/or non-virtualised network provided by another Operator. This interface can be used externally by Operators as Cloud Operator-Operator Interface, if desired.

[Vl-Ha]/CSr and [Vl-Ha]/Nr are internal interfaces between the infrastructure hardware and the virtualisation layer. This interface is also an internal interface for Cloud Services. Cloud Operators offer either a virtualised platform or an application to the end user. It may be possible for a user to bring his/her hardware and expect to run Cloud Services offered by a Cloud SP on top it. However, the platform interface to the hardware is still an internal interface for the Cloud SP.

Ha/CSr-Ha/Nr is the interface between the infrastructure network domain and the servers/storage of the compute domain. This interface is also an internal interface for the Cloud SP.
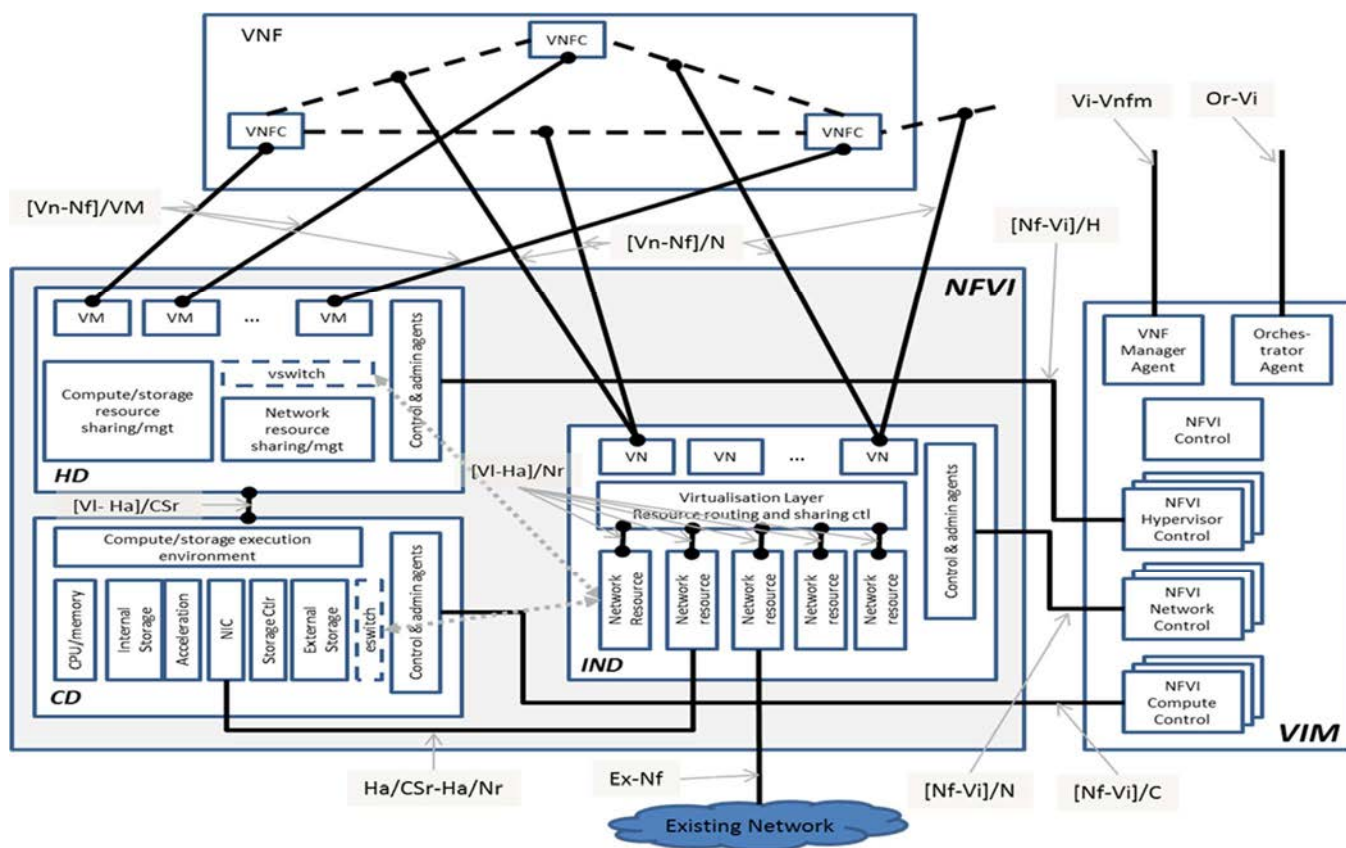
Figure 8-5- NFV Reference Points [i.11]

8.5   Container and Infrastructure Interfaces

ETSI GS NFV-INF 004 [i.13] and ETSI GS NFV-INF 001 [i.14] define Container and Infrastructure interfaces as depicted in Table 8-2 and Figure 8-6. The [Vn-Nf]/VN and [Vn-Nf]/VM] interfaces are defined as container interfaces.

Note that [Vn-Nf]/VN and [Vn-Nf]/VM] reference points rely on the de facto industry runtime solutions such as Docker® and are not defined in ETSI NFV Release 2 and 3.

NOTE: Docker is a registered trademarks of Docker, Inc.

ETSI GR NFV-IFA 029 [i.15] analyses management and orchestration of VNFs deployed in containers and recommends enhancements of the NFV architecture based on a container image on top of the shared OS kernel, in a parent virtualisation container or on bare metal.

The [Vn-Nf]/VN and [Vn-Nf]/VM interfaces as defined in Table 8-2 can be mapped to the Cloud Application Interface. Interfaces of containers on top of a shared OS, in a parent virtualisation container or bare metal are also expected to map to the Cloud Application Interface.

Table 8-2: NFV Framework Reference Points [i.14]

INF Ref point	Ref point type	Description and Comment
[Vn-Nf]/VM	Execution Environment	This reference point is the Virtual Machine (VM) container interface which is the execution environment of a single VNFC instance.
[Vn-Nf]/VN	Execution Environment	This reference point is the Virtual Network (VN) container interface (e.g. an E-Line or E-LAN) which carrying communication between VNFC instances. Note that a single VN can support communication between more than a single pairing of VNFC instances (e.g. an E-LAN VN).
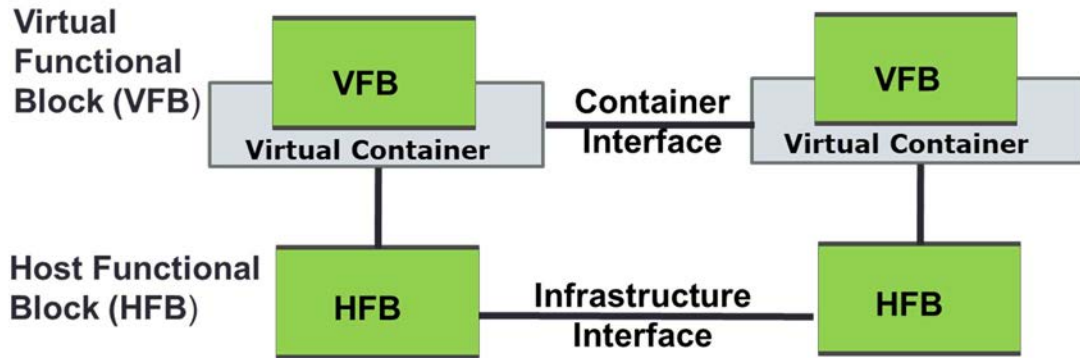
Figure 8-6: Container and Infrastructure Interfaces

8.6   ETSI GS NFV-IFA 022 Examples

ETSI GS NFV-IFA 022 [i.8] describes an EvCPE (Enterprise vCP) service which is installed with VNF has two sites (Figure 8-7). The vCPE is in one site and the vAPL is in another site. The virtual link between the VNF is supported across a WAN. Both vAPL interface and vCPE interface map to Cloud Application Interface.

The logical link between vCPE and vAPL, or between VNFs can be mapped to a Cloud VC.

Figure 8-7: vCPE and vAPL interfaces

9   Mapping of Architectural Constructs and Gaps

Mapping of architectural constructs of NFV and Cloud Services Architecture described in the clause 8 are summarized in Table 9-1.

Table 9-1: Mapping of NFV and Cloud Services Architectural Constructs

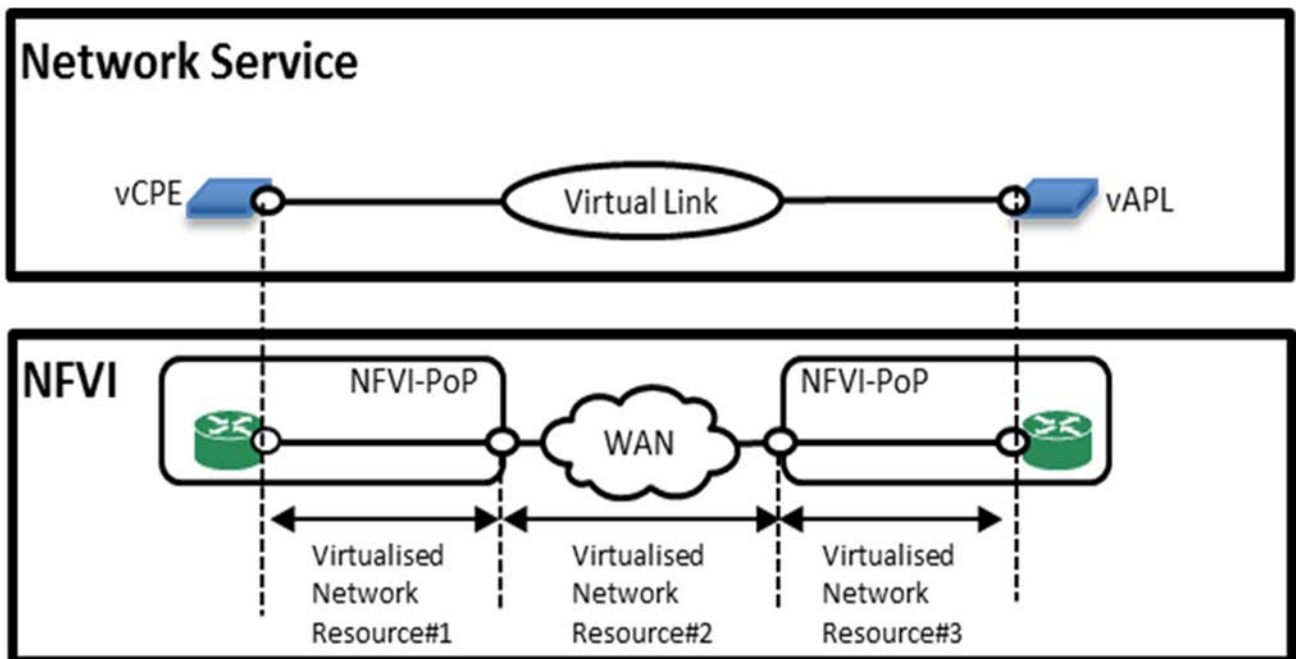| Architectural Construct	NFV Construct	Cloud Services Architecture Construct
User Interface		Cloud User Interface
Operator-Operator Interface	Ex-Nf	Cloud Operator-Operator Interface
Application Interface	vAPL Interface	Cloud Application Interface
Connection	Virtual Link	Cloud VC
Connection End Point	End Point	Cloud VC EP
VM Interface	(Vn-Nf)/VM	Cloud Application Interface
Virtual Network (VN) Container Interface between VNFC instances	(Vn-Nf)/VN	Cloud Application Interface
Interface between two VNFs	SWA-1	Cloud Application Interface

Cloud User Interface as described in clause 6.1 consists of connectivity and application functions supported by NFVI and VNF. On the other hand, there is no user interface defined to represent the combination of NFVI and VNF by ETSI NFV architecture.

Ex-Nf interface can be positioned as the Operator-Operator Interface.

10   Recommendations for ETSI NFV Architecture

10.1   Introduction

Mapping between constructs of ETSI NFV Architecture and Cloud Services Architecture is described in Table 9-1. Preliminary attributes of interfaces, connection, and connection end points for Cloud Services architecture are given in OCC 1.0 Reference Architecture [i.1]. On the other hand, ETSI NFV has not defined attributes for these architectural constructs except the attributes for Virtual Link. It is recommended that these architectural constructs (i.e. Ex-Nf, vAPL, End Point, Vn-Nf/VM, Vn-Nf/VN, and SWA-1) are defined with their attributes. This should help greatly the management of ETSI NFV components in addition to the development of Cloud Services.

10.2   Interfaces

Further work on Ex-Nf and Virtual Link interfaces are recommended:

- Ex-Nf is defined as the reference point between the infrastructure network domain and any existing and/or non-virtualised network. It is recommended that Ex-Nf definition is expanded such that it can be used as the interface between two Operators.

- ETSI NFV defines Virtual Link (VL), but does not define its interface. It is recommended that the VL interface is defined and the mapping of VL to connection is described. This will align ETSI NFV architecture with the implementations in the industry and Cloud Services architecture.

10.3   Connection and Connection End Points

In ETSI NFV architecture, there is no concept of connection and connection end points, but end-to-end network service and end points. However, the Virtual Link (VL) can be considered as a connection.

By mapping a VL to a connection, the end-to-end network service can become a Cloud VC. Its end points will become Cloud VC end points.

It is recommended that:

- connection and connection end points are added into the ETSI NFV architecture; and

- relationship between VL and connection is defined.

10.4   NFV-MANO

Management of Cloud Services requires management of all service components (i.e. interfaces, connection, connection segments, and connection end points) that are virtualised and non-virtualised. After ordering and provisioning of a Cloud Service, the run-time management functions of a service include:

- service fault management;

- service performance management;

- service security; and

- service testing.

NFV-MANO deals with the management of Network Function Virtual Infrastructure (NFVI), Network Services (NSs) and Virtual Network Functions (VNFs), via NFVO, VNFM and VIM, but ignores the run-time management of some of its components in Table 9-1 since it is considered to be outside the scope of NFV-MANO:

- Ex-Nf.

- vAPL Interface.

- End Point.

- (Vn-Nf)/VM.

- (Vn-Nf)/VN.

- SWA-1.

It is recommended that the run-time management of these components are included in the NFV-MANO. This should help the development of management systems for Cloud Services.

11   Conclusion

In the present document, Connection-Based Virtual Services' use cases and architectural components are described. ETSI NFV architectural components are briefly described and mapped into the architectural components of Connection-Based Virtual Services.

ETSI NFV has not defined attributes of some of architectural constructs (i.e. Ex-Nf, vAPL, End Point, (Vn-Nf)/VM, (Vn-Nf)/VN, and SWA-1) except the attributes for Virtual Link. Defining these architectural constructs with their attributes should help greatly the management of ETSI NFV components in addition to the development of Cloud Services.

The run-time management of some of ETSI NFV architectural components (i.e. Ex-Nf, vAPL, End Point, (Vn-Nf)/VM, (Vn-Nf)/VN, and SWA-1) are not included in NFV-MANO. Addressing the run-time management of these components in NFV-MANO is recommended to help the development of management systems for Connection-based Virtual Services.

The present documentation recommendations are summarized in Table 11-1.

Table 11-1: ETSI GR NFV-EVE 016 (the present document) Recommendations

Identifier	Recommendation Description	Comments and/or Traceability
CON-BASED-VS-REC-001	It is recommended that the following architectural constructs are defined with their attributes: • Ex-Nf. • vAPL Interface. • End Point. • (Vn-Nf)/VM. • (Vn-Nf)/VN. • SWA-1.	
CON-BASED-VS-REC-002	It is recommended that Ex-Nf definition is expanded such that it can be used as the interface between two Operators.	
CON-BASED-VS-REC-003	It is recommended that connection and connection end points are added into the ETSI NFV architecture.	
CON-BASED-VS-REC-004	It is recommended that relationship between VL and connection is defined.	
CON-BASED-VS-REC-005	It is recommended that the run-time management of the following ETSI NFV architectural components are included in the NFV-MANO: • Ex-Nf. • vAPL Interface. • End Point. • (Vn-Nf)/VM. • (Vn-Nf)/VN. • SWA-1.	

Annex A:
Change History

Date	Version	Information about changes
October, 2017	0.0.1	ToC
November, 2017	0.0.2	TOC
March 31, 2019	0.0.3	TOC
February 20, 2020	0.0.9	Clauses 3-8 are added.
April 4, 2020	0.0.10	Clauses 9,10 and 11 are added.
May 13, 2020	0.0.11	Incorporated comments for the Stable Draft
May 24, 2020	0.0.12	Incorporated comments from editHelp!

History

Document history		
V1.1.1	September 2020	Publication