Contribution Number

The following (blank) line has the fields:

MEF Specification
MEF x draft 0.1

Cloud Services Architecture
Technical Specification

April 2018

Caution – this draft represents MEF work in progress and is subject to change.

Disclaimer

Table of Contents

List of Figures

List of Tables

1List of Contributing Members

The following members of the MEF participated in the development of this document and have requested to be included in this list.

Editor Note 1: This list will be finalized before Letter Ballot. Any member that comments in at least one CfC is eligible to be included by opting in before the Letter Ballot is initiated. Note it is the MEF member that is listed here (typically a company or organization), not their individual representatives.

- ABC Networks
- XYZ Communications

2Abstract

This document defines overall architecture for Cloud Services.

3Terminology and Abbreviations

This section defines the terms used in this document. In many cases, the normative definitions to terms are found in other documents. In these cases, the third column is used to provide the reference that is controlling, in other MEF or external documents.

In addition, terms defined in MEF X [1] are included in this document by reference, and are not repeated in the table below.

Term	Definition	Reference
CaaS	Communications as a Service	[2]
Cloud UNI	Cloud User Network Interface	In his document
Cloud ENNI	Cloud External Network Network Interface	In this document
cI	Cloud Interface	In this document
cP	Cloud Provider	[2]
cSUI	Cloud Service User Interface which is also called Cloud UNI	[2] and this document
cSO	Cloud Service Operator	[2]
cSP	Cloud Service Provider	[2]
cSOcSOI	Cloud Service Operator Cloud Service Operator Interface which is also called as Cloud ENNI	In this document
cC	Cloud Carrier	[2]
cSC	Cloud Service Connection	[2]
cSCEP	Cloud Service Connection End Point	[2] and this document
cSO-c	Cloud Service Operator Connection	[2] and this document
cSOCEP	Cloud Service Operator Connection End Point	[2] and this document
NaaS	Network as a Service	[2]
PaaS	Platform as a Service	[1,2]
SaaS	Software as a Service	[1,2]
SECaaS	Security as a Service	[2]
VM	Virtual Machine	[4]
VNF	Virtual Network Function	[4]

Table 1 – Terminology and Abbreviations

4 Compliance Levels

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 (RFC 2119 [15], RFC 8174[16]) when, and only when, they appear in all capitals, as shown here. All key words must be in bold text.

Items that are **REQUIRED** (contain the words **MUST** or **MUST NOT**) are labeled as **[Rx]** for required. Items that are **RECOMMENDED** (contain the words **SHOULD** or **SHOULD NOT**) are labeled as **[Dx]** for desirable. Items that are **OPTIONAL** (contain the words **MAY** or **OPTIONAL**) are labeled as **[Ox]** for optional**.**

Editor Note 2: The following paragraph will be deleted if no conditional requirements are used in the document.

A paragraph preceded by **[CRa]<** specifies a conditional mandatory requirement that **MUST** be followed if the condition(s) following the "<" have been met. For example, "**[CR1]<**[D38]" indicates that Conditional Mandatory Requirement 1 must be followed if Desirable Requirement 38 has been met. A paragraph preceded by **[CDb]<** specifies a Conditional Desirable Requirement that **SHOULD** be followed if the condition(s) following the "<" have been met. A paragraph preceded by **[COc]<** specifies a Conditional Optional Requirement that **MAY** be followed if the condition(s) following the "<" have been met.

5 Numerical Prefix Conventions

Editor Note 3: This section will be deleted if no numerical prefixes are used in the document.

This document uses the prefix notation to indicate multiplier values as shown in Table 2.

Decimal		Binary	
Symbol	**Value**	**Symbol**	**Value**
K	10^3	Ki	2^{10}
M	10^6	Mi	2^{20}
G	10^9	Gi	2^{30}
T	10^{12}	Ti	2^{40}
P	10^{15}	Pi	2^{50}
E	10^{18}	Ei	2^{60}
Z	10^{21}	Zi	2^{70}
Y	10^{24}	Yi	2^{80}

Table 2 – Numerical Prefix Conventions

6 Introduction

MEF developed an implementation agreement, MEF 47 [3], to address the Carrier Ethernet connectivity to cloud applications. Later, Cloud Services Architecture was defined by OCC [2]. This specification builds on [2] and refines the architecture.

This specification describes overall architectural framework for MEF cloud services. Lifecycle Services Orchestration (LSO) of Cloud Services are out of scope. They will be addressed in another MEF spec.

7 Use Cases for Cloud Services

7.1 Access to Public Cloud Providers

Applications provided by a Public Cloud Provider (cP) can be accessed via Internet as described in Figure 1. Given Internet provides best effort service, we expect to see non-mission critical applications and applications that are less sensitive to network delay, jitter and loss are accessed via Internet.

Wireless network and Internet combination is also an alternative for accessing applications provided by Public Cloud Providers.

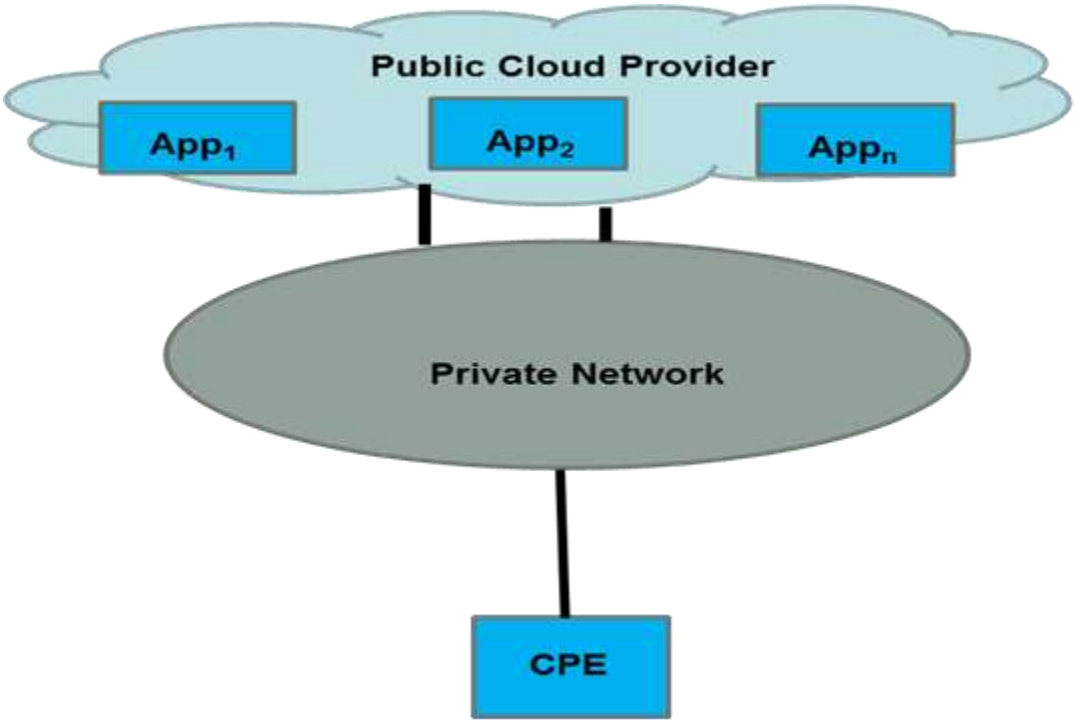
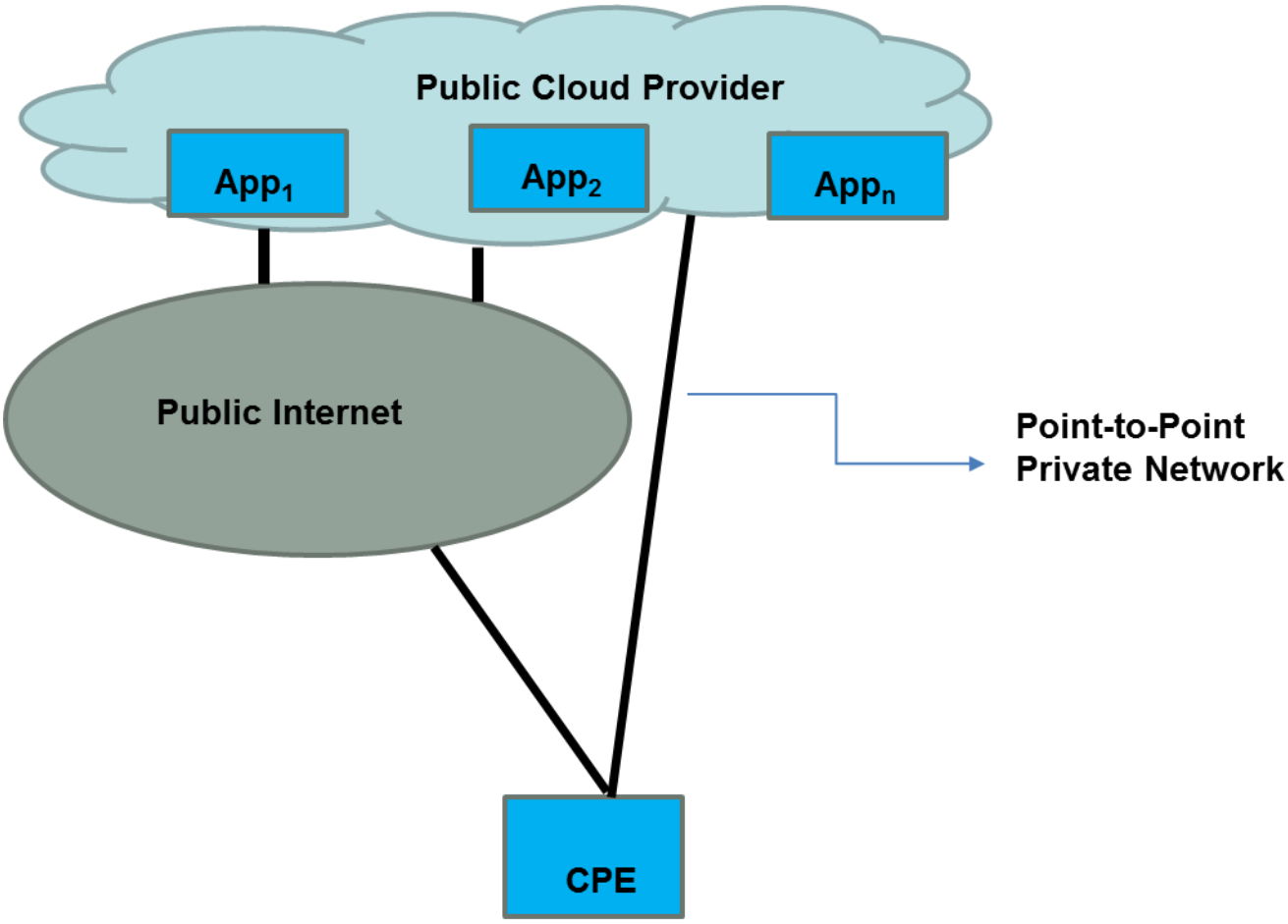


Figure 1 – Public Cloud Provider Access via Internet

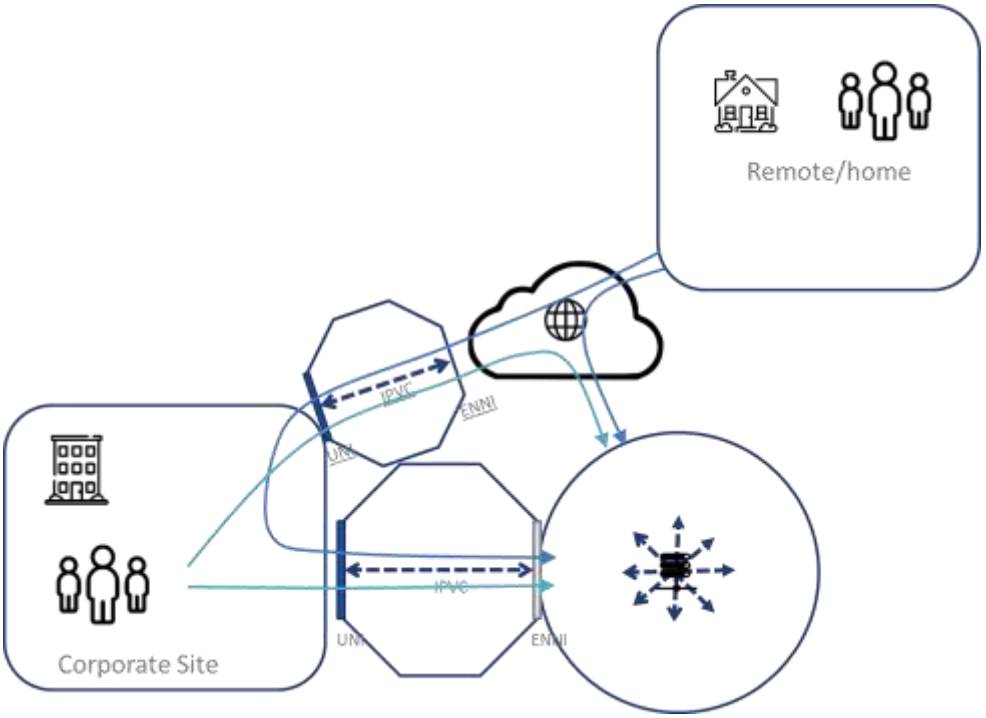
Cloud service subscribers are very likely to use private networks to access mission critical applications and applications that are sensitive to network delay, jitter and loss, where Internet is used as a back-up for connectivity as depicted in Figure 2.



202
203
204 **Figure 2 –** Public Cloud Provider Access via Private Network and Internet

205 Another use case for using Internet and Private Network for Public Cloud Provider access is de-
206 picted in Figure 3, where an employee of an enterprise may go thru the enterprise network first
207 and then access to the Public Cloud Provider or access the Public Cloud Provider directly via the
208 Internet. The interface between the enterprise and the Public Cloud Provider is expected to have
209 stricter security capabilities compared to the Public Cloud Provider's internet interface.

210 A branch office of an enterprise, that has no access to the enterprise's private network, may ac-
211 cesses to a virtual router provided by a public cP via Internet where the cP has a gateway to the
212 enterprise's private network providing connectivity to the enterprise's remaining branches.



IPVC: IP Virtual Connection

Figure 3 – Enterprise Employee Access to Public Cloud Provider

Via Internet, cloud users can access applications hosted by multiple cPs. The same access flexibility is desired over private networks, as depicted in Figure 4.

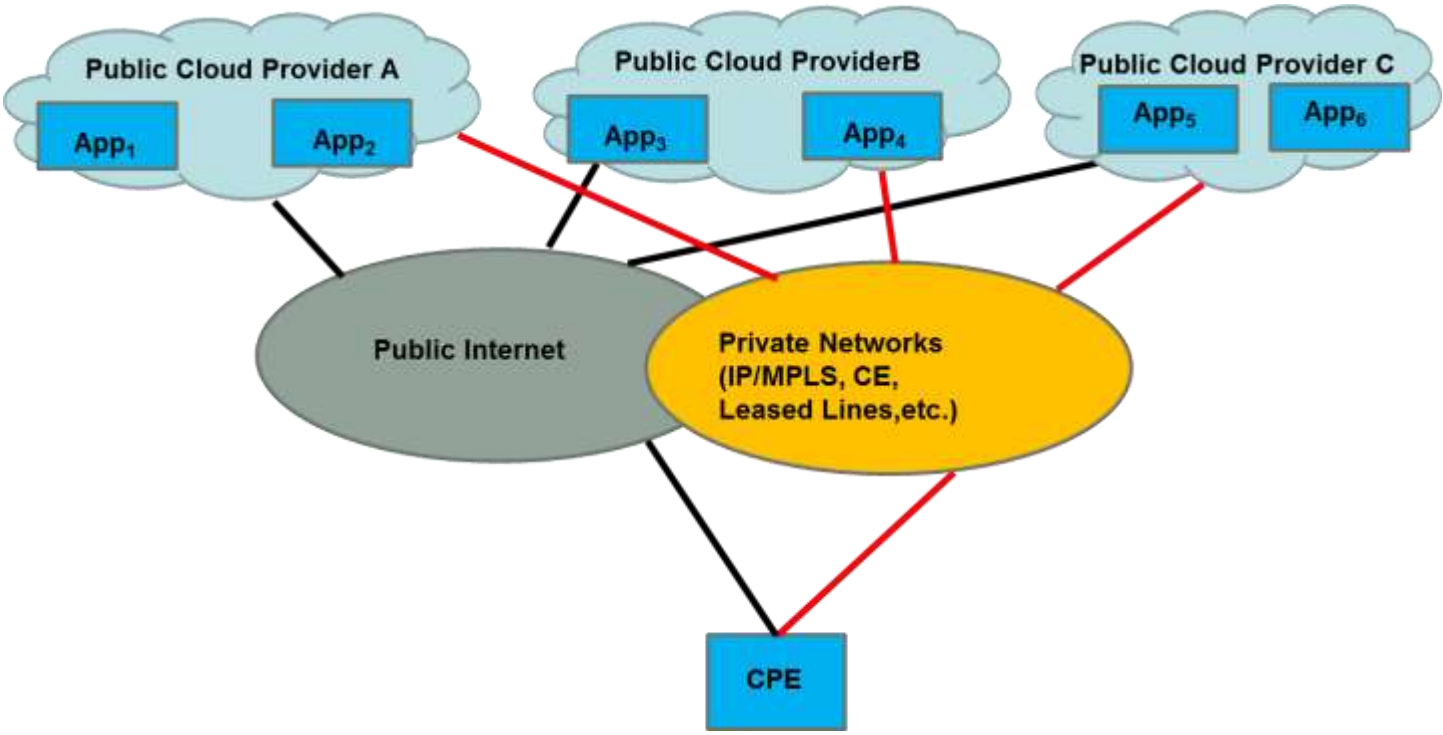


Figure 4 – Public Cloud Provider Access via Private Network and Internet

7.2 Access to Private Cloud Providers

Cloud applications and connectivity to the applications can be provided by a single Operator. The Operator's private network could be L1, L2, L3, wireless, overlay such as SD-WAN or their combinations. This is a common configuration for telecom service providers, as depicted in Figure 5.

Connectivity and applications can be provided by two different Operators as well.

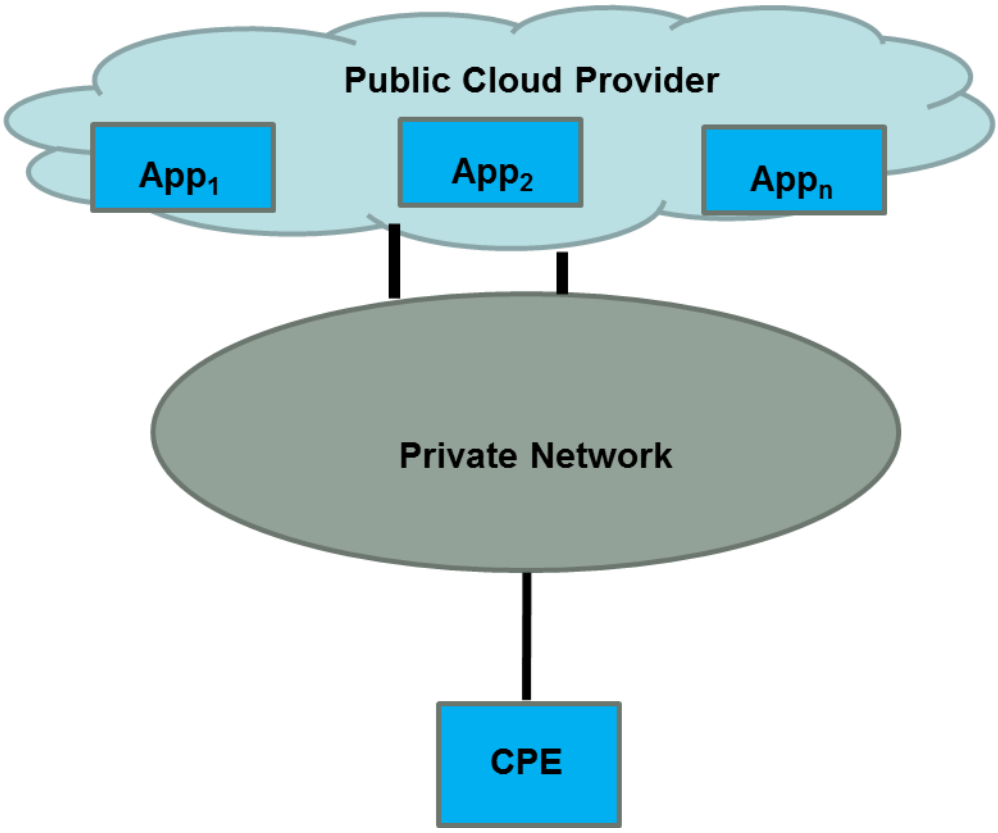


Figure 5 – Private Cloud Provider Access via Private Network

7.3 Access to Combination of Private and Public Cloud Providers

A Private Cloud Provider (Actors of Cloud Services) may team up with a Public Cloud Provider and offer applications hosted by the Public Cloud Provider to cloud users (subscribers) over its own private network. The cloud subscribers only interact with the Private Cloud Provider and are unaware of the locations of their applications, as depicted in Figure 6. The Cloud Provider with its own private network will play a role of Cloud Carrier (Actors of Cloud Services) as well.

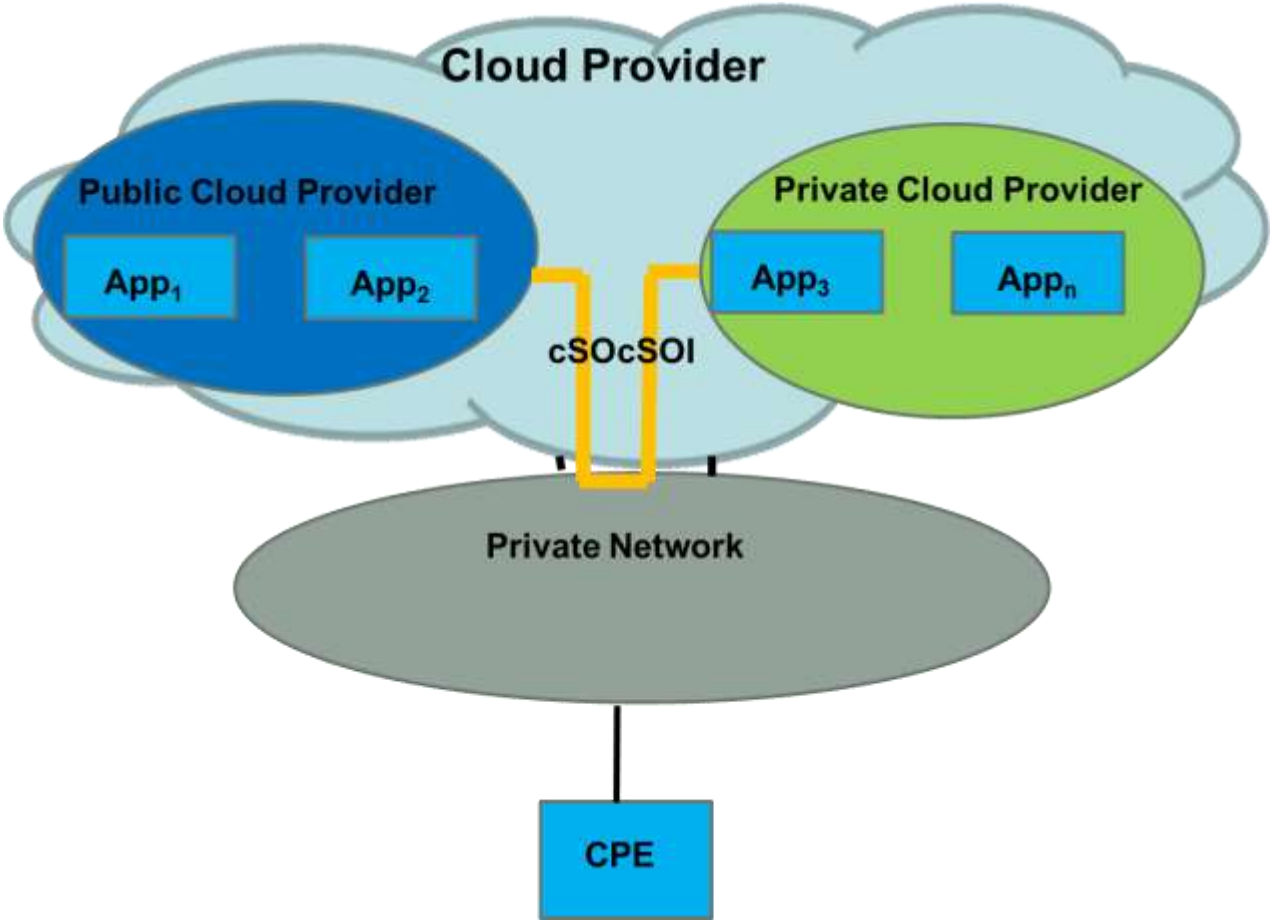


Figure 6 – Access to Private and Public Cloud Provider Combination via Private Network

7.4 Cloud Exchange Gateway

Establishing a gateway between two Cloud Carriers, a Cloud Carrier and Cloud Provider, or two Cloud Providers may not always be justified economically. A Cloud Exchange Gateway (cEGW) providing connectivity among all parties could be a viable alternative, as depicted in Figure 7.

Via cEGW, cloud subscribers will be able to move their virtualized components (e.g. applications/VNFs, VMs, containers, or their combinations) from one cP to another. They can also place their virtualized components in multiple cPs and establish service chains[1] among them.

[1] In this document, a Cloud Service component formed of connected multiple VNFs is called as 'Service Chain", instead of Network Service (NS) in ETSI NFV [4].

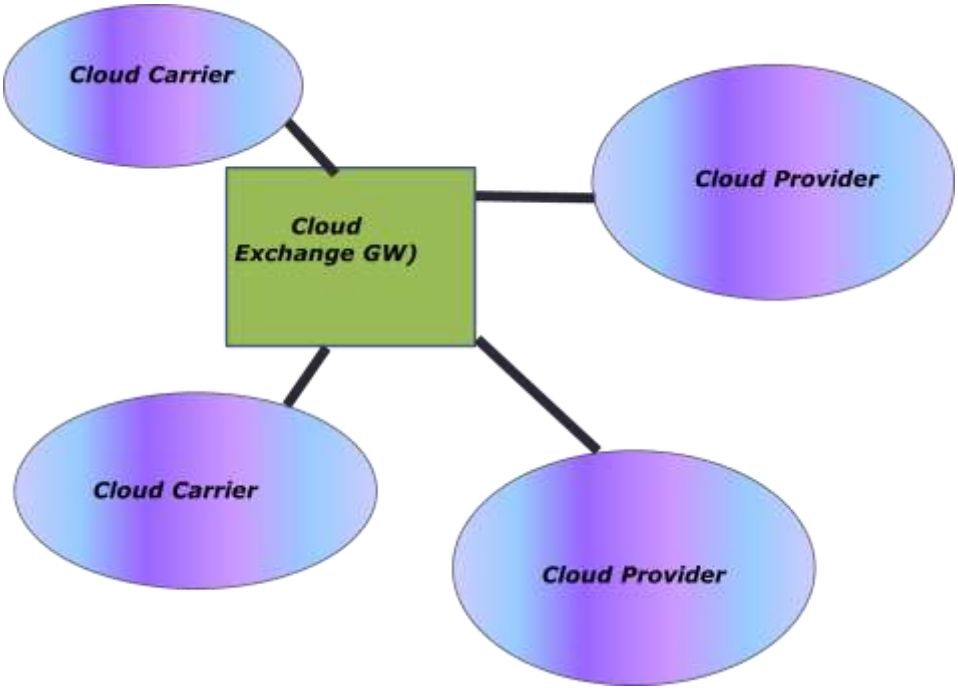


Figure 7 – Cloud Exchange Gateway among Cloud Carriers and Cloud Providers

8 Actors of Cloud Services

The key actors of Cloud Services are depicted in **Figure 8** where a Cloud Service Provider (cSP) is responsible for providing an end-to-end Cloud Service to a Cloud Service User/Subscriber using Cloud Carrier(s) and Cloud Provider(s) [2]. They are described as:

- Cloud Service: A service provided to a Cloud Subscriber using a shared pool of configurable and mobile resources on-demand (e.g., networks, servers, storage, applications) that is uncommon in legacy services.

- Cloud User/Subscriber/Consumer[2]: A person or organization that maintains a business relationship with and uses service from a Cloud Service Provider.

- Cloud Carrier: An intermediary that provides connectivity and transport between Cloud Providers and Subscribers or between Cloud Providers.

[2] In this document, user, subscriber and consumer are used synonymously.

- Cloud Provider: An entity that is responsible for making cloud applications available to Cloud Subscribers. It can be public or private.

- Cloud Service Provider: An entity that is responsible for the creation, delivery and billing of cloud services, and negotiates relationships among Cloud Providers, Cloud Carriers, Cloud Service Operators, and Cloud Subscribers. It is the single point of contact for the subscriber.

- Cloud Service Operator is an operator that provides a part of the end-to-end Cloud Service which is provided by a Cloud Service Provider.

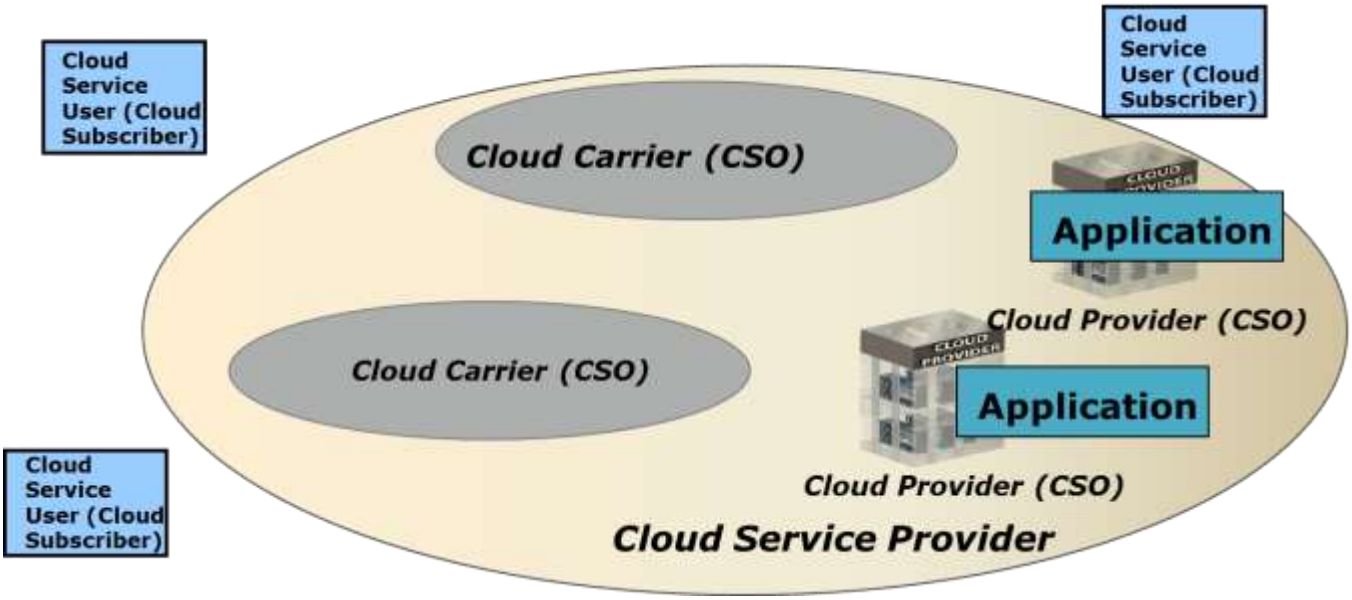


Figure 8 – Actors of Cloud Services

9 Characteristics of Cloud Services

Cloud Services provide similar or the same functionalities compared to their legacy counterparts, with greater flexibility in service order, provisioning and billing. For example, security service via a virtual firewall can be provided at customer premises, in a data center in the core network, or anywhere in between, based on the customer request. The firewall can be installed on demand and charged based on its usage.

Some of the characteristics are listed below. A Cloud Service,

- consists of virtualized components (VNFs) and non-virtualized components (PNFs),

- consists of network functions with just non-virtualized components (PNFs) or both virtualized components (VNFs) and non-virtualized components (PNFs);
- consists of applications built with virtualized components (VNFs);
- consists of connections provided by one or more Public Cloud Provider (s), Private Cloud Provider (s), and Network Operator (s) (i.e. Cloud Carriers);
- supports elasticity for on-demand service configurations by subscribers and locations of the service functionality;
- supports service monitoring and usage-tracking by subscribers;
- supports self-service by subscribers and collaboration among Cloud Providers;
- supports scalability of resources on-demand;
- supports various high availability options from physical layer to application layer; and
- supports "pay as you use" (i.e. usage based billing).

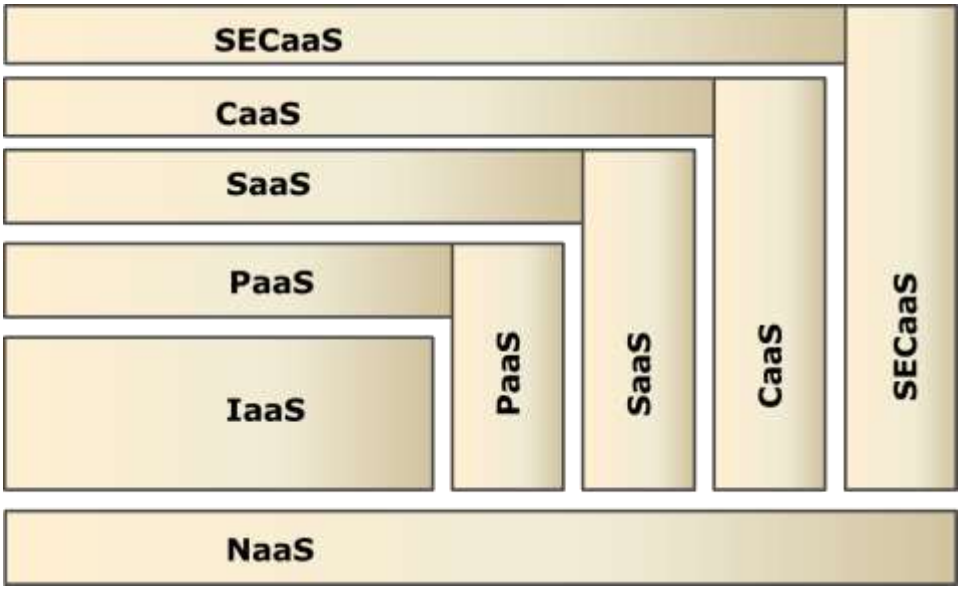
10 Cloud Services

A Cloud Service is an end-to-end service among Cloud Subscribers, Cloud Providers, and Cloud Carriers that can include virtual and non-virtual resources. The Cloud Services maybe grouped under Network as a Service (NaaS), Infrastructure as a Service (IaaS), Platform as Service (PaaS), Software as a Service (SaaS), Communications as a Service (CaaS) and Security as a Service (SECaaS) categories. Services in the same category are expected to have similar characteristics.

Fi

Figure 9 depicts an example of building cloud services in a hierarchical fashion starting with NaaS where each builds on the previous and provides services for the next in the hierarchy. The hierarchy from the bottom to the top would be NaaS, PaaS, IaaS, SaaS, CaaaS and SECaaS. It is also possible to skip the hierarchy and build on top of NaaS, such as building SaaS on top of NaaS, as depicted in **Fi**

Figure 9. This does not mean there is no infrastructure elements underneath. It means that there is no separate IaaS or PaaS or combination underneath.



Fi

Figure 9 – Cloud Services

10.1 Cloud Service Descriptions

10.2 NaaS

Network as a Service (NaaS) delivers assured and dynamic connectivity services via a virtual connection, and virtual or both physical and virtual service endpoints over one or more operators' networks. Such services enable users, applications and systems to create, modify, suspend/resume and terminate connectivity services through standardized APIs. These services are assured from both performance and security perspectives.

Some of NaaS characteristics are:

- Connectivity supported through homogenous or heterogeneous networks by one or more operators where one of the operators acting as cSP;
- On-demand network configuration capability;
- QoS-guarantee according to the negotiated service level agreement (SLA); and
- Connection security.

It is the responsibility of NaaS provider which is aCloud Carrier (cC), or cSP, to maintain and manage the network resources. It is possible that cSP may not own NaaS, but provides coordination with cC. NaaS offers network as a utility.

NaaS examples are:

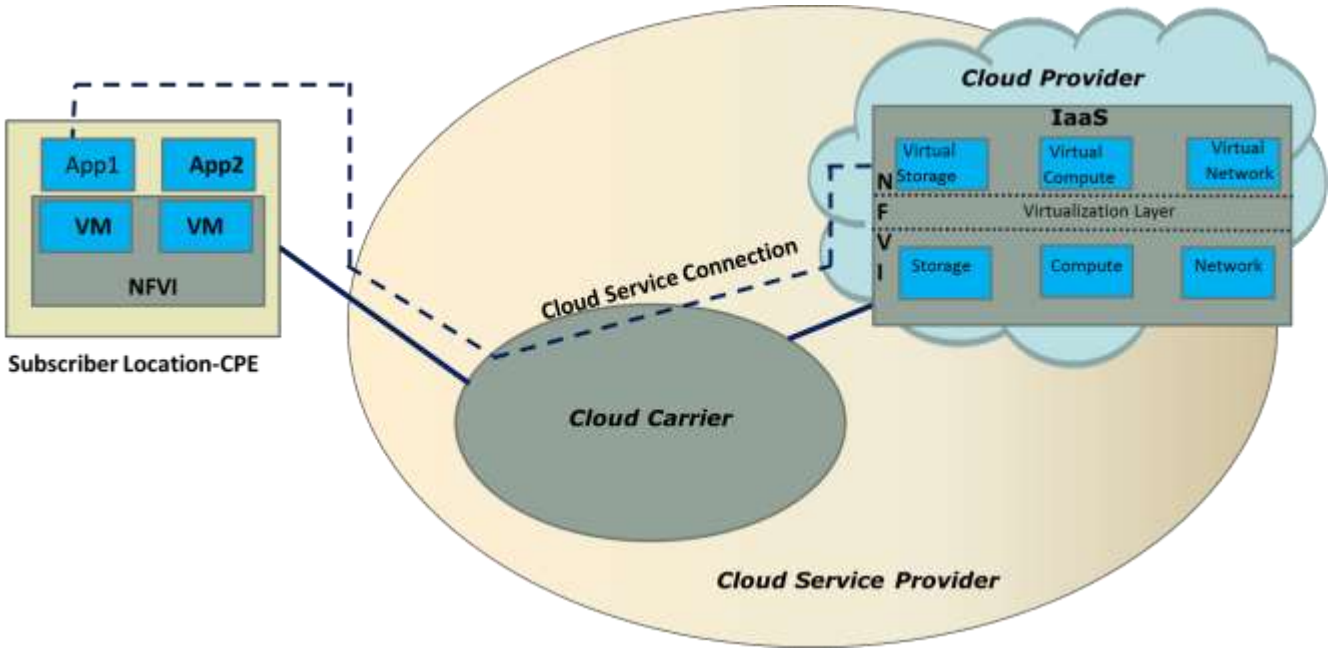
- MEF Carrier Ethernet Network Services [5]
- IP Network Services [6]
- SD-WAN [7]

10.3 IaaS

The capability provided to the subscriber via IaaS is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

In summary, an IaaS cP configures, deploys and maintains computing, storage and networking resources for user. Also, the IaaS cP provides the capability for users to use and monitor computing, storage and networking resources so that they are able to deploy and run arbitrary software.

An example IaaS is depicted in **Figure 10**. In this example, customer/subscriber may have a CPE with web browser and no virtualized platform accessing IaaS provided by a cP. The CPE may have a virtualized platform that is used in conjunction with the IaaS to run certain applications.



NFVI: Network Function Virtualization Infrastructure [8]

Figure 10- An example IaaS architecture

For example, Cloud Computing as an IaaS allows subscribers to provision computing and storage resources on-demand, specifically storage and virtual servers that can be accessed on demand. Virtual datacenters can be created from commodity servers, enabling subscribers to stitch together memory, I/O, storage, and computational capacity as a virtualized resource pool available over the network.

10.4 PaaS

By Platform as a Service (PaaS) [1], the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by a cP. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations as depicted in **Figure 11**.

PaaS can be a stand-alone development environment that does not include technical, licensing or financial dependencies on specific SaaS applications or web services. These development environments are intended to provide a generalized development environment.

PaaS can be application delivery-only environments that do not include development, debugging and test capabilities as part of the service, though they may be supplied offline. The services provided generally focus on security and on-demand scalability.

PaaS can be an Open platform as a service that does not include hosting as such, rather it provides open source software to allow a PaaS provider to run applications. Some open platforms let the developer use any programming language, any database, any operating system, any server, etc. to deploy their applications.

With PaaS, a scalable and high-performing network can be formed with a fully managed application platform for running and consolidating software applications and databases in the cloud.

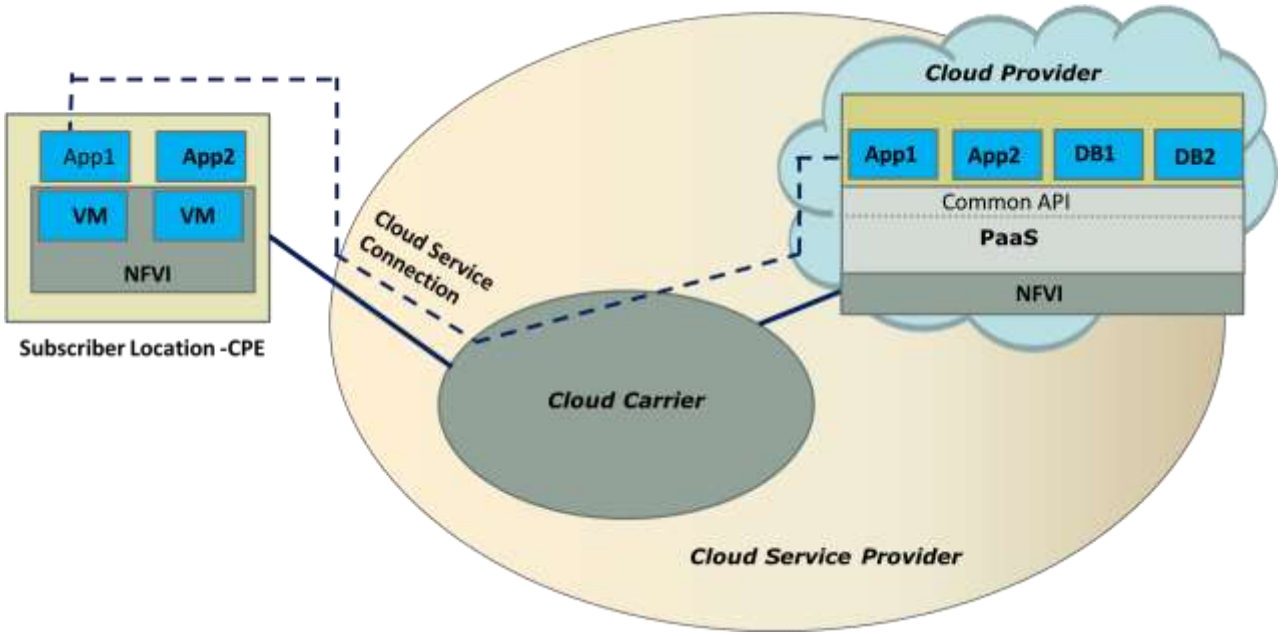
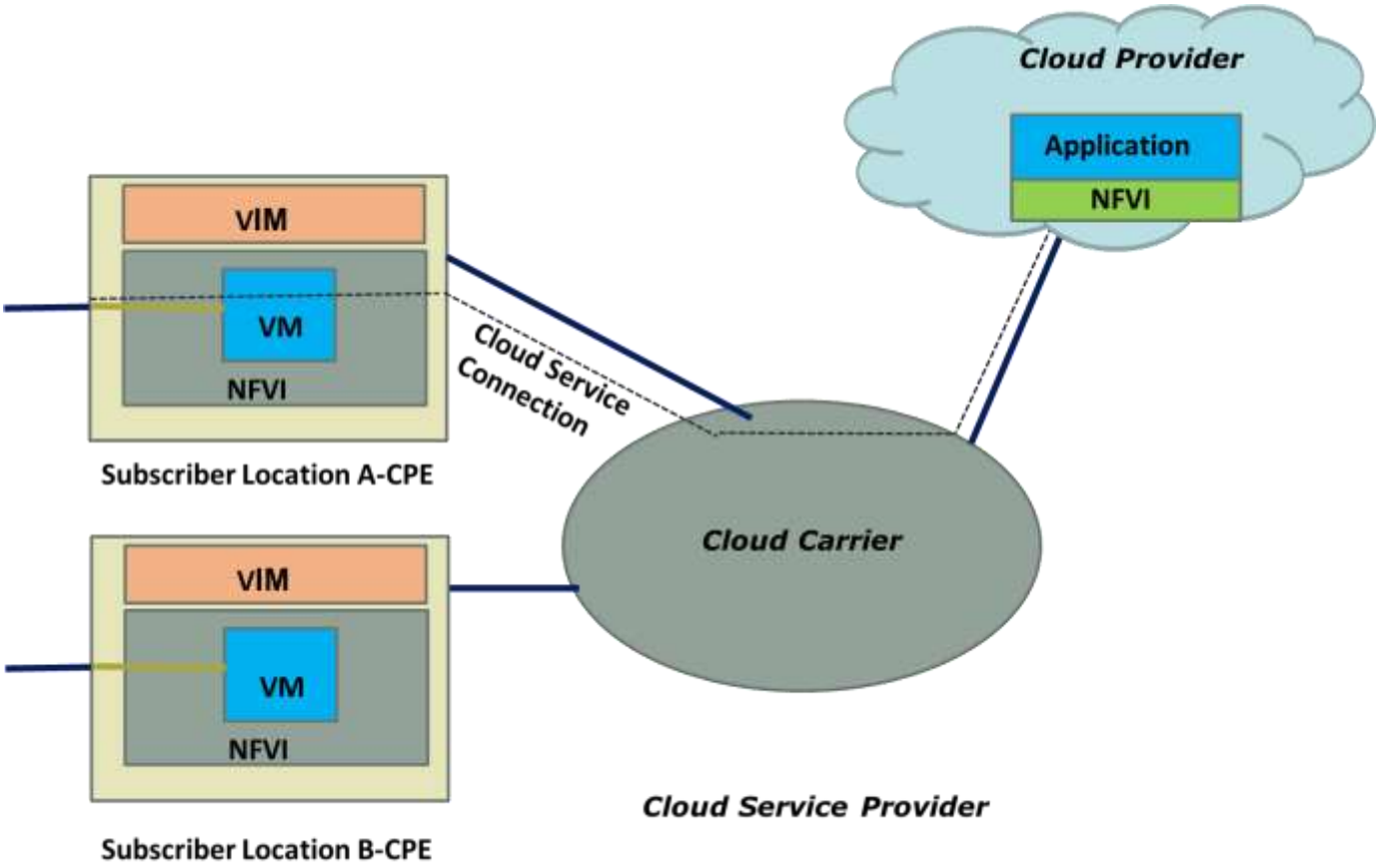


Figure 11- An example PaaS architecture

PaaS can be provided via a DC as well as by a Cloud-in-a-Box[3]. **Figure 12** depicts a virtual platform in a CPE provided by a cSP. A VNF owned and maintained by a subscriber can run over this platform to perform intended service function such as security. The VNF on CPE may service chain with another VNF provided by a Cloud Provider to support additional capabilities.

Cloud Carrier and Cloud Provider could be two different entities requiring a standards interface between them.

[3] Cloud in-a-box is an edge computing infrastructure that supports a suite of applications customized to the specific company or industry vertical [9].



VIM: Virtual Infrastructure Manager [10] VM: Virtual Machine [8]

Figure 12- Cloud-in-Box providing a virtualized platform for consumer managed applications

10.5 SaaS

The capability provided to the consumer via SaaS [1] is to use the Cloud Provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Software is installed on demand and licensed. Open-source and enterprise operating system software options from various vendors could be available.

Figure 13 depicts a cloud service user accessing an application VNF (i.e. SaaS).

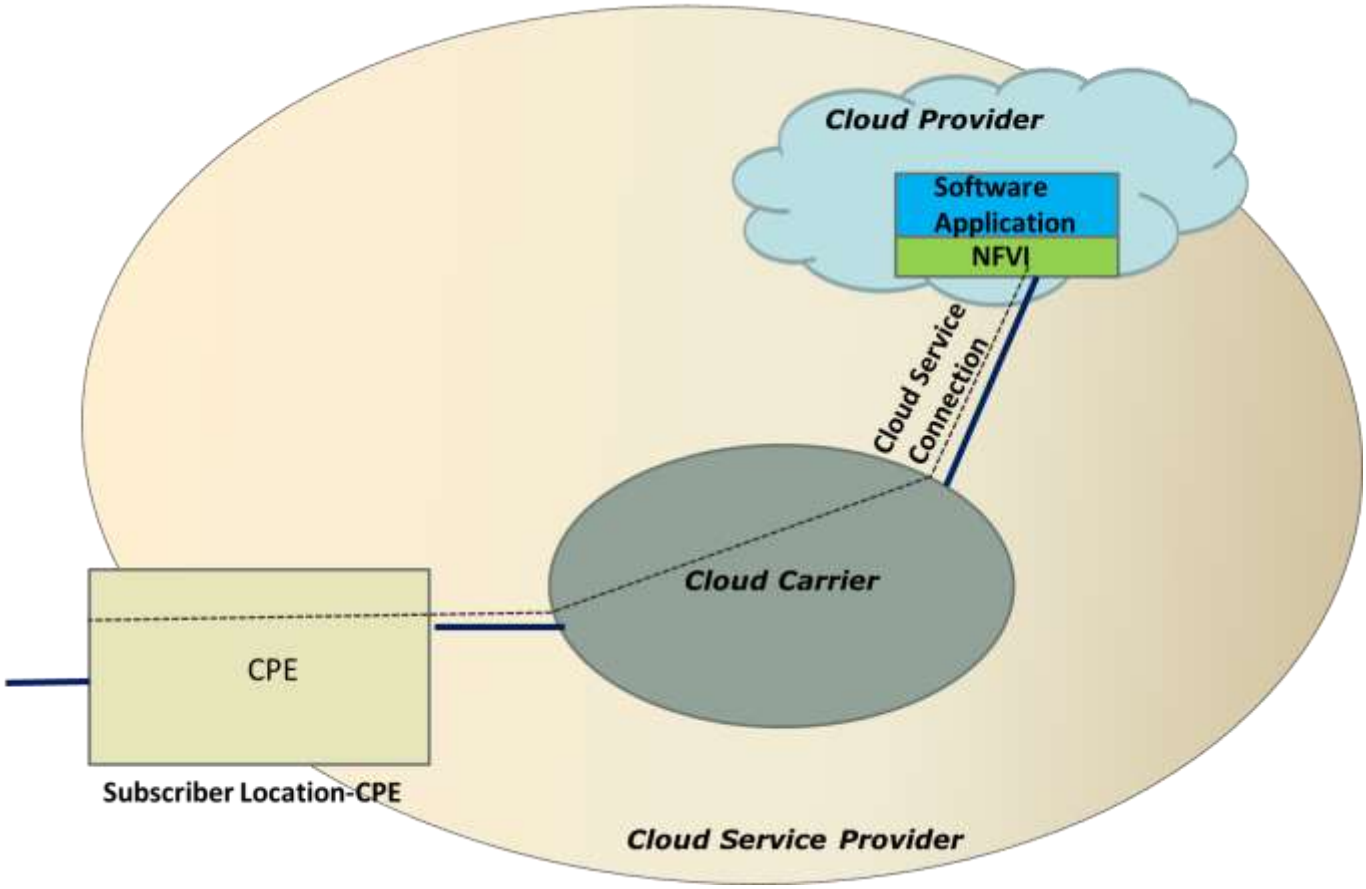


Figure 13- SaaS provided by cSP

10.6 CaaS

Real-time services such as Virtual PBX, voice and video conferencing systems, collaboration systems and call centers can be considered as forming Communication as a Service (CaaS). Some of the services in CaaS category are:

- Local and domestic long distance point-to-point or multipoint Voice Calling
- Fixed Mobile Convergence which removes the distinctions between fixed and mobile networks, providing seamless services using a combination of fixed broadband and local access wireless technologies
- Voicemail in user inbox or on user smartphone
- Integrated business communications making calls from user desk or mobile phone and have it appear as user office number
- Point-to-point or multipoint Video Calling
- Point-to-point or multipoint voice and video conferencing
- Professional voice recording service for user greetings and other messages

11 Architectural Components of Cloud Services

From sections 9 and 10, we can conclude the following architectural components of cloud services:

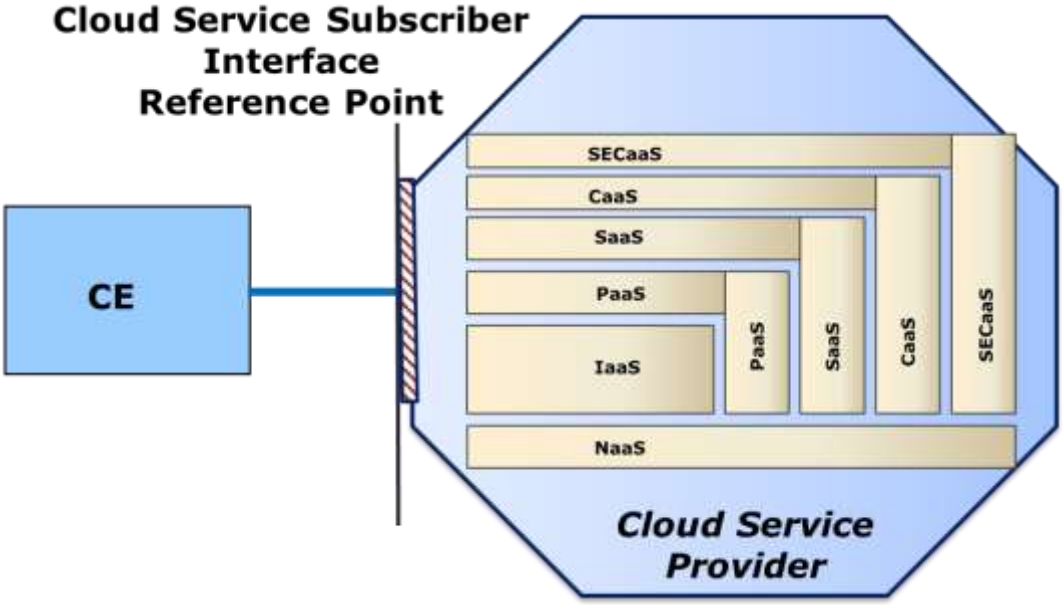
- Cloud Service Interface between Cloud Subscriber and Cloud Service Provider, Cloud UNI, which is a standards interface for subscribers to connect and operate over cloud platforms; and connect and run applications provided by a cSP.
- Interface between Cloud Subscriber and Application or Cloud Platform, Cloud Application Interface or Cloud Interface (cI)
- Interface between Cloud Applications, Cloud Interface (cI)
- Interface between Cloud Carriers, Cloud ENNI
- Interface between Cloud Carrier and Cloud Provider, Cloud ENNI
- Interface between Cloud Providers, Cloud ENNI
- Connection between a Cloud Subscriber and Application, cSC
- Connection between/among Cloud Subscribers, cSC
- Connection between/among Cloud Applications, cSC
- Segment of cSC in a Cloud Service Operator, cSO-c

11.1 Interfaces

11.1.1 Cloud Service Subscriber Interface

A Cloud Subscriber interfaces to a Cloud Service Provider (cSP)'s facilities via a Cloud Service Subscriber Interface consisting of Cloud Connectivity UNI and Cloud Application UNI, as depicted in **Figure 14** and **Figure 15** which are implemented over a bi-directional link that provides the various data, control and management capabilities required by the cSP to clearly demarcate the two different connectivity domains and two different application domains involved in the operational, administrative, maintenance and provisioning aspects of the service. The Cloud Application UNI may not exist at the Cloud Service Subscriber Interface when only connectivity services are offered at this interface.

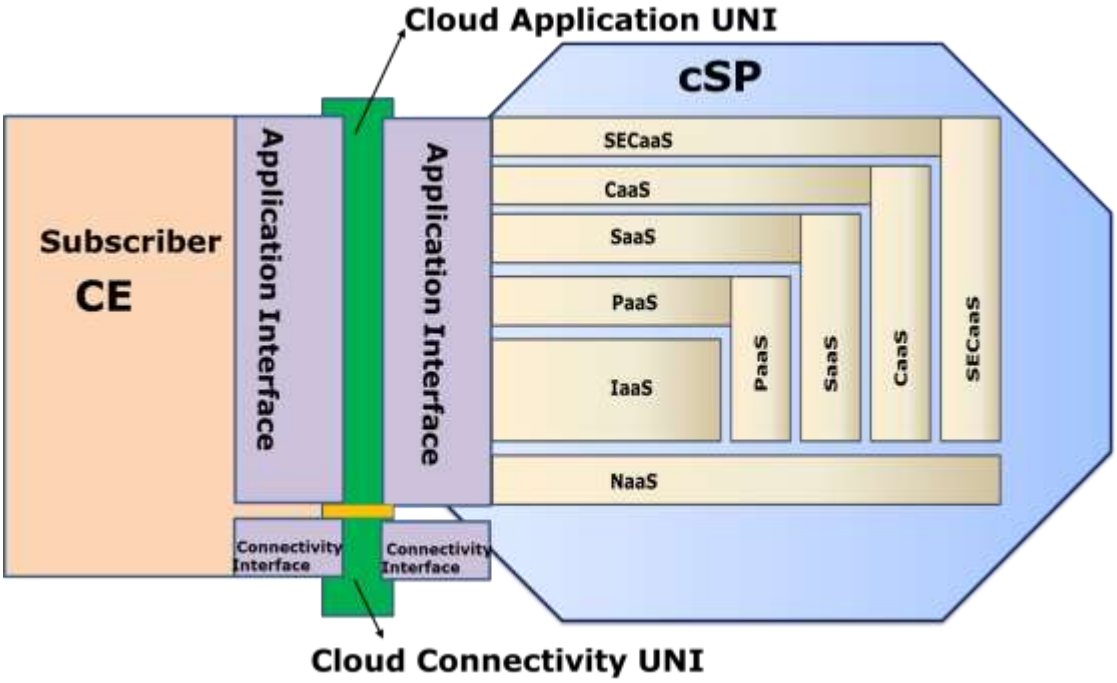
The Cloud Service Subscriber Interface Reference point is the demarcation point between the domains under the responsibility of the cSP and the domains under the responsibility of the Cloud Service Subscriber. It is dedicated to a single Cloud Service Subscriber such as an enterprise. Multiple flows can be multiplexed over this interface using logical connections.



505
506

507 **Figure 14-** Cloud Service Subscriber Interface functionalities are distributed between Customer
508 Edge (CE) and cSP.

509



510

511 **Figure 15-** Cloud Connectivity UNI and Cloud Application UNI between Customer Edge (CE)
512 and cSP.

513

514

The subscriber in **Figure 14** and **Figure 15** can be an enterprise with multiple users sharing the same Cloud Service Subscriber Interface where CE may represent a gateway device. It could be a physical equipment with an Internet browser, a VNF/VM/Container, or a collection of VNFs/VMs/Containers with a virtual switch. Individual functional elements in a CE may be either entirely in the user domain, or may be entirely in the cSP domain and managed by the cSP, or in both sides.

From this interface, the subscriber establishes a connection, Cloud Service Connection (cSC), with a Cloud Service Provider (cSP) providing a physical or virtual resources such as physical storage, virtual storage, a virtual machine (VM), Container, and application (i.e. VNF).

The CE and cSP exchange service packets across the Cloud Service Subscriber 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). We will call all of them as PDU in the rest of this specification.

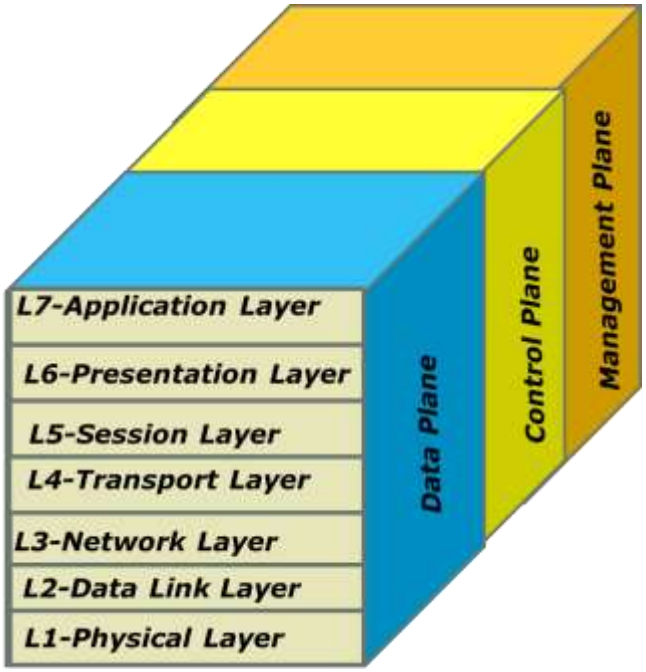
The PDU transmitted across the Cloud Service Subscriber Interface toward the Cloud Service Provider is called an ingress service PDU. The PDU transmitted across the Cloud Subscriber Interface toward the Cloud Service Subscriber is called an egress service PDU.

Cloud Service Subscriber Interface protocol stack is depicted in

Figure 16 that may combine protocol stacks for Cloud Connectivity UNI and Cloud Application UNI as illustrated in **Figure 17** and **Figure 18** , respectively.

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, an L3 interface for IP services, and L7 interface for multimedia applications.

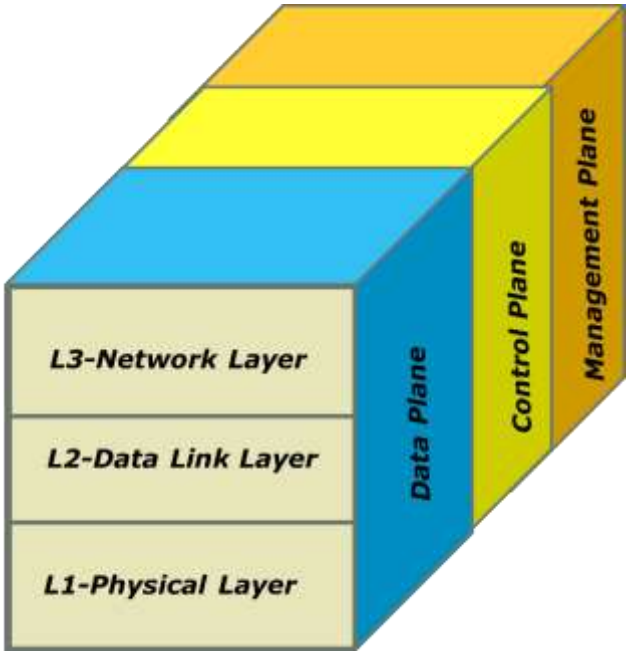
Depending on the service offering, the protocol stack for Cloud Application UNI can be L2 and above. For example, Cloud Application UNI is a L7 interface for multimedia applications.



548
549
550

551 **Figure 16** – Cloud Service Subscriber Interface Protocol Stack

552



553

554 **Figure 17** – Cloud Connectivity UNI Protocol Stack

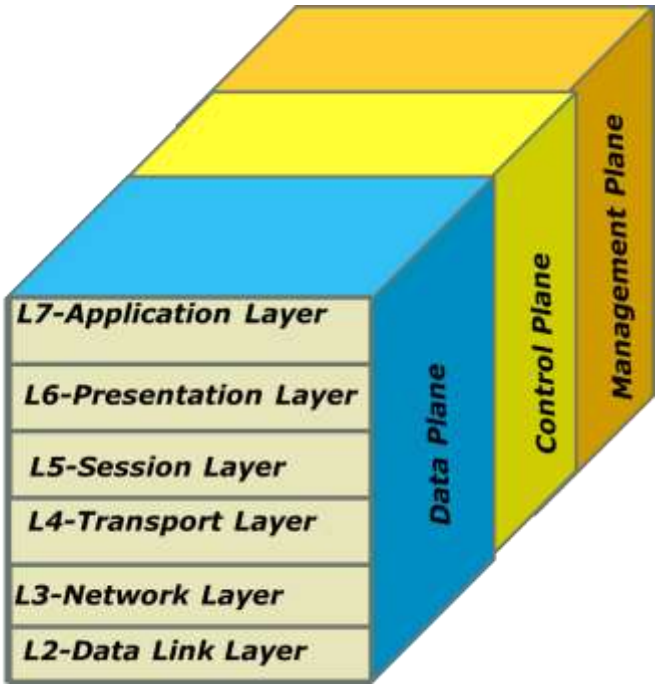


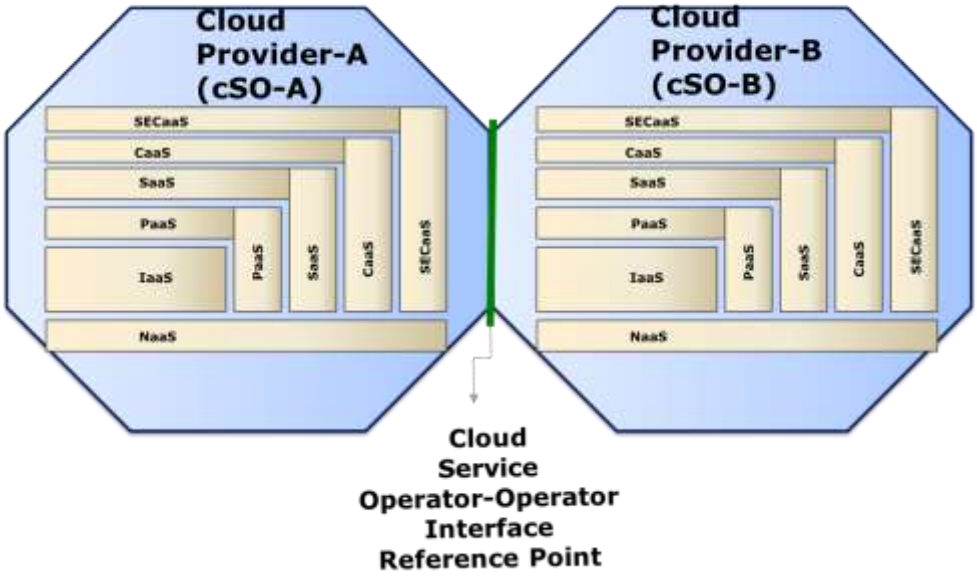
Figure 18 – Cloud Application UNI Protocol Stack

11.1.2 Cloud Service Operator- Operator Interface

As we discussed in Section 7, applications and connectivity to applications can be provided by a single cloud service operator (cSO) as well as multiple cSOs, in providing a cloud service to a cloud subscriber. A cSO represents a Cloud Carrier or a Cloud Provider. The Cloud Provider can be a public or private Cloud Provider.

Two cSOs interface to each other via a Cloud Service Operator-Operator Interface as depicted in **Figure 19**. Cloud Service Operator-Operator interface is defined as a reference point representing the boundary between two cSOs that are operated as separate administrative domains. This reference point provides demarcation between two cSOs for cloud services.

Cloud Service Operator-Operator Interface consisting of Cloud Connectivity ENNI and Cloud Application ENNI as illustrated in **Figure 21Figure 20**. The Cloud Application ENNI may not exist at the Cloud Service Operator-Operator Interface when only connectivity services are offered at this interface.

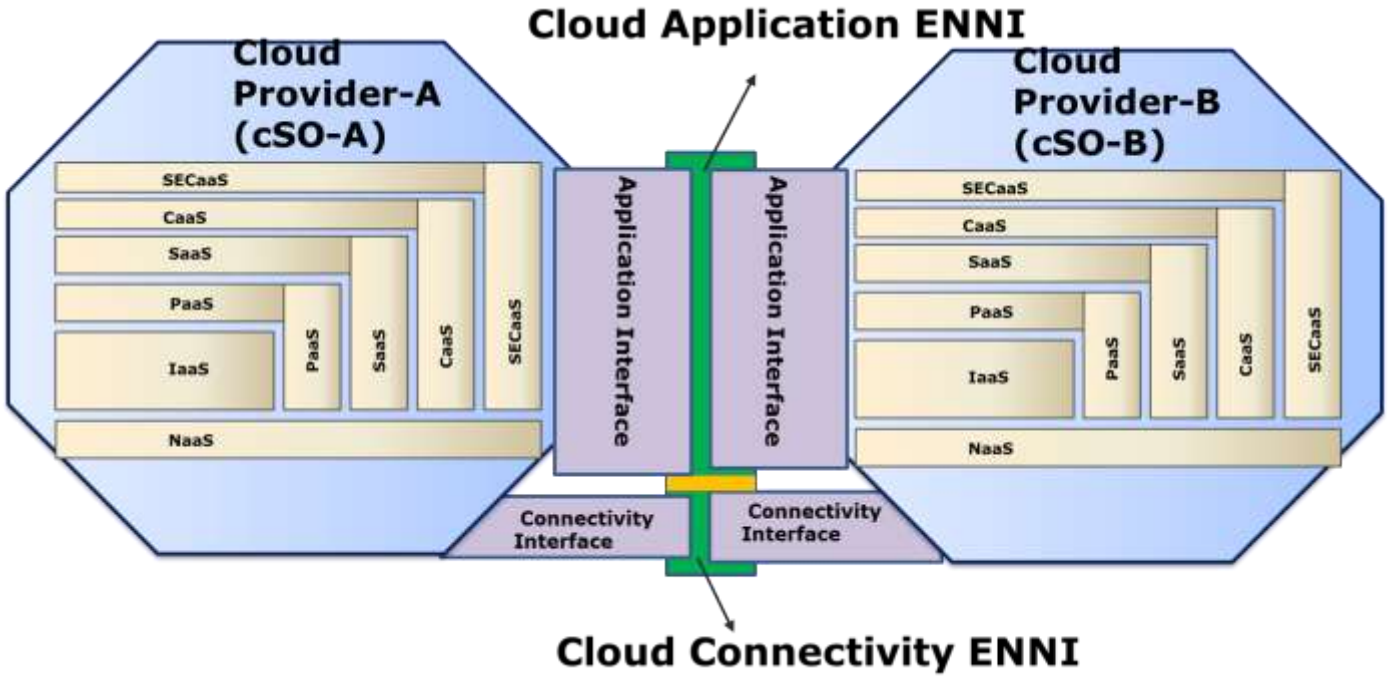


574

575

576 **Figure 19** – Two cSOs interfacing each other via Cloud ENNI

577



578

579 **Figure 20** – Cloud Connectivity ENNI and Cloud Application ENNI between two cSOs.

580

The protocol stacks for Cloud Connectivity ENNI and Cloud Application ENNI are described in **Figure 21** –Cloud Connectivity ENNI Protocol Stack between two cSOs.**Figure 21** and **Figure 22**.

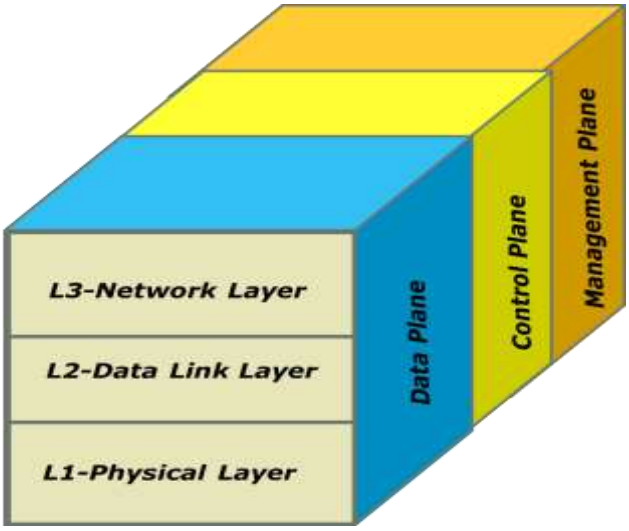


Figure 21 –Cloud Connectivity ENNI Protocol Stack between two cSOs.

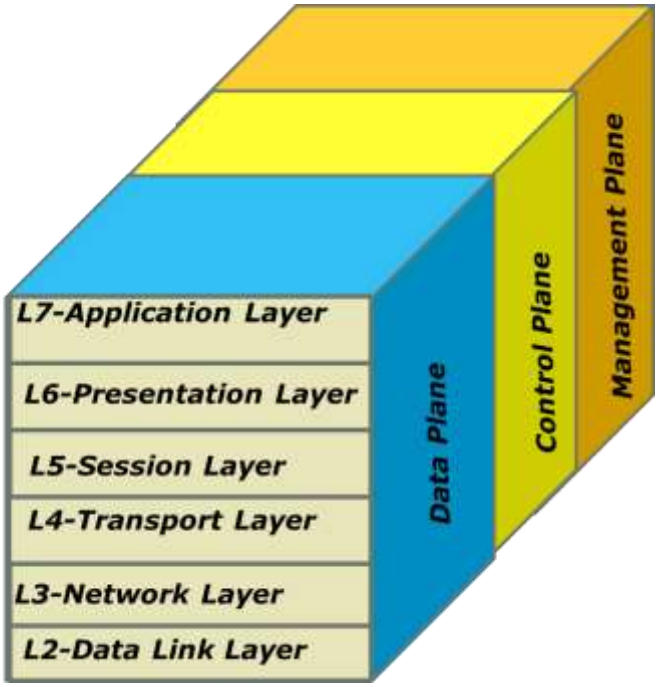


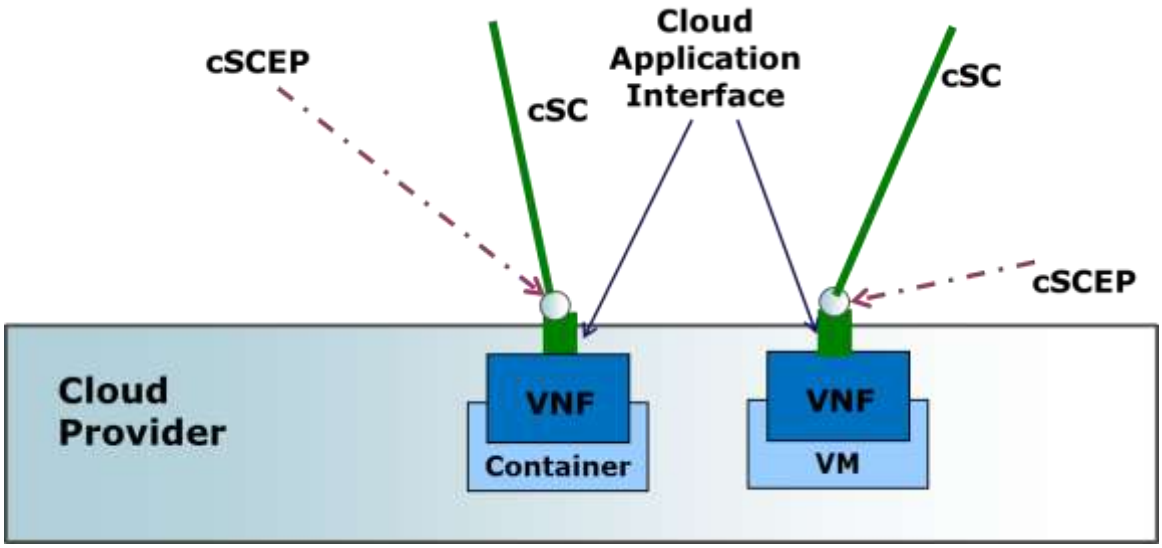
Figure 22 –Cloud Application ENNI Protocol Stack.

Cloud Connectivity ENNI is expected to be very similar to ENNI [13] if the interface is an L2 Ethernet interface.

cSOs may use a gateway to interface to external entities as described in Appendix-A.

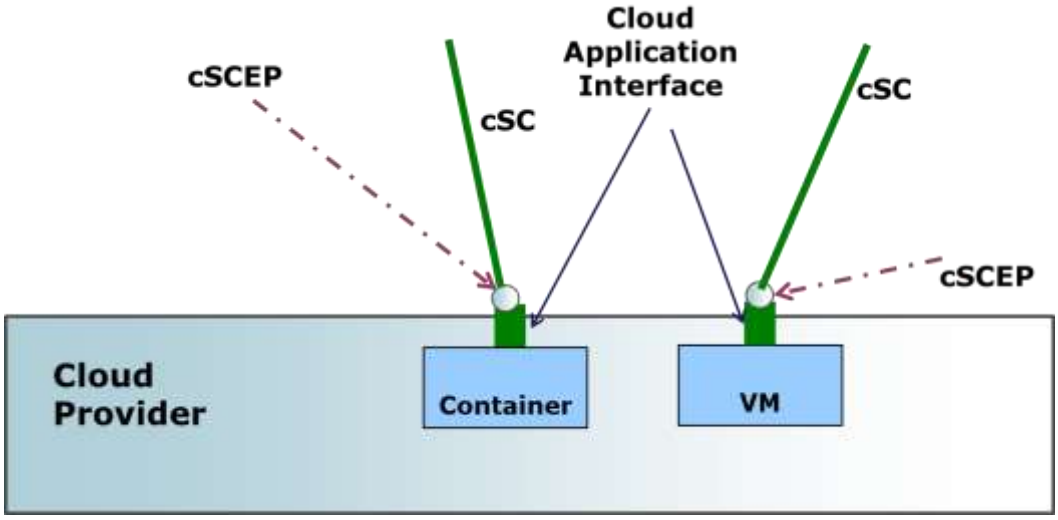
11.1.3 Cloud Application Interface

The Cloud Application Interface is the interface of a Cloud Service Application or Cloud Service Platform supported by a Cloud Provider (cP) or a Cloud Service Provider (cSP). Therefore, it can be an interface of a VNF, VM or Container, as depicted in **Figure 23**, **Figure 24**, **Figure 25**, **Figure 26**, and **Figure 27**.



cSCEP: Cloud Service Connection End Point
cSC: Cloud Service Connection

Figure 23- Application Interface for VNF



615

616 cSCEP: Cloud Service Connection End Point
617 cSC: Cloud Service Connection

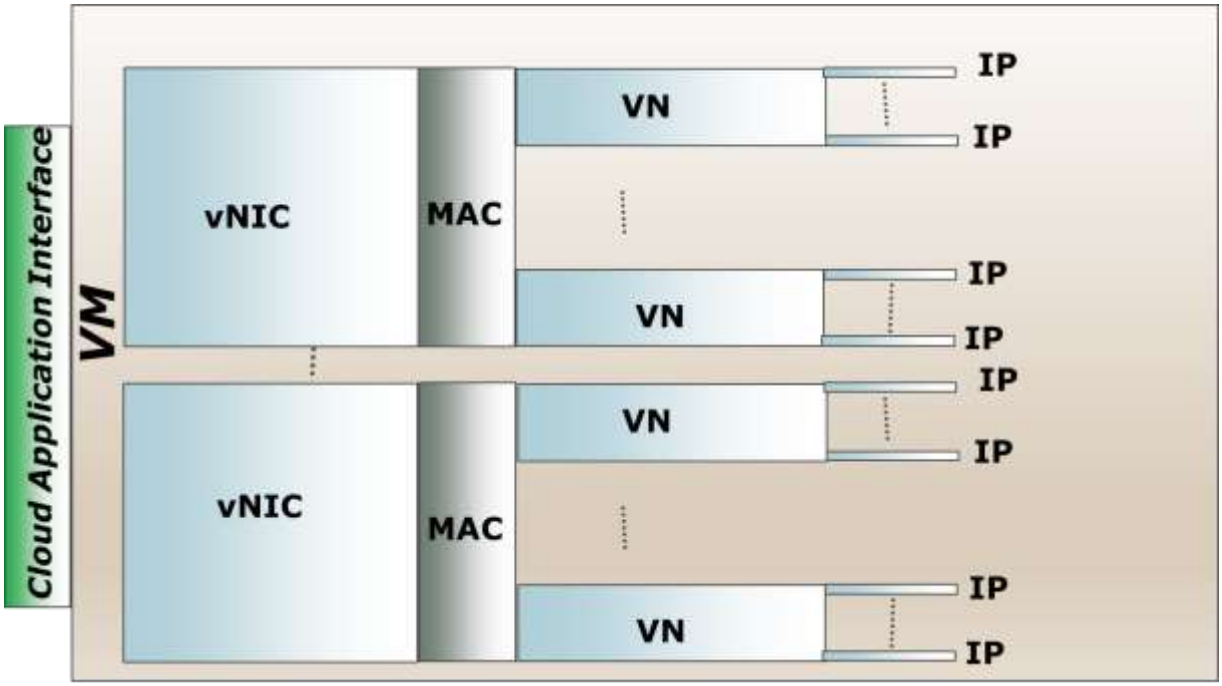
618

619 **Figure 24:** Application Interface for VM or Container

620

621

622

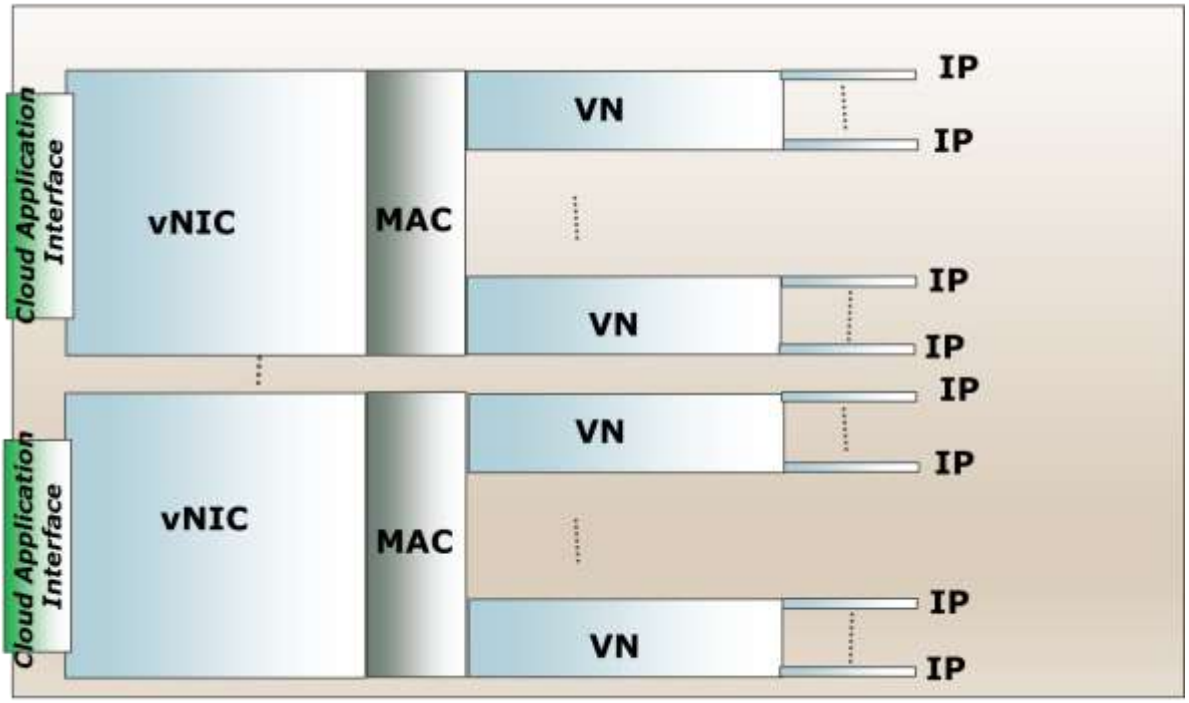


623

624

625 **Figure 25-** Application Interface for VM

626



627

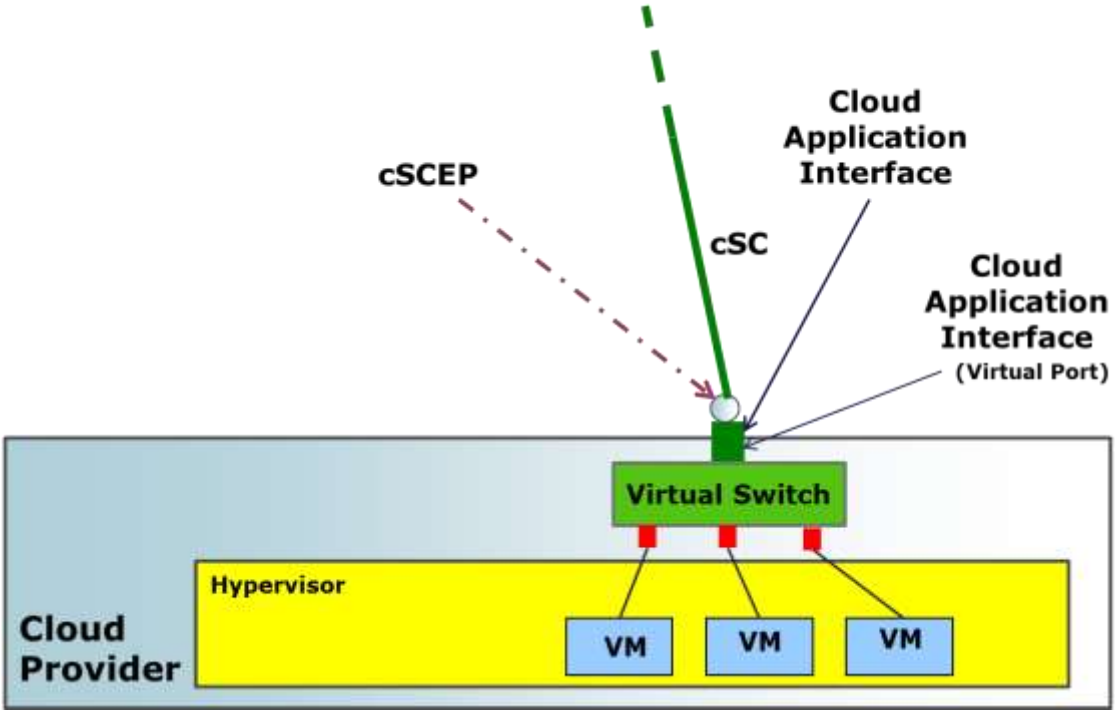
628 vNIC: Virtual Network Interface Controller

629 VN: Virtual Network

630 **Figure 26-** Application Interface for vNIC

631

632



cSC: Cloud Service Connection

Figure 27- Application Interface for Virtual Switch Port

Cloud Application Interface could be Cloud Application UNI or Cloud Application ENNI, with its protocol stack, as illustrated in **Figure 15**, **Figure 18**, **Figure 20** and **Figure 22**.

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

An example for protocol stack and examples of subscriber configuration parameters for cI are given in the Appendix-B.

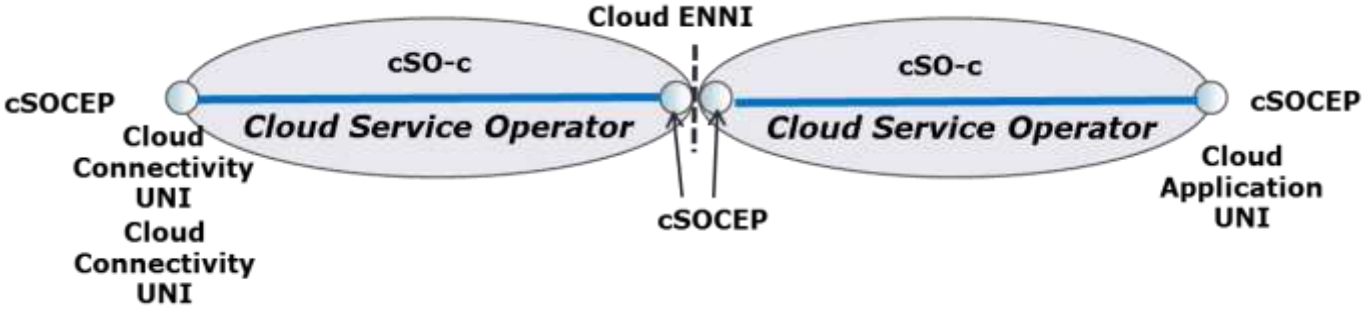
11.2 Connection and Connection End Points

Connection and connection end points providing cloud services are depicted in **Figure 28** for a Cloud Service Connection (cSC) crossing one or more administrative domains.

When a cSC crosses multiple cSOs, the cSC segments and their end points in each cSO are called cSO-c (Cloud Service Operator Connection) and Cloud Service Operator Connection End Point (cSOCEP), respectively.

The following sections will describe them in details.

(a) cSC between two end points residing on the resources of a cSP.



(b)cSC between two end points residing on the resources of two different cSOs

Figure 28- Cloud Service Connection and Segments

11.2.1 Cloud Service Connection End Point (cSCEP)

The cSCEP is an end point of a cSC when the cSC is within the boundaries of one administrative domain. Cloud Subscribe Interface identifier, availability, bandwidth profile, parameters of security functionalities, administrative state and operational state are among the attributes of cSCEP.

For implementations using Ethernet Virtual Connection (EVC), attributes of "EVC Per UNI" in [5], L2CP in [11] and L2 SOAM [12] are a subset of the attributes of cSCEP.

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

11.2.2 Cloud Service Connection (cSC)

The cSC is a cross connect between two or more cSCEPs. The cSC could be an EVC, LSP, IP VPN or SD-WAN connection. Identifiers of cSCEPs associated with this cSC, connection type, SLS, redundancy, connection start time, connection duration, connection period, billing options, MTU, administrative and operational states are among the attributes of cSC.

For implementations using Ethernet Virtual Connection (EVC), EVC service attributes in [5], and EVC performance attributes and parameters in [5] are a subset of attributes of cSC.

A cSC can support connecting multiple VMs via multiple sessions as depicted in **Figure 27** where a virtual switch routes traffic to destination VM.

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

11.2.3 Cloud Service Operator Connection (cSO-c)

The cSC may cross multiple Cloud Service Operator domains as depicted in **Figure 29**. Each domain will carry a segment of the cSC. The segment in each cSO domains is called Cloud Service Operator Connection (cSO-c).

cSO_c is another cSC. We call them differently to identify the connection whether it is a segment or an end-to-end connection.

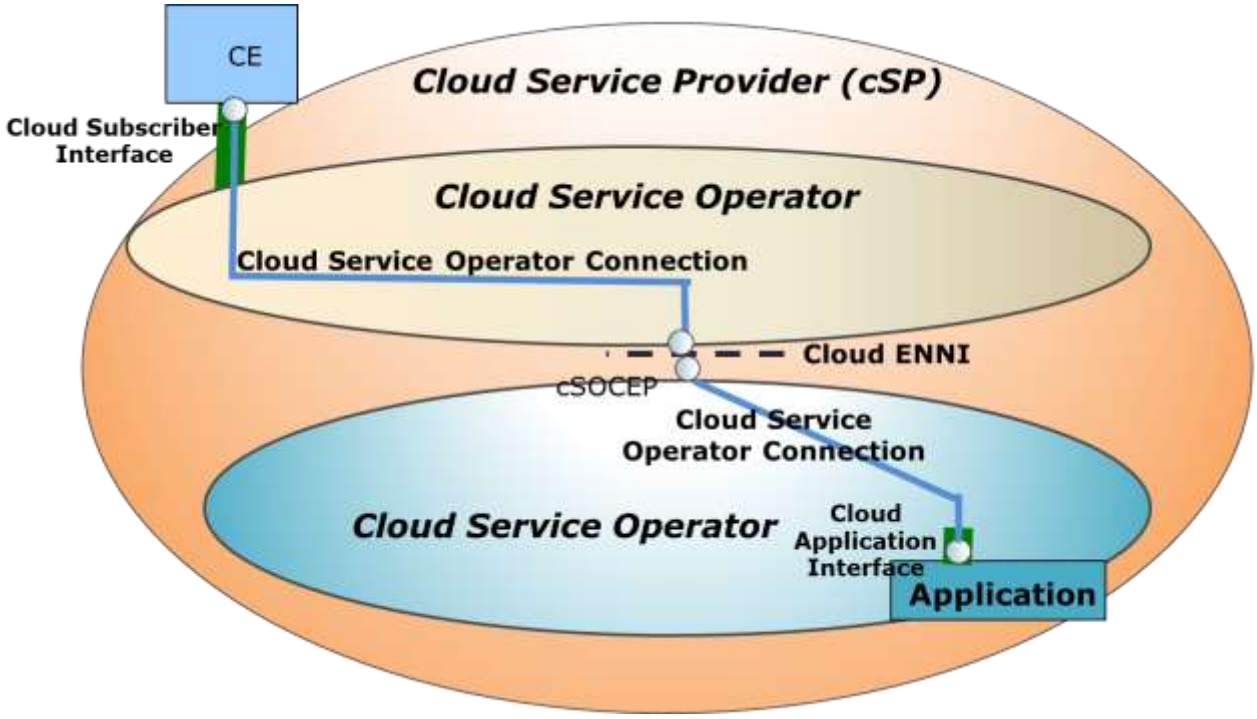


Figure 29- Segments of cSC crossing multiple cSOs.

The cSO-c is a cross connect between two cSOCEPs. The cSO-c could be very similar to san Operator Virtual Connection (OVC), LSP, IP VPN connection segment, or SD-WAN connection.

Identifiers of cSOCEPs associated with this cSO-c, connection type, SLS, redundancy, connection start time, connection duration, connection period, billing options, MTU, administrative and operational states are among the attributes of cSO-c.

For implementations using OVC, OVC service attributes including CoS preservation in [13] are a subset of attributes of cSO-c.

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

11.2.4 Cloud Service Operator Connection End Point (cSOCEP)

The cSOCEP is an end point of a cSO-c when the cSO-c is within the boundaries of one administrative domain. For high availability, cSOCEP can be redundant where primary and secondary units could be located at different devices. Cloud Service Operator-Operator Interface identifier, Cloud Subscriber Interface identifier, band-width profile, parameters of security functionalities, administrative state and operational state are among the attributes of cSOCEP.

cSOCEP at Cloud Subscriber Interface or Cloud Application UNI is equivalent to the cSCEP at Cloud Subscriber Interface or Cloud Application UNI.

For implementations using OVC, attributes of “OVC per ENNI”, “OVC Per UNI” in [5], L2CP in [11] and L2 SOAM [12] are a subset of the attributes of cSOCEP.

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

12 References

[1] National Institute of Standards and Technologies (NIST) Special Publication 500-291, 2106 NIST Cloud Computing Roadmap, July 2013.

[2] OCC 1.0 Reference Architecture, December 2014.

[3] MEF 47 Services for Cloud Implementation Agreement, October 2014

[4] ETSI GS NFV 002 v1.2.1 (2014-12) "Network Functions Virtualisation (NFV): Architectural Framework"

[5] MEF 6.2, EVC Ethernet Services Definitions Phase 3, August 2014

[6] MEF 61.1 draft 0.11, IP Service Attributes, May 2018

[7] MEF SD-WAN Service Attributes and Service Definitions, April 2018.

[8] ETSI GS NFV-INF 001 v.1.1.1 (2015-01) "Network Functions Virtualisation (NFV): Infrastructure Overview"

[9] Cloud Edge Computing: Beyond the Data Center, https://www.openstack.org/edge-computing/

[10] ETSI GS NFV-MAN 001 v.1.1.1 (2014-12) "Network Functions Virtualisation (NFV): Management and Orchestration"

[11] MEF 45 Multi-CEN L2CP, August, 2014.

[12] MEF 30.1 Service OAM Fault Management Implementation Agreement Phase 2, April 2013.

[13] MEF 26.1 External Network Network Interface (ENNI)–Phase 2, January 2012.

[14] Network Working Group S. Bradner

[15] RFC 2119 BCP: 14 "Key words for use in RFCs to Indicate Requirement Levels", March 1997

[16] RFC8174 "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", May 2017.

Appendix A Cloud Service Gateway (Informative)

The cSOs may employ a gateway, Cloud Service Gateway (cSGW), to connect to each other asdepicted in

Figure 30. The cSGW might provide connection multiplexing among other features that are required by cSOcSOI such as Cloud ENNI link redundancy.

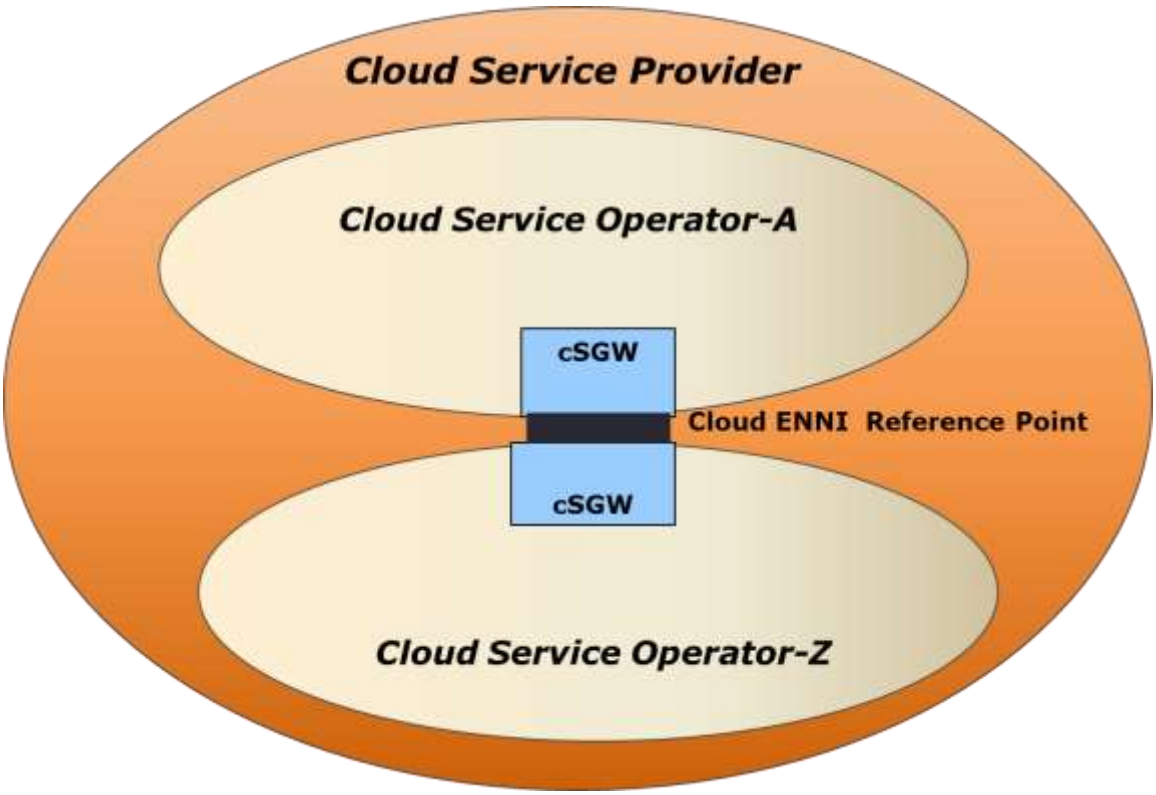
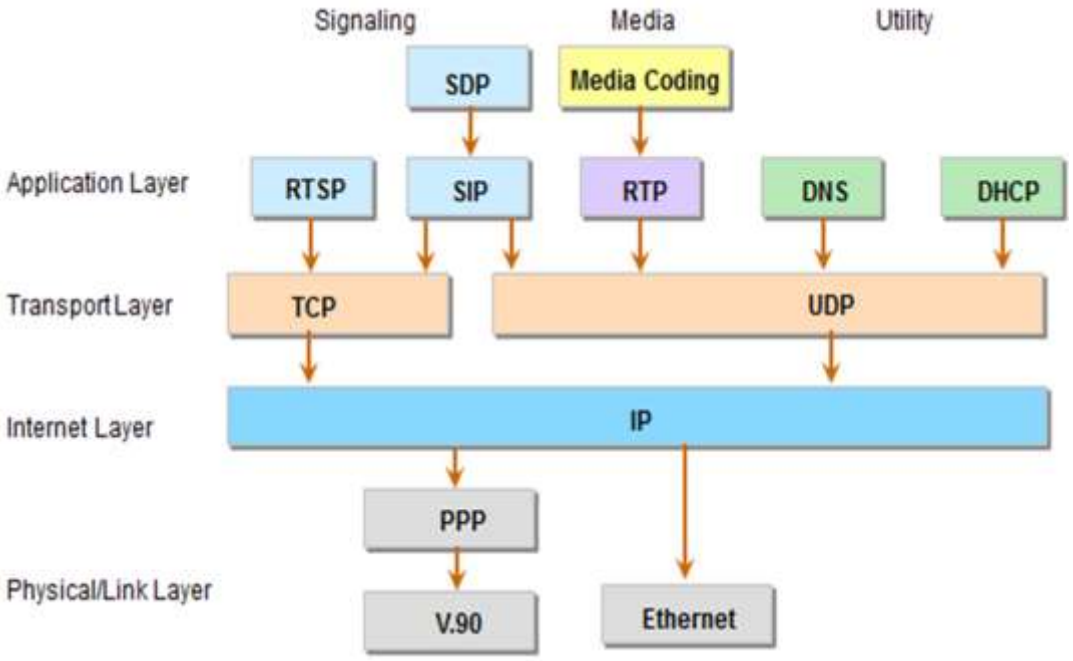


Figure 30 – Two cSOs interface each other via Cloud ENNI

Appendix B cI Examples (Informative)

As an example for the cI protocol stack, the protocol stacks for a session border controller to support voice and multimedia application are depicted in **Figure 31**. Virtual session border controller VNF supports the protocol stack above the physical layer.



RTP: Real-time Transport Protocol

RTSP: Real Time Streaming Protocol

PPP: Point-to-Point Protocol

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name Servers

SDP: Session Description Protocol

SIP: Session initiation protocol

Figure 31 – SIP Protocol Stack for Session Border Controllers

VNF and VM interfaces are more common Cloud Interfaces. As indicated in Section 7, VNF and/or VM can be configured and managed by an SP as well as self-configured by a subscriber.

B.1 Virtual Machine (VM) Attributes

After a subscriber connects to the virtual platform provided by an SP, some of the attributes that a subscriber configures for cI are:

- Number of Virtual CPUs
- Size of Virtual RAM
- Size and Locations of Virtual Disks
- Virtual NIC (s) and associated MAC addresses and IP addresses
- Guest Operating System
- Inbound Traffic Port
- Outbound Traffic Port
- Redundancy with Affinity or Anti-Affinity
- Single Root I/O Virtualization (SR-IOV) Support

B.2 Virtual Network Function (VNF) Attributes

Applications such as virtual phone, virtual router and virtual firewall are provided by VNFs. Clearly each VNF has its own unique attributes. Below are some of the attributes of a vR to be configured either by the cSP as part of Day-0 and Day-1 configurations, and by the subscriber as part of Day-2 configurations[4].

- License Type
- Fragmentation and Reassembly
- Single tenant
  - VLAN ID
  - Tenant VRF
- Multiple tenants
  - VDC (Virtual Data Center)
  - VLAN IDs
  - Tenant VRFs
- Routing protocol and option configurations
  - Static Routing
  - BGP
  - EIGRP
  - Intermediate system-to-intermediate system (IS-IS)
  - Open shortest path first (OSPF)
- Loopback Address

[4] There is no consensus about the definitions of Day-0,1 and 2 for a VNF. We use the followings in this document: a) Day 0: VNF image is uploaded and on-boarded. b) Day 1: VNF interfaces and network connectivity have been configured. It is ready to carry traffic c) Day 2: Customer configurations can be performed. Billing and performance reports are available.

- NTP Server IP
- Routing table groups
- IP Multicast
  - Internet Group Management Protocol (IGMP)
  - Protocol Independent Multicast (PIM)
- Per-packet load balancing
  - Equal-cost multi-path routing (ECMP)
- Autonomous system numbers (ASNs)
- Autonomous system confederation ID and members
- Fault Management Protocols
  - Internet Control Message Protocol (ICMP)
  - Bidirectional Forwarding Detection (BFD)
- DHCP Relay
- MAC addresses, IPv4/6 addresses
- Encapsulation
  - GRE

• VPN

- Dynamic multipoint virtual private network (DMVPN)
- FlexVPN
- Secure Sockets Layer (SSL) VPN

- MPLS

• SNMP

- Secure Shell (SSH)
- Network address translation (NAT)
- Remote Authentication Dial-In User Service (RADIUS)

As Cloud Services are defined by MEF, attributes of each interface including cI, connection and connection end points are expected to be defined in details as part of these service definitions.