Technical Specification

OCC 1.0

OCC Reference Architecture

December, 2014

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Disclaimer

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and the Open Cloud Connect (OCC) is not responsible for any errors. The OCC does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by the OCC concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by the OCC as a result of reliance upon such information.

The information contained herein is intended to be used without modification by the recipient or user of this document. The OCC is not responsible or liable for any modifications to this document made by any other party.

The receipt or any use of this document or its contents does not in any way create, by implication or otherwise:

a) any express or implied license or right to or under any patent, copyright, trademark or trade secret rights held or claimed by any OCC member company which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

b) any warranty or representation that any OCC member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

c) any form of relationship between any OCC member companies and the recipient or user of this document.

Implementation or use of specific Cloud Ethernet standards or recommendations and OCC specifications will be voluntary, and no company shall be obliged to implement them by virtue of participation in the Cloud Ethernet Forum. The OCC is a non-profit international organization accelerating industry cooperation on Cloud Ethernet technology. The OCC does not, expressly or otherwise, endorse or promote any specific products or services.

© The Cloud Ethernet Forum 2014. All Rights Reserved.

Table of Contents

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

List of Figures

List of Tables

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

List of Contributing Members

Author and Editor: Mehmet Toy, Ph.D., Comcast

Contributing OCC member companies agreed to be listed:

Avaya
Alcatel-Lucent
BTI Systems
Hewlett-Packard
Iometrix
Verizon
Veryx
Wedge Networks

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

1.Introduction

In recent years, types of user devices and applications for cloud services have grown rapidly with little standardization. The users prefer services that are on-demand, scalable, survivable and secure with usage-based billing. In order to meet these demands, service providers need to be able to quickly create the services and utilize their resources effectively [1]. Cloud Services are aimed to support these objectives.

In addition to Cloud initiatives, network function virtualization (NFV) by ETSI [40], overlay networks by Network Virtualization Overlays (nvo3) of IETF [38], and auto-provisioning of resources and separation of data and control planes via Software-Defined Networking (SDN) by Open Networking Foundation (ONF) [41] are also aimed to improve efficiency in resource utilization and network operations. Cloud Services consist of physical and virtual resources which may employ virtualization, overlay and SDN techniques defined by ETSI, IETF and ONF.

The US National Institute of Standards and Technology (NIST) [2] defined a generic high level conceptual model for the development of cloud computing architectures and a companion taxonomy. The OCC's charter is to define standards and terms for Cloud Services including those based on Carrier Ethernet. This document describes Cloud Services, actors, architectures, and standard interfaces for Cloud Services.

To better describe the interfaces, connections, connection termination points and services provided in this document, examples of possible attributes and features are used. These attributes and features are only examples and not requirements at this time, although many of the items could become requirements in future documents. The reader must pay attention to where items are described as possible attributes and features and not infer possible items as hard requirements.

2.Terminology and Acronyms

This section defines the terms used in this document. In many cases, the normative definitions to terms are found in other documents. The third column in Table 1 is used to provide the reference for the definitions.

Terms	Definitions	Reference
AIS	Alarm Indication Signal	
BWP	Bandwidth Profile	MEF 10.3[17]
CaaS	Communication as a Service - A category of cloud services where the capability provided to the cloud service user is to use real-time communication and collaboration services.	ITU-T Y.3500 [81] and FG Cloud TR, v1.0 [3]
cCcPI	Cloud Carrier Cloud Provider Interface	This document

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

CDN	Content Delivery Network	
C-VLAN	Customer VLAN	IEEE 802.1Q [30]
Carrier Ethernet Network (CEN)	A network from a Service Provider or network Operator supporting the MEF (Metro Ethernet Forum) service and architecture models.	MEF12.2[56]
CE	Customer Edge which is a user device supporting cSUI. It can be an equipment provided by a cSP or an equipment selected by the user, that may contain Virtual Machines (VMs).	This document
Cloud Consumer	A person or organization that maintains a business relationship with and/or uses service from a Cloud Service Provider via a Cloud Service User Interface (cSUI).	This document
Cloud Service User	A person or organization that maintains a business relationship with and/or uses service from a Cloud Service Provider via a Cloud Service User Interface (cSUI).	This document
Cloud Carrier	An intermediary that provides connectivity and transport between Cloud Providers and Cloud Consumers or between Cloud Providers.	This document
Connection Start Time	Connection Start Time indicates the time at which a requested connection is established.	This document
Connection Start Interval	Connection Start Interval indicates the acceptable interval after the Start Time during which the connection request can be made.	This document and [66]
Connection Duration	Connection Duration indicates the time interval for which the requested connection remains in effect before automatically torn down.	This document
Connection Period	Connection Period indicates the time interval at which the connection request is to repeat.	This document and [66]
CoS	Class of Service	MEF 10.3 [17]
CoS ID	Class of Service Identifier	MEF 23.1 [47]
Cloud Provider (cP)	An entity that is responsible for making cloud applications available to Cloud Consumers (Cloud Service Users).	NIST Special Publication 500-291 [2]

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

cSC (Cloud Service Connection)	A connection between two users or between a user and a virtual machine (VM) or between two machines or VMs provided by a Cloud Service Provider and its associated entities.	This document
cSC-c (Cloud Carrier Connection)	The segment of cSC within the boundaries of a Cloud Carrier.	This document
cSC-p (Cloud Provider Connection)	The segment of cSC within the boundaries of a Cloud Provider.	This document
cSC-cp	The segment of cSC within the boundaries of a Cloud Service Provider where cSC crosses multiple Cloud Service Providers	This document
cSGW	Cloud Service Gateway	This document
cSI	Cloud Service Interface (cSI) is the interface of a Cloud Service application supporting entity of a Cloud Provider such as VM.	This document
cSO	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.	This document
cSP (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 Consumers. It is the single point of contact for the consumer.	This document
cSCTP (Cloud Service Connection Termination Point)	A logical entity that originates or terminates cSC at a logical user or machine interface.	This document
cSI	Demarcation Point between Cloud Service Providing entity such as a server or VM, and Cloud Service Provider.	This document
cSPcSPI	Cloud Service Provider Cloud Service Provider Interface	This document
cSPcSPI-P	cSPcSPI Provider (Functional Element)	This document
cSC-csp	Cloud Service Provider Connection	This document
cSC-csp-TP	Cloud Service Provider Connection Termination Point	This document
cSC-cp-TP	Cloud Carrier-Provider Connection Termination Point	This document

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

cSUI	Demarcation Point between a Cloud Consumer and Cloud Service Provider.	This document
cSUI-C	cSUI Client (Functional Element)	This document
cSUI-P	cSUI Provider (Functional Element)	This document
Data Center (DC)	A data center is an infrastructure equipped with servers, storage, network devices along with power and air conditioning systems designed for supporting cloud applications.	This document.
DDoS	Distributed Denial of Service	RFC4732[59]
DEI	Discard Eligibility Indicator	IEEE 802.1Q [30]
DLP	Data Loss Prevention	
DSCP	Differentiated Service Code Point	RFC 2474[60]
Durable Reduced Availability (DRA) Storage Buckets	Durable Reduced Availability storage bucket is a lower cost and lower availability storage bucket providing the same durability as Cloud Storage buckets.	This document and [63]
E-Access	Ethernet Access Service	MEF 33 [21]
ENNI	External Network Network Interface	MEF 4[57]
EI	External Interface	MEF 4 [57]
Dynamic Block Store (DBS)	Dynamic Block Store is the persistent block level storage volumes that are automatically replicated within its Availability Zone offering the consistent and low-latency performance.	This document and [64]
EVC	Ethernet Virtual Connection	MEF 10.3 [17]
FCS	Frame Check Sequence	IEEE 802.1Q [30]
Hypervisor	A software, firmware or hardware running on a server that enables creation of virtual machines and runs them.	This document
IaaS	Infrastructure as a Service is a category of cloud services where the capability provided by the cloud service provider to the cloud service user is to provision processing, storage, intra-cloud network connectivity services (e.g. VLAN, firewall, load balancer, and application acceleration), and other fundamental computing resources of the cloud infrastructure where the cloud service user is able to deploy and run arbitrary applications.	NIST Special Publication 500-291 [2] and ITU-T FG Cloud TR, v1.0 [3]
ICMP	Internet Control Message Protocol	

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

IPSec ESP	Internet Protocol Security Encapsulating Security Payload	
L2CP	Layer Two Control Protocol	MEF 10.3[17]
LAN	Local Area Network	IEEE 802 [4]
LLC	Logical Link Control	ISO/IEC 8802-2 [65]
LSP	Label-switched Path	
MAC	Media Access Control	IEEE 802 [4]
MCF	MAC Convergence Function	IEEE 802.1Q [30]
MEG	Maintenance Entity Group	ITU-T Y.1731[15]
MEG Id	An identifier for a MEG, unique over the domain that SOAM is to protect against the accidental concatenation of service instances which is quivalent to the IEEE term Maintenance Association Identifier (MAID).	ITU-T Y.1731[15]
MPLS	Multiprotocol Label Switching	
MTU	Maximum Transmission Unit	
NaaS	An entity or a group of entities that deliver (s) assured, dynamic cloud connectivity services via virtual, or virtual and physical service end points orchestrated over multiple operators' networks.	This document and [74]
NE	Network Element	
NID	Network Interface Device	
NVA (Network Virtualization Authority)	The entity that provides address mapping and other information to NVEs	RFC7365[38]
Network Virtualization Edge (NVE)	An NVE is the network entity that sits at the edge of an underlay network and implements L2 and/or L3 network virtualization functions	RFC7365 [38]
OVC	Operator Virtual Connection	MEF 26.1[22]
PaaS	A category of cloud services where the capability provided to the cloud service user is to deploy user-created or acquired applications onto the cloud infrastructure using platform tools supported by the Cloud Provider.	NIST Special Publication 500-291 [2] and ITU-T FG Cloud TR, v1.0 [3]
PCP	Priority Code Point	IEEE 802.1Q [30]

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Protocol Data Unit (PDU)	Information that is delivered as a unit among peer entities of a network and that may contain control information, such as address information, or user data.	
REST API	Representational State Transfer Application Programming Interface	
RMP	Rooted Multipoint	MEF 10.3[17]
RDI	Remote Defect Indicator	RFC6428 [82] and MEF 30.1 [25]
SaaS	Software as a Service is a category of cloud services where the capability provided to the cloud service user is to use the cloud service provider’s applications running on a cloud infrastructure.	NIST Special Publication 500-291 [2] and ITU-T FG Cloud TR, v1.0 [3]
SCTP	Stream Control Transmission Protocol	
SLO	Service Level Objective	The same as Service Level Specification (SLS) as in MEF 23.1 [47] and MEF 6.2 [70]
S-VLAN	Service VLAN (also referred to as Provider VLAN)	IEEE 802.1Q [30]
SLS	Service Level Specification	MEF 10.3[17]
SSL	Secure Sockets Layer	
SSL VPN	Secure Sockets Layer Virtual Private Network	
TCP-AO	Transmission Control Protocol- Authentication Option	
TCP SYN	Transmission Control Protocol Synchronize	
Tenant	The customer using a virtual network and any associated resources (e.g., compute, storage and network). A tenant could be an enterprise, or a department/organization within an enterprise.	RFC7365 [38]
Tenant System	A physical or virtual system that can play the role of a host, or a forwarding element such as a router, switch, firewall, etc. It belongs to a single tenant and connects to one or more VNs of that tenant.	RFC7365 [38]
TLS	Transport Layer Security	
UDP	User Datagram Protocol	
UNI	User Network Interface	MEF 4 [57]

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

UNI-C	UNI - Client (Functional Element)	MEF 4[57]
UNI-N	UNI - Network (Functional Element)	MEF 4 [57]
VAPs (Virtual Access Points)	A logical connection point on the NVE for connecting a Tenant System to a virtual network.	RFC7365 [38]
VLAN	Virtual LAN	IEEE 802.1Q [30]
VLAN ID	VLAN Identifier	IEEE 802.1Q [30]
VM (Virtual Machine)	A VM is an emulation of a particular computer system, operating in a real or hypothetical computer, its implementation may involve specialized hardware, software, or a combination of both, providing a complete substitute for the targeted real machine and a level of functionality required for the execution of a complete operating system that can execute a single computer program.	This document
VM Orchestration System	The system that manages server virtualization across a set of servers such as VMware's vCenter Server or Microsoft's System Center Virtual Machine Manager	draft-ietf-nvo3-arch-01.mht [39]
VM Portability	It is being able to move VM to another site or zone, or moving data/applications from one server to another	This document
VUNI	Virtual UNI	MEF 28 [24]

Table 1: Terminology and Acronyms

3.OCC Architecture Model

The key actors of the OCC architecture for Cloud Services are depicted in Figure 1 where a Cloud Service Provider is responsible for providing an end-to-end Cloud Service to a Cloud Consumer (i.e. customer) using Cloud Carrier(s) and Cloud Provider(s).

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

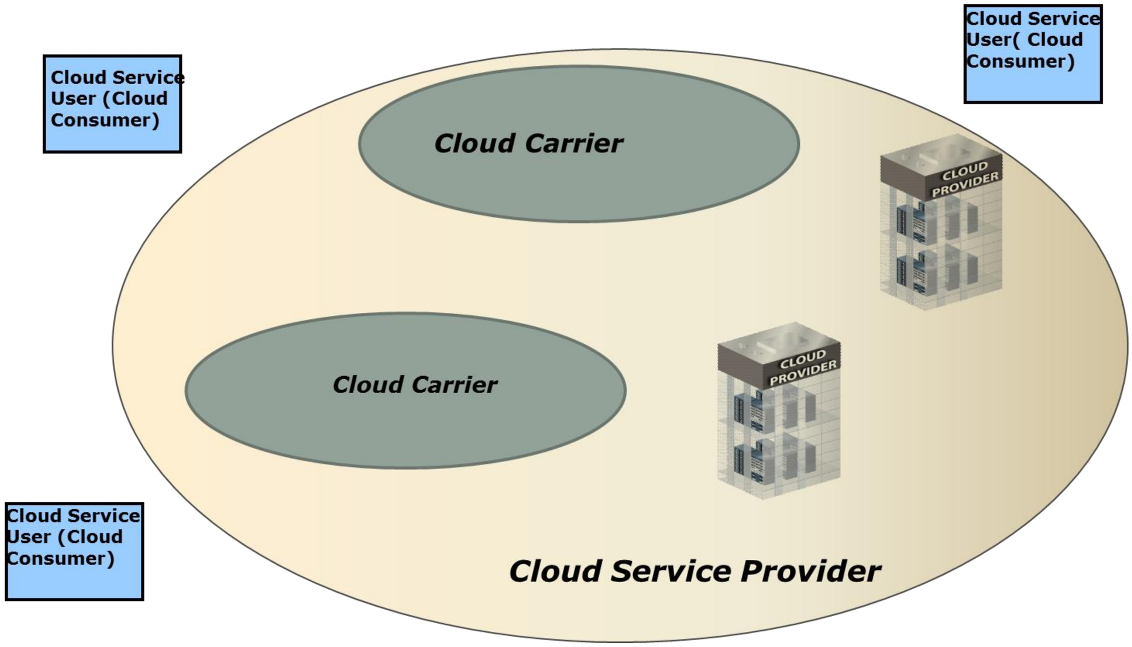

Cloud Service User (Cloud Consumer)
Cloud Service User(Cloud Consumer)
Cloud Carrier
CLOUD PROVIDER
Cloud Carrier
CLOUD PROVIDER
Cloud Service User (Cloud Consumer)
Cloud Service Provider

Figure 1: Cloud Service Actors

A Cloud Consumer interfaces to a Cloud Service Provider (cSP)'s facilities via a standards interface called Cloud Service User Interface (cSUI) (Figure 2) which is a demarcation point between the Cloud Service Provider and the Cloud Consumer[1]. From this interface, the consumer establishes a connection, Cloud Service Connection (cSC), with a Cloud Provider (cP) entity providing the application (Figure 3) where the cP entity can be a virtual machine (VM) with Cloud Service Interface (cSI) or a physical resource such as storage with a cSUI. In addition, a cSC can be between two Cloud Provider entities (Figure 4) or between two Cloud Consumers (Figures 6 and 9).

[1] The user in Figure 2 can be an enterprise with multiple users sharing the same cSUI where CE may represent a gateway device. The CE contains all of the functional elements to request services from a cSP. It could be a physical equipment, a VM, or a collection of VMs 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).

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

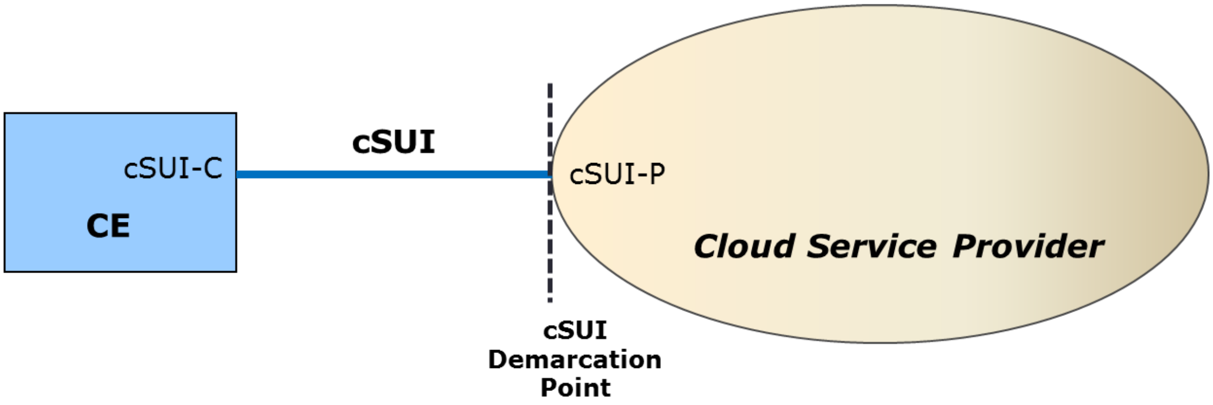


Figure 2: cSUI functionalities are distributed between Customer Edge (CE) and cSP as cSU-C and cSUI-P.

When a cSC is between a Cloud User and a cP physical or virtual resource, the cSC is established between two Cloud Service Connection Termination Points (cSCTPs) residing at the user interface (i.e. cSUI) and the cP interface (i.e. cSUI or cSI).

In Figures 3 and 4, the cSP owns the cP and Cloud Carrier (cC) facilities. When the cP and the cC are two independent entities belonging to two different operators as depicted in Figures 4 and 5, the standards interface between them is called cCcPI (Cloud Carrier Cloud Provider Interface). In this case, a cSC for cloud services can be terminated at either cCcPI or cSI (Figure 12).

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

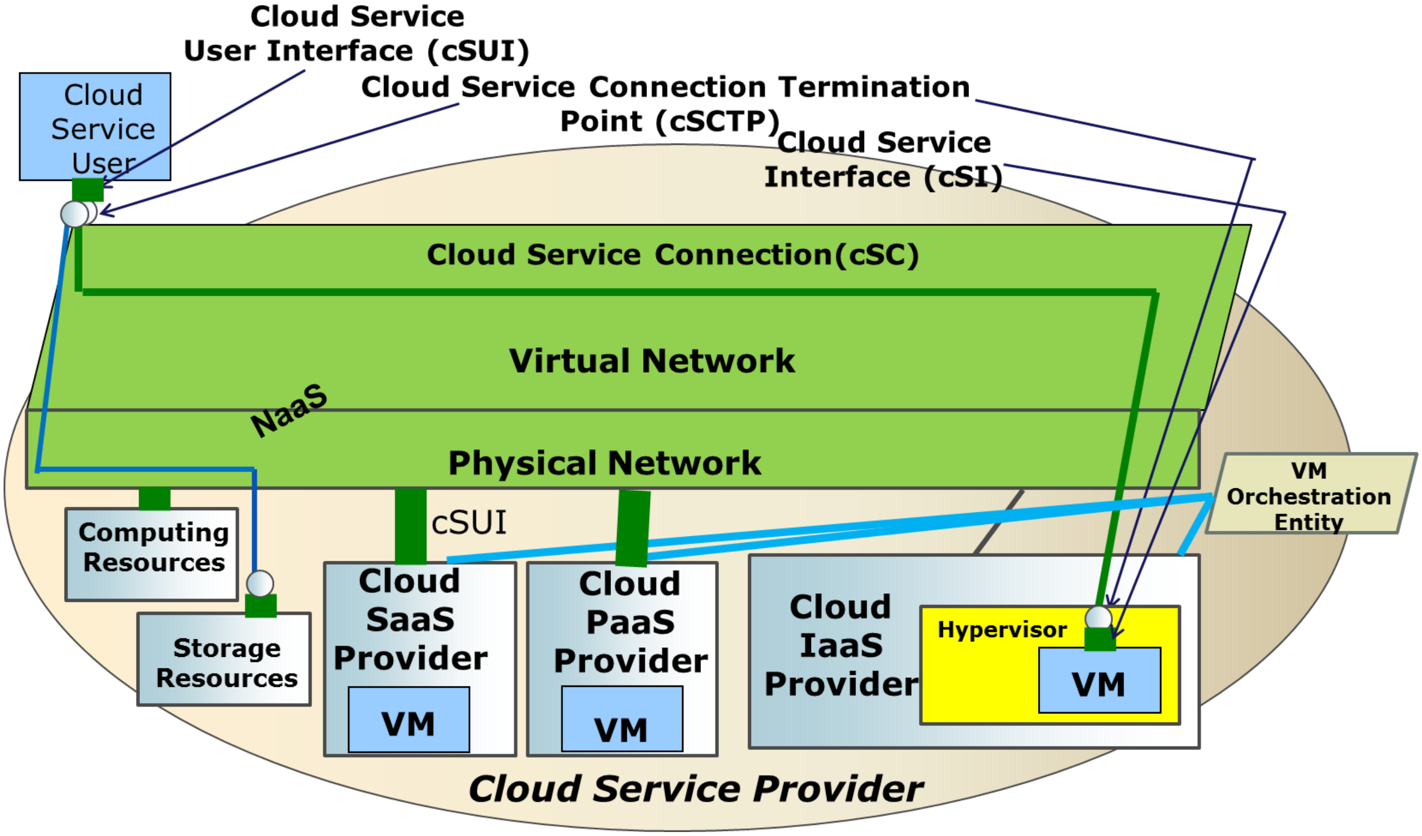
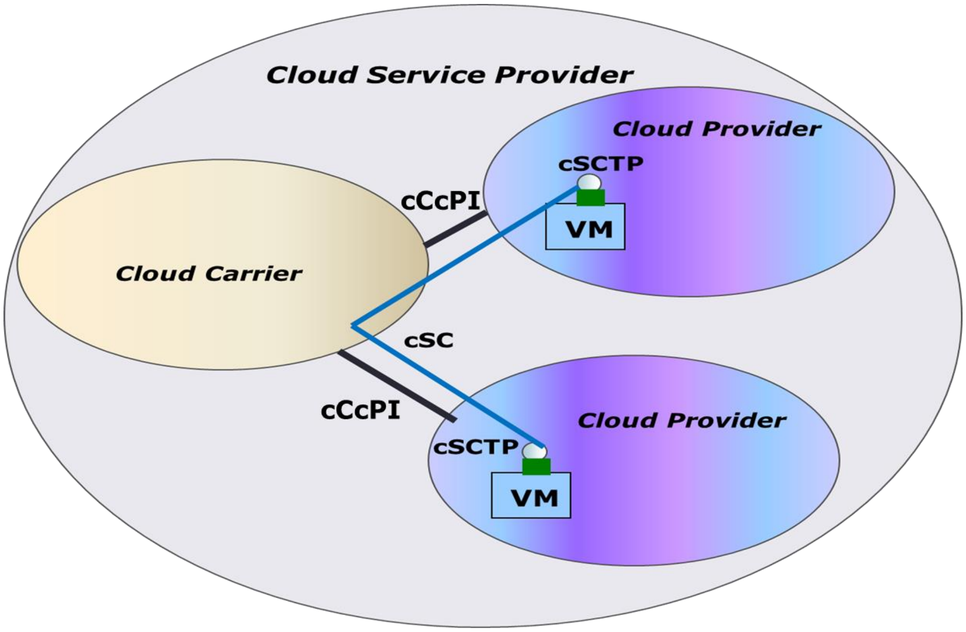


Figure 3: Virtual resources (i.e. VMs) and Physical resources (i.e. computing and storage resources), that belong to one Operator, providing cloud applications.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.



305

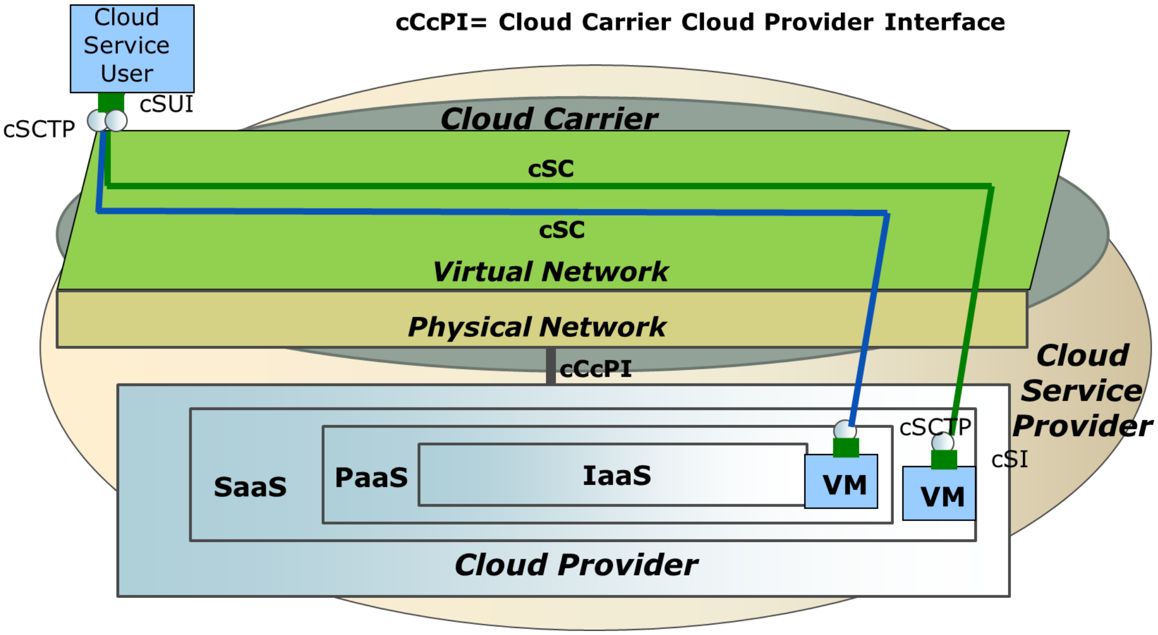
306

307 **Figure 4:** cSC between two Cloud Provider entities.

308

309

310



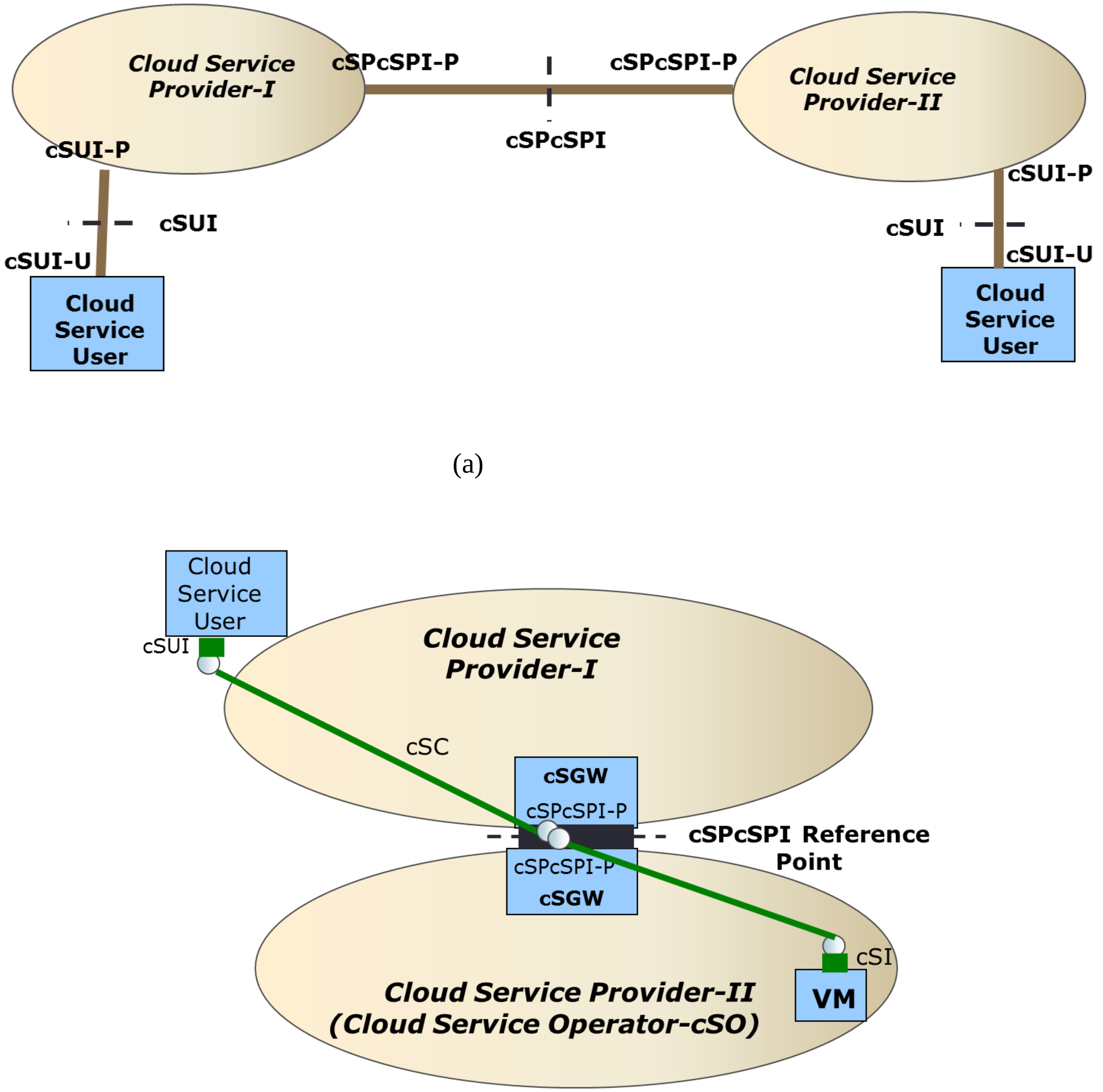
311

312 **Figure 5:** Cloud Provider and Cloud Carrier belong to two different Operators

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

It is also possible for two or more cSPs to be involved in providing a cloud service to a Cloud Consumer as depicted in Figure 6 where two cSPs interface to each other via a standards interface called Cloud Service Provider Cloud Service Provider Interface (cSPcSPI). In this scenario, only one of the cSPs needs to interface to the end user, coordinate resources and provide a bill. The cSP that does not interface to the end user is called Cloud Service Operator (cSO).

The cSPs may employ a gateway to connect to each other (Figure 6), Cloud Service Gateway (cSGW). The cSGW might provide connection multiplexing among other features that are required by cSPcSPI.



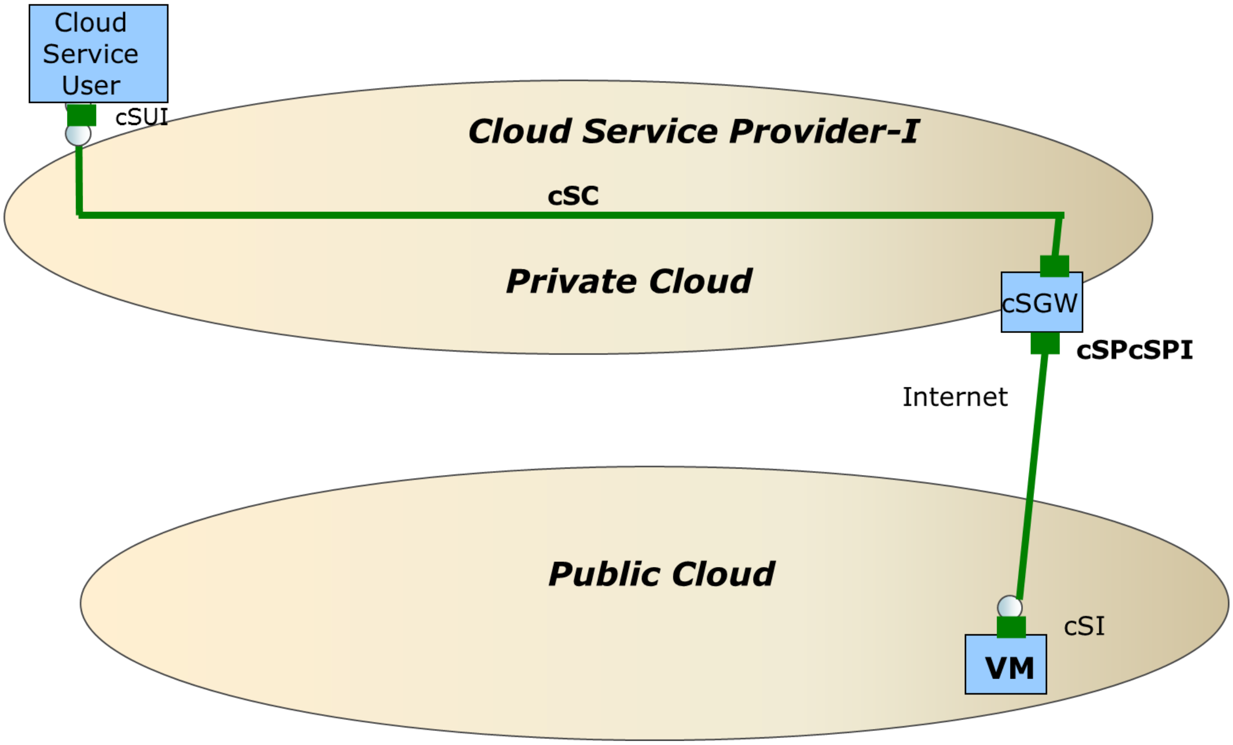
(a)

(b)

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Figure 6: Two Cloud Service Providers collectively providing Cloud Services

A cSP can be private or public. There could be cases that both private and public cSPs collectively provide a cloud service to a cloud consumer, as depicted in Figure 7.

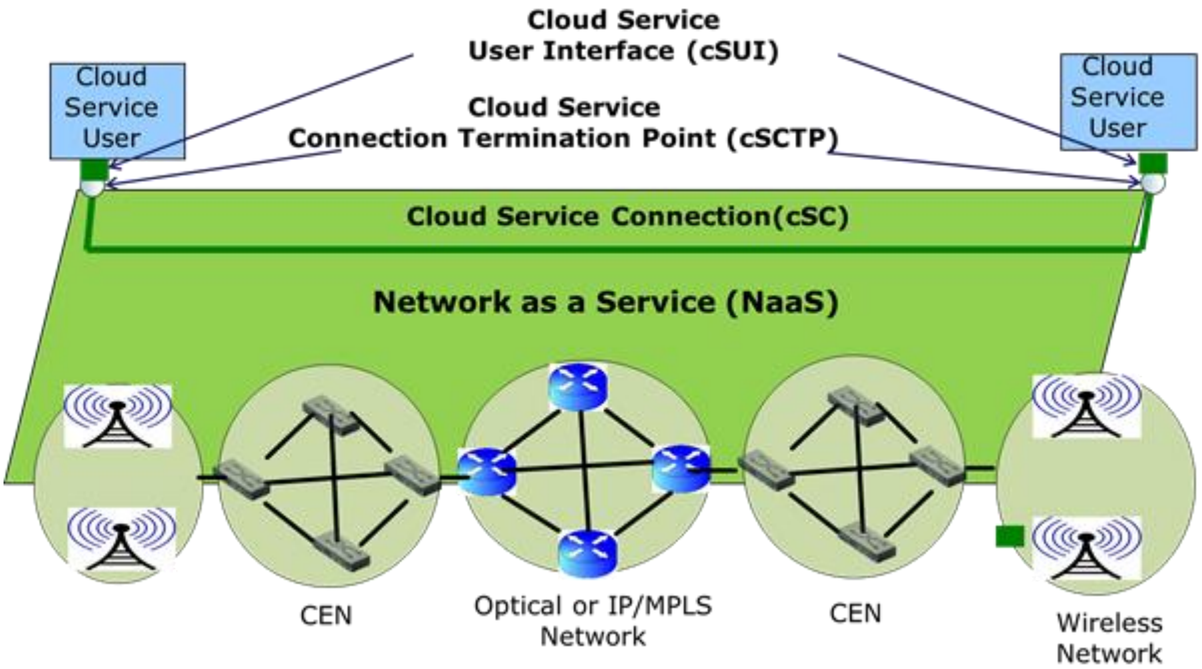


cSGW: Cloud Service Gateway

Figure 7: Private and Public cSPs

A cloud service can be just a network connectivity service provided by a Network as a Service (NaaS), as depicted in Figures 8 and 9. In Figure 9 (a) where Carrier Ethernet Network (CEN) is at the access, MEF UNI is a subset of cSUI in this configuration.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

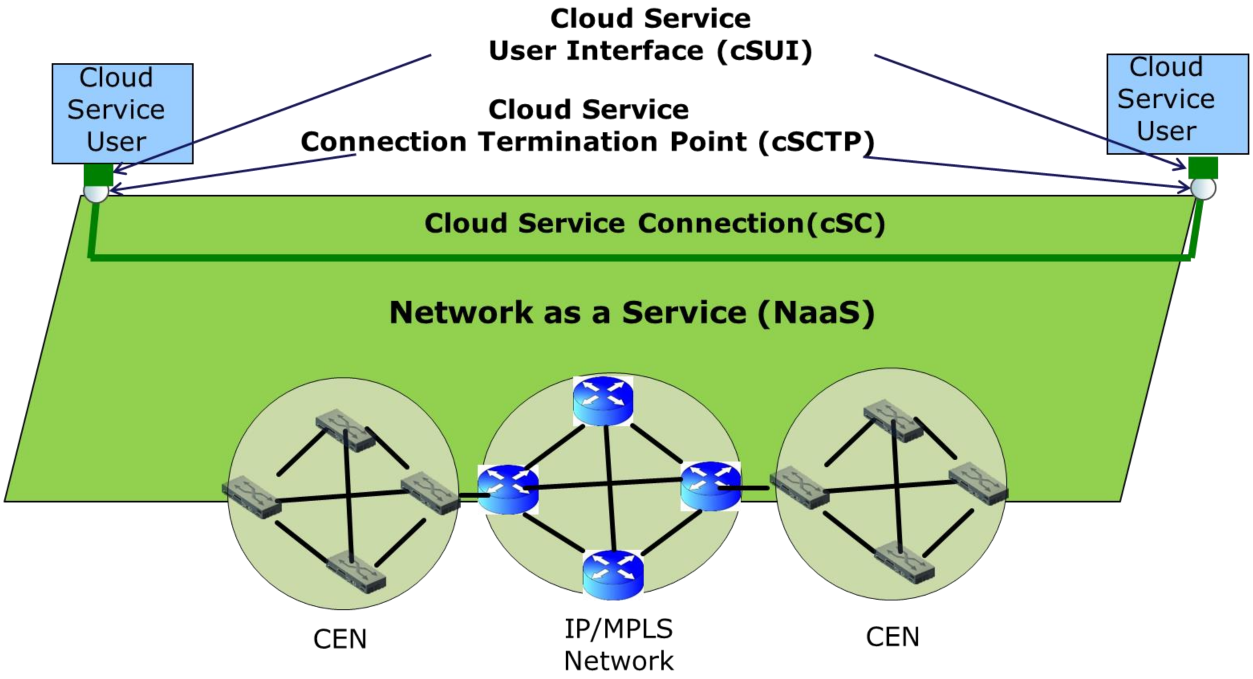


347

348

349

350 **Figure 8:** Network Connectivity Cloud Service provided by NaaS

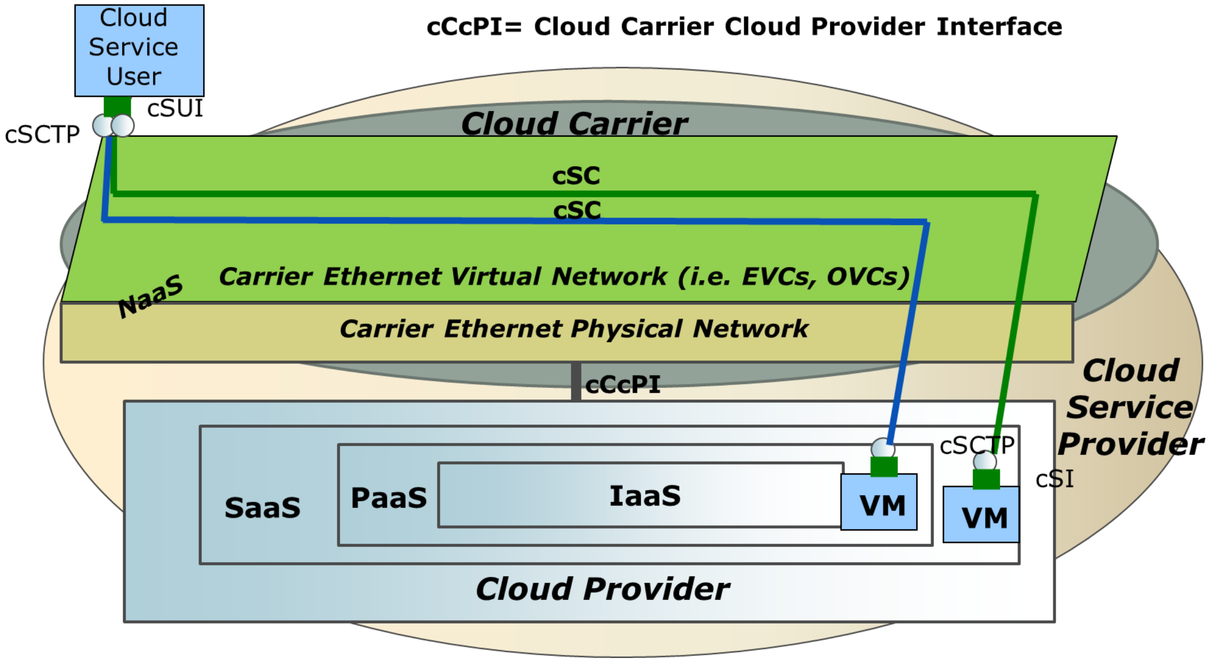


351

352

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

(a)CEN and IP/MPLS network, supporting NaaS andproviding cloud services between two cloud consumers where a cSC is riding over an EVC supported by Carrier Ethernet and IP/MPLS networks.


Cloud Service User
cCcPI= Cloud Carrier Cloud Provider Interface
cSUI
cSCTP
Cloud Carrier
cSC
cSC
NaaS
Carrier Ethernet Virtual Network (i.e. EVCs, OVCs)
Carrier Ethernet Physical Network
cCcPI
Cloud Service Provider
cSCTP
cSI
SaaS
PaaS
IaaS
VM
VM
Cloud Provider

(b)CEN supporting NaaS and providing access to various cloud applications.

Figure 9: Examples of Network Connectivity Cloud Service

A cloud service can be just an application provided by a cP as depicted in Figure 9 (b) where NaaS is used as a dedicated interface to cP facilities. In this case, NaaS is supported by non-cloud resources.

NaaS may consist of multiple layers including Overlay Network Layer as depicted in Figure 10 where Tenant Systems are aggregated at Network Virtual Edge (NVE) providing logical connection points (i.e. Virtual Access Points-VAPs) for Tenant Systems to connect to a virtual network. A VAP can be identified by various types of labels such as a VLAN ID or an internal Virtual Switch (vSwitch) ID connected to a VM.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

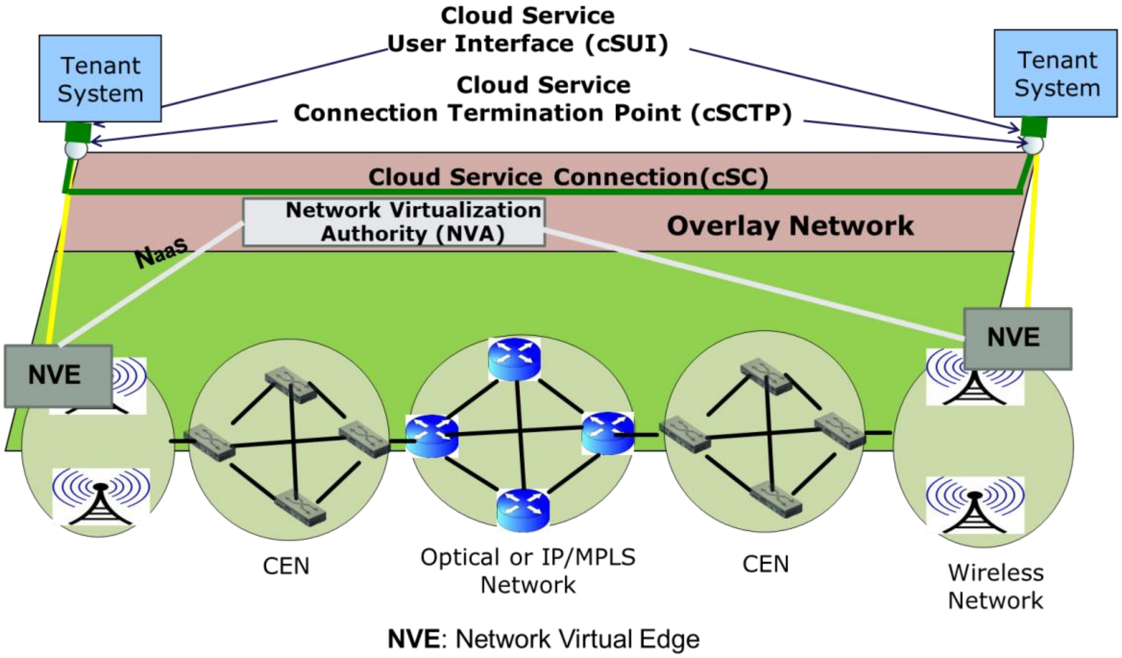
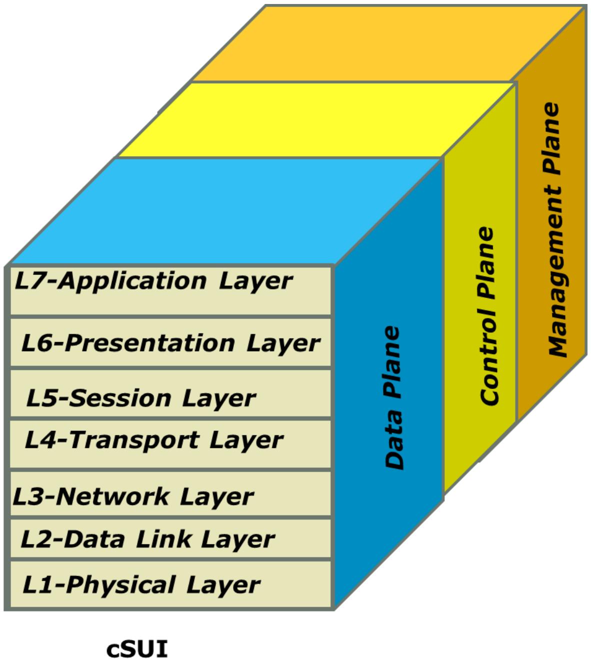

Cloud Service
User Interface (cSUI)
Tenant System
Tenant System
Cloud Service
Connection Termination Point (cSCTP)
Cloud Service Connection(cSC)
Network Virtualization Authority (NVA)
Overlay Network
NaaS
NVE
NVE
CEN
Optical or IP/MPLS Network
CEN
Wireless Network
NVE: Network Virtual Edge

Figure 10 : NaaS Consisting of Overlay Network Layer

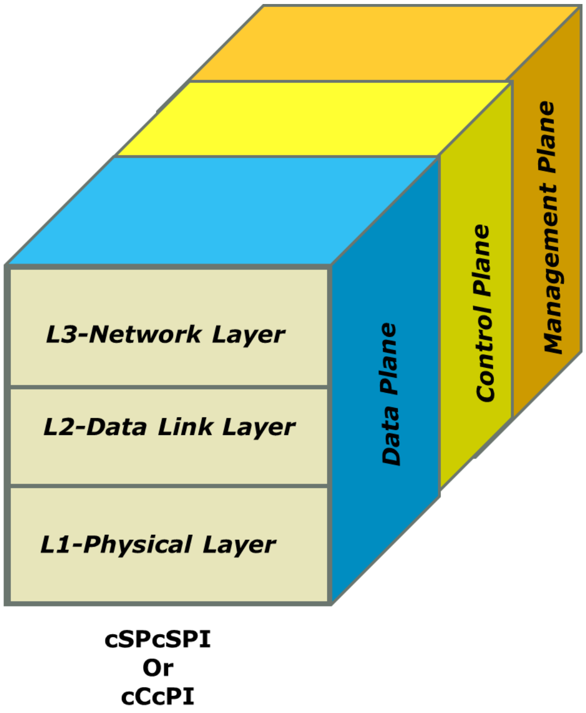
4.Interfaces

The previous section identified interfaces between user and cSP, between cSPs, between cP and cC, between NaaS and Cloud Service application supporting entity. The protocol stack at each interface that can be supported is depicted in Figure 11. Each of the protocol layer may be further decomposed into their data, control and management plane components.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

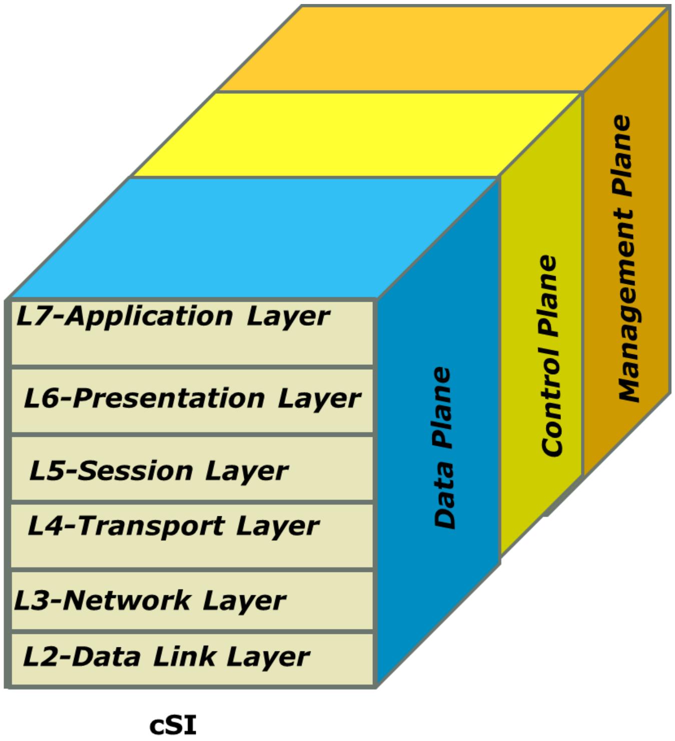


(a)



(b)

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.



(c)

Figure 11 : Protocol Stacks that can be supported at external interfaces

The following sub-sections describe interfaces between entities involved in providing Cloud Services. In order to make the descriptions clear, possible attributes for each interface are listed.

4.1. Cloud Service User Interface (cSUI)

The CE and cSP exchange Service packets (frames) across the cSUI (Figure 2). The cSUI is the physical demarcation point between the domain under the responsibility of the Cloud Service Provider and the domain under the responsibility of the Cloud Service User (or Cloud Consumer). It is dedicated to a single Cloud Service User such as an enterprise. Multiple flows can be multiplexed over this interface using logical connections.

The cSUI is used to interconnect a Cloud Service User to its Cloud Service Provider (s), indicating the location where the responsibility of the service provider ends, and the responsibility of user begins. Functionally the cSUI is an asymmetric, compound functional element that consists of a user side, referred to as the cSU-C, and a cSP side, referred to as the cSUI-P, as illustrated in Figure 2. Thus, the term cSUI is used to refer to these two functional elements, and to the data, management and control plane functions associated with them.

The cSU-C represents all of the functions required to connect a user to a cSP. Individual functions in a cSU-C are entirely in the user domain, and may or may not be managed by the cSP. From the perspective of the cSP, the cSU-C supports the set of functions required to exchange

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

data, control and management plane information with a cSP user or a VM . As such, the cSU-C includes functions associated with NaaS and application specific components.

The cSUI-P represents all of the functions required to connect a cSP to a cSP user. The individual functions in a cSUI-P are entirely in the cSP domain. From the perspective of the user, the cSUI-P supports the set of functions required to exchange data, control and management plane information with the cSP. As such, the cSUI-P includes functions associated with NaaS and application specific components. The cSUI-P could be distributed within the cSP.

A Service packet can be an Ethernet frame, an IP packet, an MPLS packet, or an application PDU transmitted across the cSUI toward the Cloud Service Provider (called an ingress Service Packet) or an Ethernet frame, an IP packet, an MPLS packet, or an application PDU transmitted across the cSUI toward the Cloud Service User (called an egress Service Packet).

The service packet type depends on the interface. For example, in a L2 Ethernet interface, IP packets can be encapsulated in an Ethernet frame such that the user packet becomes an Ethernet frame. On the other hand, in a L3 interface, the user packet is an IP packet.

4.1.1. Attributes

Possible attributes of a cSUI are listed in Table 2.

cSUI attributes		Descriptions and Recommended Values of Attributes
cSUI Id		Arbitrary text string to identify cSUI
Tenant ID		ID of a tenant that cSUI belongs to, If an overlay network is supported at this interface. It is globally unique in a given domain and based on virtual network (VN) identifier such as VLAN IDs. Multiple VN identifiers can belong to a tenant [38].
NaaS Identifier[2]		
Physical Interface		
Ethernet if supported[4]	speed, mode, physical medium	
	MAC Layer	
DOCSIS if supported [5,6]	speed, mode, physical medium	
EPON if supported [7,8]	speed, physical medi-	

[2] NaaS Identifier is included to identify the NaaS that cSUI is connected to. This cSUI-NaaS relationship may be represented via association in the information model instead of an attribute of the cSUI object.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	um	
GPON if supported [9]	speed, physical medium	
WDM if supported [10,11]	speed, physical medium	
SONET/SDH if supported [12, 13]	speed, physical medium	
Optical Transport Network (OTN) [78]		
Maximum Transmission Unit (MTU)		≥ 1522 bytes
Connection Multiplexing		Yes or No
Maximum number of Connection Termination Points(or End Points)		
L2 Ethernet configuration attributes		
MEF UNI Service attributes for Ethernet Private Services in Table 11 of MEF 6.2 [70]		
MEF UNI L2CP Service Attributes for UTA in Table 18 of MEF 45[69]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70]		
MEF UNI L2CP Service Attribute for vNID Case A in Table 23 of MEF 45 [69]		
MEF UNI L2CP Service Attribute for vNID Case B in Table 26 of MEF 45 [69]		
MEF UNI Service attributes for EPL in Table 7 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70] MEF UNI Service attributes for EVPL in Table 10 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70] MEF UNI Service attributes for EP-LAN in Table 13 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70] MEF UNI Service attributes for EVP-LAN in Table 16 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70] MEF UNI Service attributes for EP-Tree in Table 19 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70]		

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

MEF UNI Service attributes for EVP-Tree in Table 22 of MEF 6.2 [70]		
Other L2 Protocols such as Point-to-Point Protocol (PPP) and Point-to-Point Tunneling Protocol (PPTP) if supported		
L3 attributes if L3 protocol such as IP and/or MPLS is supported		
MPLS UNI attributes [49] if MPLS is supported	LSP ID, MTU, Ingress Bandwidth Profile, Egress Bandwidth Profile, MPLS Link Down, MPOLS Link Up, AIS, RDI, Lock Status	
IPv4 Address		
DSCP Marking		
IPv6 Address		
IPv4 VPN[31]		
IPv6 VPN [32]		
L4 attributes if L4 protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Stream Control Transmission Protocol (SCTP) are supported		
L5 attributes if L5 protocols such as NFS, NetBios names, RPC and SQL are supported.		
L6 attributes if L6 protocols such as ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI are supported		
L7 attributes if L7 protocols/applications such as WWW browsers, NFS, SNMP, Telnet, HTTP, FTP are supported.		
Operational State		Enabled or Disabled[3]
Admin State		Enabled or Disabled
Interface Level Security		
ACL (Access Control List) attributes		
Packet Encryption	IPSec Encapsulating Security Payload (ESP) attributes	
	SSL VPN (Secure Sockets Layer Virtual Private Network)	
Connection Authentication		
	IPSec Authentication Header (AH) attributes	

[3] Operational state and Administrative state attribute values are aligned with ITU-T M.3100 [72]. RFC2863 [73] define them differently.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	TCP- Authentication Option (TCP-AO) attributes	
Service Level Security		
	Rate limiting for DoS attacks: Rate limiting of TCP SYN packets and ICMP/Smurf attributes.	
	Keys for API	
Billing		
	Recurring Charges	
	Non-recurring Charges	

Table 2 : cSUI Attributes

4.1.2. Dynamic Attributes

The following attributes are likely to be configured on-demand:

- MTU or Maximum Service Frame Size
- Connection Multiplexing
- Maximum Number of Connection Termination Points
- Bandwidth Profile Parameters
- Mapping of CoS ID value to CoS Name [67]

4.1.3. Traffic Management

Traffic management applies to user frames or packets at cSUI supporting L2 and above. The traffic management functionalities include bandwidth profile, policing, marking and traffic shaping at the interface.

For Ethernet L2 cSUI, bandwidth profile parameters and algorithms defined in MEF 10.3 [17] and MEF 41 [67] per UNI apply.

For IP networks, DSCP marking is used to mark packets that are processed according to the network policies for admission control, prioritization, mapping into classes of Integrated Services, or combinations of these techniques. In L2 Ethernet networks, both PCP and DSCP are used for traffic prioritization and coloring.

In MPLS networks, EXP field (or Traffic Classification field) is used for marking [50]. Traffic engineering is further addressed in [77].

4.1.4. Fault Management

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

The fault management functions of cSUI consist of fault management functions at physical layer, L2, L3, and above (if supported). They include:

- AIS and RDI for physical port failures
- Link level OAM [7]
- UNI MEG for Service OAM [25] for L2 interface
- ELMI related OAM [51] for L2 interface
- MPLS OAM [52] for MPLS interface

If the interface is IP/WDM, notifications for wavelength event, port event, and fiber event are part of fault management functionalities.

4.1.5.Performance Management

User frames or packets of received, transmitted, and dropped of yellow and green colors [34,35] will be counted at cSUI.

For L2 Ethernet interface, relevant performance requirements in MEF15 [18], MEF35 [27], MEF 35.0.1[28], and MEF 35.0.2 [68] apply.

For L3 interface, relevant performance requirements in RFC 4293 [33], RFC 2697 [35] and RFC 2698 [34] apply.

4.1.6.Security

Security capabilities of cSUI established between the CE and cSP are:

- Authentication between CE and cSP
- Data/Packet encryption
- Service Level Security against attacks such as Distributed Denial of Service (DDoS) attacks
- Service invocation key exchange schemes

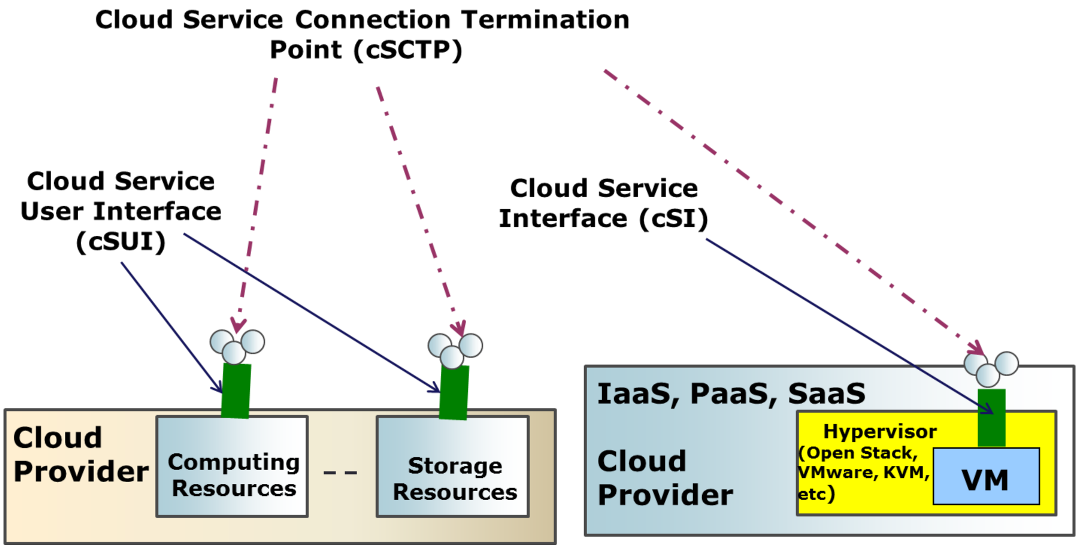
4.1.7.Billing

Service charges can be non-recurring installation charge and recurring charges. The recurring charges can be monthly or usage based. The usage based billing choice depends on the service. For example, if it is a storage service, it can be based on the size of storage in Gbytes and duration of the usage.

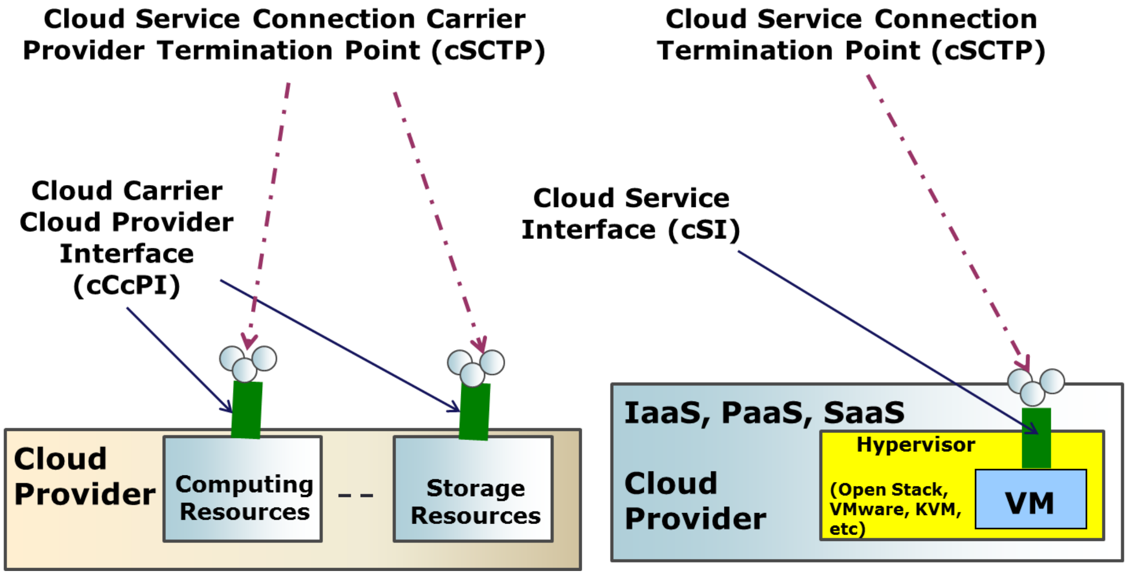
4.2. Cloud Service Interface (cSI)

The cSI is the interface of a Cloud Service application supporting entity of a Cloud Provider (cP) such as VM over Open Stack or VMware [44,45,46].

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.


Cloud Service Connection Termination Point (cSCTP)
Cloud Service User Interface (cSUI)
Cloud Service Interface (cSI)
IaaS, PaaS, SaaS
Cloud Provider
Computing Resources
Storage Resources
Cloud Provider
Hypervisor
(Open Stack, VMware, KVM, etc)
VM

(a) cP physical resources are interfacing cC via cSUI while cP virtual resources are interfacing cC via cSI


Cloud Service Connection Carrier Provider Termination Point (cSCTP)
Cloud Service Connection Termination Point (cSCTP)
Cloud Carrier Cloud Provider Interface (cCcPI)
Cloud Service Interface (cSI)
IaaS, PaaS, SaaS
Cloud Provider
Computing Resources
Storage Resources
Cloud Provider
Hypervisor
(Open Stack, VMware, KVM, etc)
VM

(b) cP physical resources are interfacing cC via cCcPI while cP virtual resources are interfacing cC via cSI

Figure 12: cSI

Multiple VMs can be accessed via single cSC as depicted in Figure 13.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

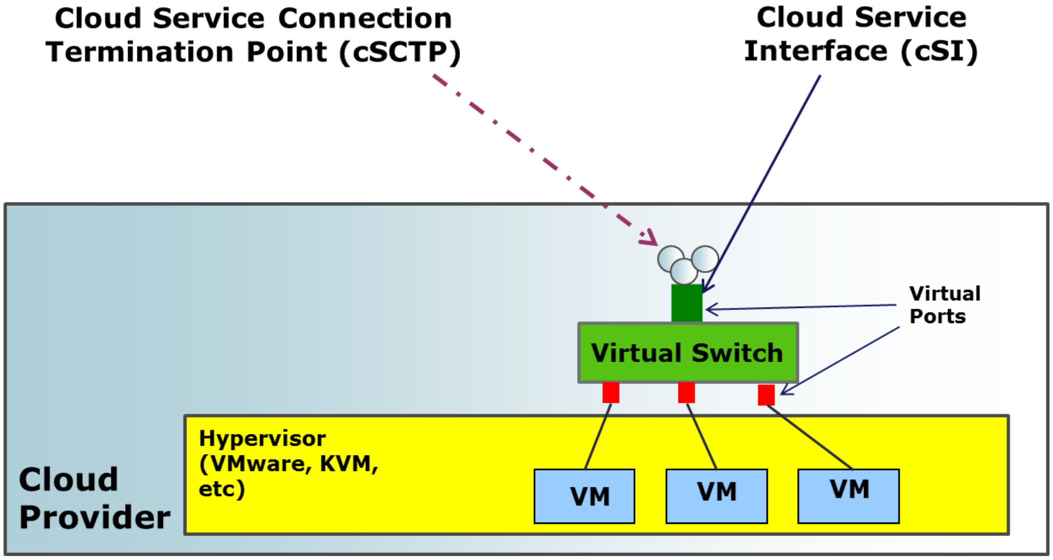
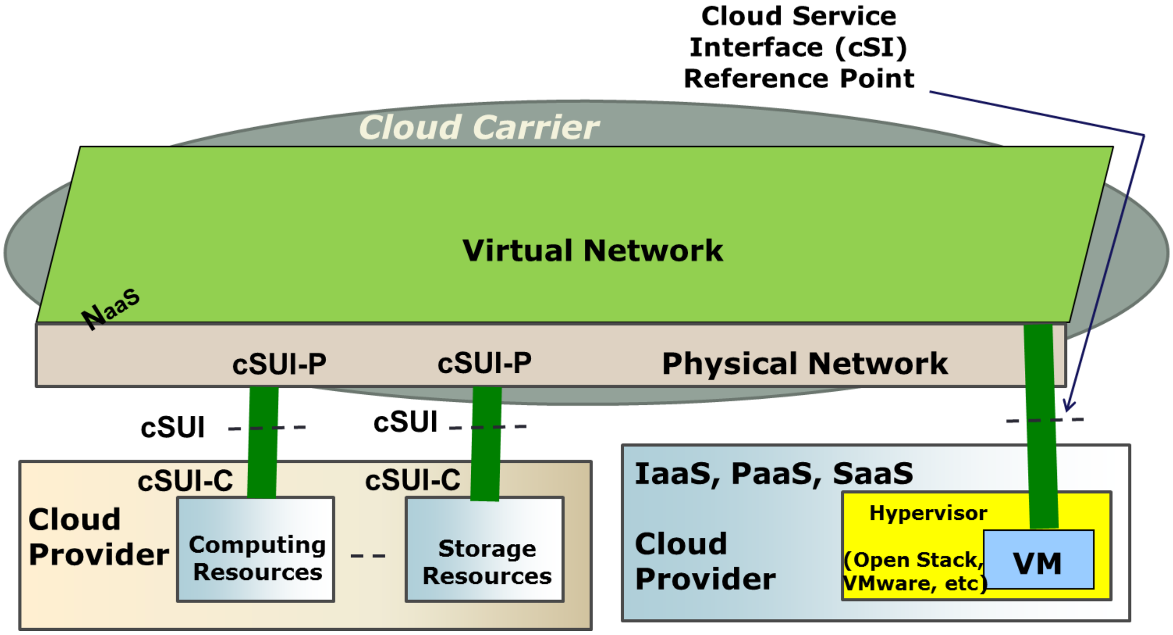
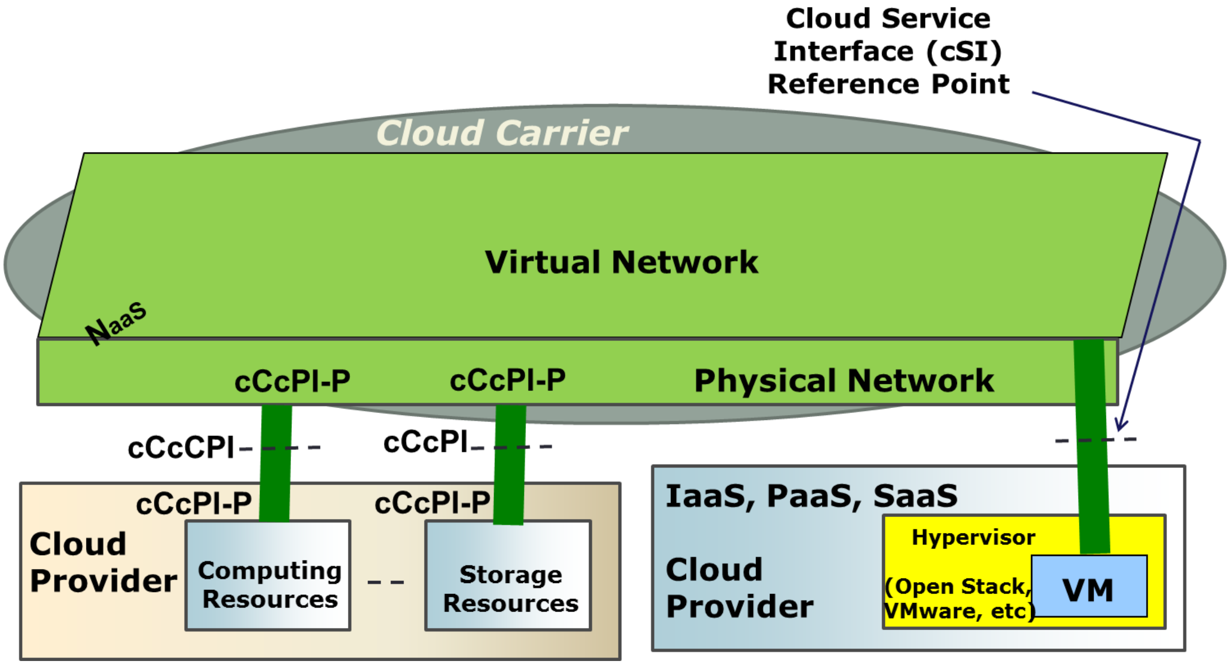

Cloud Service Connection Termination Point (cSCTP)
Cloud Service Interface (cSI)
Virtual Ports
Virtual Switch
Hypervisor (VMware, KVM, etc)
VM
VM
VM
Cloud Provider

Figure 13: Accessing multiple VMs via single cSC



(a) cSUI and cSI are the demarcation points between cP resources and cC

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.



(b) Physical Resources comply with cCcPI while virtual resources comply with cSI

Figure 14: cSI Reference Point

A cloud service may or may not use virtual resources of a cP. For example, a Cloud Storage Service (see section 6) employs physical servers. These servers may be accessed via the cCcPI between cP and cC as depicted in Figure 14 (b). This is analogous to MEF ENNI of CEN. The interface between cC and cP can be a cSUI as well, as depicted in Figure 14 (a). This is analogous to MEF UNI of CEN.

4.2.1. Attributes

The cSI possible attributes are listed in Table 3.

cSI attributes	Descriptions and Recommended Values of Attribute
cSI Id	Arbitrary text string to identify cSI
VM ID	http://www.ietf.org/id/draft-ietf-opsawg-vmm-mib-00.txt [53] uses 128-bit Universally Unique ID (UUID) [36] as a unique identifier for a VM in an administrative region.
List of NaaS	List of NaaS employing this VM or server (i.e. application entity is shared or dedicated)
Interface Protection	1+1 or 1:1 or None

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Connection Multiplexing		Yes or No
Maximum number of Connection Termination Points		
L2 Ethernet configuration attributes[17, 71, 66]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70]		
MEF UNI Service attributes for EPL in Table 7 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70] MEF UNI Service attributes for EVPL in Table 10 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70] MEF UNI Service attributes for EP-LAN in Table 13 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70] MEF UNI Service attributes for EVP-LAN in Table 16 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70] MEF UNI Service attributes for EP-Tree in Table 19 of MEF 6.2 [70]		
MEF UNI Service attributes in Table 4 of MEF 6.2 [70] MEF UNI Service attributes for EVP-Tree in Table 22 of MEF 6.2 [70]		
Other L2 Protocols such as Point-to-Point Protocol (PPP) and Point-to-Point Tunneling Protocol (PPTP) if supported		
VM Protection (if supported)	This would be redundant VM or redundant server or redundant resource offering the service	

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

VM Portability[4]		Yes or No
L3 attributes if L3 protocol such as IP and MPLS are supported		
MPLS UNI attributes [49] if MPLS is supported	LSP ID, MTU, Ingress Bandwidth Profile, Egress Bandwidth Profile, MPLS Link Down, MPLS Link Up, AIS, RDI, Lock Status	
IPv4 Address		
DSCP Marking		
IPv6 Address		
IPv4 VPN[31]		
IPv6 VPN [32]		
NAT		
L4 attributes if L4 protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Stream Control Transmission Protocol (SCTP) are sup-ported		
General Ports	32111 (TCP): Open in both directions between user VMware View Virtual Desktop and user VMware View Client. This facilitates USB redirection between user View Client and Virtual Desktop.	
	9427 (TCP): Multimedia Redirection (MMR) is supported by View Client and View Client with Offline Desktop on certain operating systems where MMR is not required in both directions.	
PCoIP (PC over IP) Ports	50002(TCP/UDP): Used for PCoIP in a VMware View 4.0.x and later environment. This port is required for the PCoIP display protocol on the software client and must be open in both inbound	

[4] VM Portability is being able to move VM to another site/zone or moving data/applications from one server to another. A VM could be moved across different hypervisors, such as VMware's ESXi, the Apache Software Foundation's Xen, Microsoft's Hyper-V and the open source KVM (kernel-based virtual machine).

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	and outbound directions.	
	4172 (TCP/UDP): Used for PCoIP in a VMware View 4.5 and later environment. This port is required for the PCoIP display protocol. The port 4172 UDP must be open in both inbound and outbound directions.The port 4172 TCP must be open in only the inbound direction.	
RDP (Remote Desktop Protocol) Ports	3389 (TCP): This port is required for usage in a View environment where Microsoft Remote Desktop Protocol (RDP) is the preferred display protocol. This port must be open between either the View Client and the Virtual Desktop, or the VMware View Connection or security server and the Virtual Desktop.	
Connection server Ports	4001 (TCP): This port must be open in the outbound direction so the View agent can report its status to the connection broker it is bound to.	
L5 attributes if L5 protocols such as NFS, NetBios names, RPC and SQL are supported.		
L6 attributes if L6 protocols such as ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI are supported		
L7 attributes if L7 protocols/applications such as WWW browsers, NFS, SNMP, Telnet, HTTP, FTP are supported.		
Operational State		Enabled or Disabled
Admin State		Enabled or Disabled
Security		
SSL (Secure Socket Layer) Termination	Terminating SSL traffic for services such as load	

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	balancer providing: • Centralized Certificate Management • SSL acceleration for improved throughput • Reduced CPU load at the application server for improved performance • HTTP and HTTPS Session Persistence	
ACL		
Packet encryption	IPSec ESP (Encapsulating Security Payload)	
	SSL VPN	
Connection Authentication	IPSec AH	
	TCP-AO	
Service Level Security	Rate limiting of DoS attacks and excessive resource consumption	
Data confidentiality/privacy	Prevent tenants from eavesdropping on each other via logical separation	
Session Layer Security	REST API (Representational State Transfer Application Programming Interface) over SSL (Secure Sockets Layer) /TLS (Transport Layer Security)	
	API keys	
Billing	Recurring Charges	
	Non-recurring Charges	

Table 3 : cSI Attributes

4.2.2. Dynamic Attributes

The following attributes are likely to be configured on-demand:

- MTU or Maximum Service Frame Size
- Bandwidth Profile Parameters
- Portability
- VM Protection
- Server Protection

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

4.2.3.Traffic Management

The traffic management functionalities include bandwidth profile, policing, marking and traffic shaping at the interface.   For cSI employing L2 Ethernet, bandwidth profile parameters and algorithm defined in MEF 10.3 can be used as a base.

For IP networks, DSCP marking is used to mark packets that are processed according to the network policies for admission control, prioritization, mapping into classes of Integrated Services, or combinations of these techniques. In L2 Ethernet networks, both PCP and DSCP are used for traffic prioritization and coloring.

For MPLS networks, EXP field is used for marking [50]. Traffic engineering is further addressed in [77].

4.2.4. Fault Management

For cSI employing L2 Ethernet, fault management consists of :

- UNI MEG for Service OAM [25]
- AIS and RDI for EVC failures

For cSI employing L3 IP VPN interface, fault management consists of notifications related to the VPN interface:

- SSL VPN Login failure
- Internet Key Exchange (IKE) VPN Tunnel failure

For cSI employing MPLS interface, fault management consists of:

- MPLS OAM [50] that includes link down and AIS notifications.

4.2.5.Performance Management

Service frames or packets received, transmitted, and dropped will be counted at cSI.

For cSI employing L2 Ethernet, EVC performance requirements in MEF15 [18], MEF35 [27] and MEF 35.0.1 [28] apply.

For cSI employing L3, IP Flow performance requirements in RFC 7012 [54] apply.

4.2.6.Security

Security capabilities of cSI established between the Cloud Service Application Entities and cC or cSP are:

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

•Connection Authentication such as IPSec-AH (Authentication Header) or TCP-AO (Authentication Option)
•Packet encryption such as VPN
•Data confidentiality and privacy such as identity and access management, or DLP (Data Loss Prevention) at the virtual network level
•Service Level Security against attacks such as DDoS (Distributed Denial of Service)
•Session Layer Security such as REST (Representational State Transfer) API (Application Programming Interface) invocation over SSL (Secure Sockets Layer) or TLS (Transport Layer Security)
•Service invocation key exchange schemes

4.2.7.Billing

Billing will depend on the service features and their usage.

4.3. Cloud Carrier Cloud Provider Interface (cCcPI)

The cCcPI is defined as a reference point representing boundary between a Cloud Carrier and Cloud Provider that are operated as separate administrative domains (Figure 5). This reference point provides demarcation between cC and cP for cloud services.

The cCcPI-P representing the functionality at cCcPI supports the protocol stack depicted in Figure 11. Furthermore, it is expected to preserve the cCcPI crossing cSC characteristics that are reflected in attributes listed in Tables 7.

This interface is expected to be very similar to ENNI [22] if the interface is L2 Ethernet.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

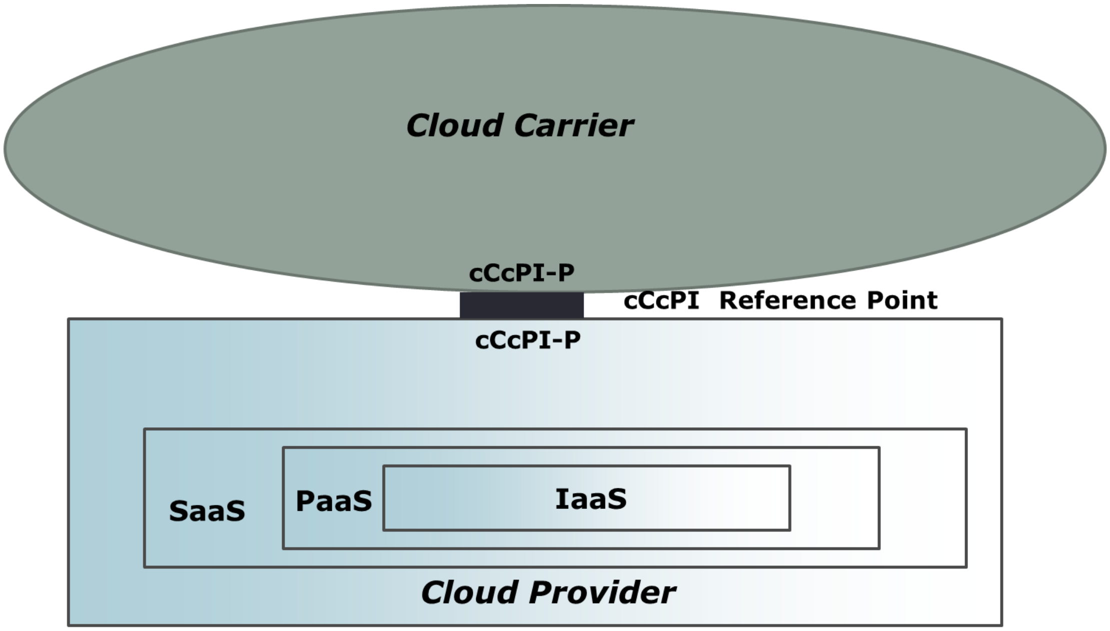


Figure 15: cCcPI

4.3.1. Attributes

The cCcPI possible attributes are listed in Table 4.

cCcPI attributes		Descriptions and Recommended Attribute Values
cCcPI Id		Arbitrary text string to identify the cCcPI
Name of cSP[5]		Arbitrary text string to identify the cSP
Physical Interface		
Ethernet[4]	speed, mode, physical medium	
	MAC Layer	
DOCSIS if supported [5,6]	speed, mode, physical medium	
EPON if supported[7,8]	speed, mode, physical medium	
GPON if supported[9]	speed, mode, physical medium	
WDM if supported[10,11]	speed, mode, physical medium	
SONET/SDH if supported [12,13]	speed, mode, physical	

[5] This attribute can be represented via an association between cC and cSP obects, and cP and cSP objects.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	medium	
Optical Transport Network (OTN) [78]		
MTU		≥ 1522 bytes
Connection Multiplexing		Yes or No
Maximum number of Connection Termination Points (or End Points)		
L2 Ethernet configuration attributes[21,22]		
MEF ENNI Service attributes in Table 2 of MEF 26.1 [22]		
MEF ENNI L2CP Service Attributes for Access EPL in Table 17 of MEF 45 [69]		
MEF ENNI L2CP Service Attributes for UTA in Table 20 of MEF 45 [69]		
MEF ENNI L2CP Service Attributes for vNID Case A in Table 25 of MEF 45 [69]		
MEF ENNI L2CP Service Attributes for vNID Case B in Table 28 of MEF 45 [69]		
L2 Ethernet SOAM attributes [25]		
Maintenance Entity Group (MEG) Id		
Maintenance End Point (MEP) Id		
MEP Level		
LAG MEG		
LAG Link MEG		
Other L2 Protocols such as Point-to-Point Protocol (PPP) and Point-to-Point Tunneling Protocol (PPTP) if supported		
L3 attributes if L3 protocol such as IP and MPLS are supported		
MPLS UNI attributes [49] if MPLS is supported	LSP ID, MTU, Ingress Bandwidth Profile, Egress Bandwidth Profile, MPLS Link Down, MPLS Link Up, AIS, RDI, Lock Status	
Fast Reroute [71,62]		
NAT		
IPv4 Subnet Address		
IPv6 Subnet Address		
DSCP Marking		
IPv4 VPN [31]		
IPv6 VPN [32]		
Security (between CP and CC) (if supported)		
ACL		
Packet encryption	IPSec ESP	
	SSL VPN	
Connection Authentication	IPSec AH	

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Service Level Security	Rate limiting of DoS attacks and excessive resource consumption	
Data confidentiality/privacy	Prevent tenants from eavesdropping on each other via logical separation	

Table 4 : cCcPI Attributes

4.3.2. Dynamic Attributes

The cCcPI attributes are most likely to be static. It is expected to have gateways on both sides to handle the interface. The cC gateway maybe shared among cPs. Similarly cP gateway may be shared among cCs. In these cases where the gateways are not dedicated, bandwidth profile attributes maybe configured dynamically.

4.3.3.Traffic Management

Traffic management applies to service frames or packets crossing cCcPI supporting L2 and above. The traffic management functionalities include bandwidth profile, policing, marking and traffic shaping at the interface.

For Ethernet L2 cCcPI, bandwidth profile parameters and algorithm defined in MEF 26.1 [22] will be used as base here.

For IP networks, DSCP marking is used to mark packets that are processed according to the network policies for admission control, prioritization, mapping into classes of Integrated Services, or combinations of these techniques. In L2 Ethernet networks, both PCP and DSCP are used for traffic prioritization and coloring.

For MPLS networks, EXP field is used for marking [50]. Traffic engineering is further addressed in [77].

4.3.4. Fault Management

The fault management functions of cCcPI consist of fault management functions at physical layer, L2, and L3 (if supported). These are including:

- AIS and RDI for physical port failures
- Link level OAM [7]
- ENNI MEG for Service OAM [25] for L2 interface
- LAG MEG [25]
- LAG Link MEG [25]
- MPLS OAM [52]

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

If the interface is IP/WDM, generating notifications for Wavelength event, Port event, and Fiber event; and protection at WDM layer are part of fault management functionalities.

4.3.5.Performance Management

Service frames or packets of received, transmitted, and dropped of yellow and green colors [34,35] will be counted at cCcPI.

For L2 interface, relevant performance requirements in MEF 15[18], MEF35 [27], MEF 35.0.1 [28], and MEF 35.0.2 [68] apply.

For L3 interface, relevant performance requirements in RFC 4293 [33], RFC 2697 [35] and RFC 2698 [34] apply.

4.3.6.Link Protection

For L2 Ethernet interface, LAG/LACP can be used when there are at least two links, as described in MEF32 [55].

For MPLS/WDM, traffic is protected either at the light-path level or at the label switched path (LSP) level based on the restoration time requirements. In light-path-level protection, traffic on a LSP is protected by routing it over primary light-paths which are protected at the optical layer by their respective backup light-paths. In LSP-level protection, the traffic on a primary LSP is protected at MPLS layer by a backup LSP. In this case, both primary and backup LSPs traverse unprotected light_paths.

In addition to LAG/LACP, protection capabilities such as Fate Sharing [61], Loop-Free Alternatives [62] or Shared Risk Link Groups can be employed to protect traffic during link failures.

4.3.7.Security

Security capabilities of cCcPI that are established between the cC and cP are:

- •Connection Authentication such as IPSec-AH
- •Packet encryption such as VPN
- •Data confidentiality and privacy such as identity and access management, or DLP at the virtual network level
- •Service Level Security against attacks such as DDoS

4.3.8.Billing

The billing might depend on the relationship between cC and cP. It is possible that below certain number of transactions, neither side will pay anything. The side exceeding the pre-set limit may pay the other side based on their agreement.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

4.4. Cloud Service Provider Cloud Service Provider Interface (cSPcSPI)

cSPcSPI is defined as a reference point representing the boundary between two Cloud Service Providers (cSPs) that are operated as separate administrative domains. This reference point provides demarcation between two cSPs for cloud services. It is depicted in Figure 6 and Figure 7.

The cSPcSPI-P representing the functionality at cSPcSPI supports the protocol stack depicted in Figure 11. Furthemore, it is expected to preserve the cSPcSPI crossing cSC characteristics that are reflected in attributes listed in Tables 7.

The cSPcSPI is expected to be very similar to the cCcPI and a superset of to ENNI [22] if the interface is L2 Ethernet.

4.4.1. Attributes

The cSPcSPI possible attributes are listed in Table 5. The attributes are the same as those for cCcPI, but may take different values.

cSPcSPI attributes		Descriptions and Recommended Attribute Values
cSPcSPI Id		Arbitrary text string to identify the cSPcSPI
Name of cSPs interfacing each other		Arbitrary text string to identify the cSP
Physical Interface		
L2 Ethernet[4]		
	speed, mode, physical medium	
	MAC Layer	
DOCSIS if supported [5,6]	speed, physical medium	
EPON if supported[7,8]	speed, physical medium	
GPON if supported[9]	speed, physical medium	
WDM if supported[10,11]	speed, physical medium	
SONET/SDH if supported [12,13]	speed, physical medium	
Optical Transport Network (OTN) [78]		
MTU		≥ 1522 bytes
Connection Multiplexing		Yes or No
Maximum number of Connection Termination Points (or End Points)		
L2 Ethernet configuration attributes[20,22]		
MEF ENNI Service attributes in Table 2 of MEF 26.1 [22]		
MEF ENNI L2CP Service Attributes for Access EPL in Table 17 of MEF 45 [69]		

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

MEF ENNI L2CP Service Attributes for UTA in Table 20 of MEF 45 [69]		
MEF ENNI L2CP Service Attributes for vNID Case A in Table 25 of MEF 45 [69]		
MEF ENNI L2CP Service Attributes for vNID Case B in Table 28 of MEF 45 [69]		
L2 Ethernet SOAM attributes [25]		
Maintenance Entity Group (MEG) Id		
Maintenance End Point (MEP) Id		
MEP Level		
Maintenance Intermediate Point (MIP) Id		
LAG MEG		
LAG Link MEG		
Operator MEG		
Other L2 Protocols such as Point-to-Point Protocol (PPP) and Point-to-Point Tunneling Protocol (PPTP) if supported		
L3 attributes if L3 protocol such as IP and MPLS are supported		
MPLS UNI attributes [49] if MPLS is suported	LSP ID, MTU, Ingress Bandwidth Profile, Egress Bandwidth Profile, MPLS Link Down, MPOLS Link Up, AIS, RDI, Lock Status	
Fast Reroute [71,62]		
NAT		
IPv4 Subnet Address		
IPv6 Subnet Address		
DSCP Marking		
IPv4 VPN [31]		
IPv6 VPN [32]		
Security between cSPs (if supported)		
ACL		
Packet encryption	IPSec ESP	
	SSL VPN	
Connection Authentication	IPSec AH	
Service Level Security	Rate limiting of DoS attacks and excessive resource consumption	

Table 5 : cSPcSPI Attributes

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

4.4.2. Dynamic Attributes

The cSPcSPI attributes are most likely to be static, except administrative state. It is expected to have gateways on both sides to handle the interface. The gateways maybe shared among multiple cSPs. In these cases where the gateways are not dedicated, bandwidth profile attributes may need to be configured dynamically.

4.4.3.Traffic Management

Traffic management applies to service frames or packets crossing cSPcSPI supporting L2 and above. The traffic management functionalities include bandwidth profile, policing, marking and traffic shaping at the interface.

For Ethernet L2 cSPcSPI, traffic management parameters defined in MEF 26.1 [22] apply here.

For IP networks, DSCP marking is used to mark packets that are processed according to the network policies for admission control, prioritization, mapping into classes of Integrated Services, or combinations of these techniques. In L2 Ethernet networks, both PCP and DSCP are used for traffic prioritization and coloring.

For MPLS networks, EXP field is used for marking [50]. Traffic engineering is further addressed in [77].

4.4.4. Fault Management

The fault management functions of cSPcSPI consist of fault management functions at physical layer, L2, and L3 (if supported). These are:

- AIS and RDI for physical port failures
- Link level OAM [7]
- ENNI MEG for Service OAM [25] for L2 interface
- LAG MEG [25]
- LAG Link MEG [25]
- MPLS OAM [52]

If the interface is IP/WDM, generating notifications for Wavelength event, Port event, and Fiber event; and protection at WDM layer are part of fault management functionalities.

4.4.5.Performance Management

Service frames or packets of received, transmitted, and dropped of yellow and green colors [34,35] will be counted at cSPcSPI.

For L2 Ethernet interface, relevant performance requirements in MEF15 [18], MEF35 [27], MEF 35.0.1 [28], and MEF 35.0.2 [68] apply.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

For L3 interface, relevant performance requirements in RFC 4293 [33], RFC 2697 [35] and RFC 2698 [34] apply.

4.4.6.Link Protection

For L2 Ethernet interface, LAG/LACP can be used when there are at least two links, as described in MEF 32 [55].

For MPLS/WDM, traffic is protected either at the light_path level or at the label switched path (LSP) level based on the restoration time requirements. In light_path-level protection, traffic on a LSP is protected by routing it over primary light_paths which are protected at the optical layer by their respective backup light_paths. In LSP-level protection, the traffic on a primary LSP is protected at MPLS layer by a backup LSP. In this case, both primary and backup LSPs traverse unprotected light_paths.

4.4.7.Security

Security capabilities of cSPcSPI that are established between two cSPs:

- •Connection Authentication such as IPSec-AH
- •Packet encryption such as VPN
- •Data confidentiality and privacy such as identity and access management, or DLP at the network level
- •Service Level Security against attacks such as DDoS

4.4.8.Billing

The billing might depend on the relationship between cSPs. It is possible to have a peering relationship between cSPs such that below certain number of transactions, neither side pays anything. The side exceeding the preset limit may pay the other side based on their agreement.

5 Connections and Connection Termination Points

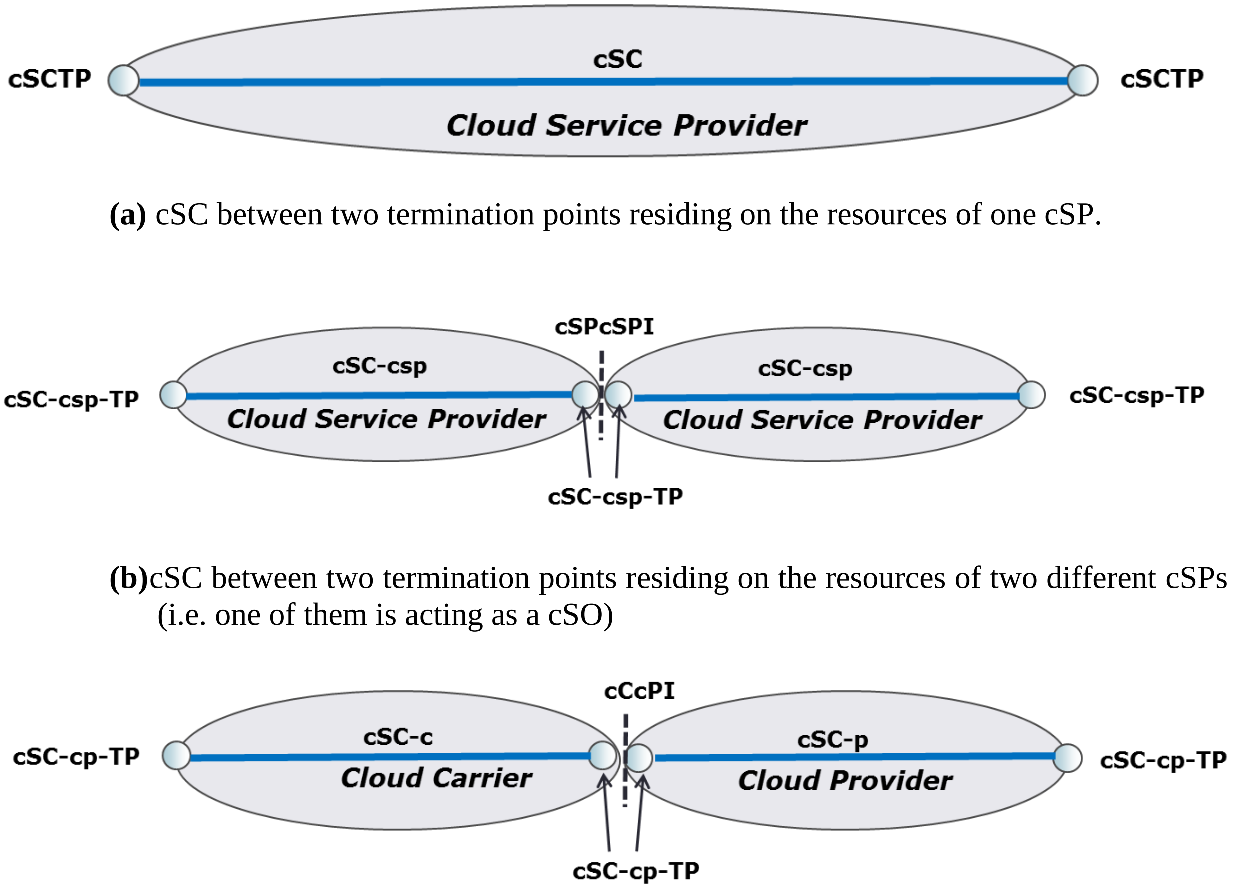
Connection and connection termination points providing cloud services are depicted in Figure 16 for a cSC crossing one or more administrative domains.

When a cSC crosses multiple cSPs, the cSC segments and their termination points in each cSP are called cSC-csp (Cloud Service Provider Connection) and Cloud Service Provider Connection Termination Point (cSC-csp-TP), respectively.

When a cSC crosses cP and cC administrative domains, the cSC segments and their termination points are called cSC-c (Cloud Carrier Connection), cSC-p (Cloud Provider Connection), and Cloud Carrier-Provider Connection Termination Point (cSC-cp-TP), respectively.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

The following sections will describe them in details.



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

(b)cSC between two termination points residing on the resources of two different cSPs (i.e. one of them is acting as a cSO)

(c) cSC between a termination point residing on cC and a termination point residing on a cP.

Figure 16: Cloud Service Connection Types

5.1Cloud Service Connection Termination Point (or End Point) (cSCTP)

The cSCTP is a termination point of a cSC when the cSC is within the boundaries of one administrative domain.

5.1.1 Attributes

The cSCTP possible attributes are listed in Table 6.

cSCTP attributes	Descriptions and Recom-

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

		mended Values of Attributes
cSCTP Id		Arbitrary text string to identify the cSCTP
cSUI Ids and cSI Ids[6]		Arbitrary string
cSC Id		
Overlay Network Attributes	Virtual Access Point (VAP) Id	
	NVE Interface Id	4 decimal digits
L2 Ethernet attributes		
MEF EVC per UNI Service attributes in Table 5 of MEF 6.2 [70]		
MEF EVC per UNI Service attributes for EPL Service in Table 8 of MEF 6.2 [70]		
MEF EVC per UNI Service attributes for EVPL Service in Table 11 of MEF 6.2 [70]		
MEF EVC per UNI Service attributes for EP-LAN Service in Table 14 of MEF 6.2 [70]		
MEF EVC per UNI Service attributes for EVP-LAN Service in Table 18 of MEF 6.2 [70]		
MEF EVC per UNI Service attributes for EP-Tree Service in Table 20 of MEF 6.2 [70]		
MEF EVC per UNI Service attributes for EVP-Tree Service in Table 23 of MEF 6.2 [70]		
MEF EPL Option 2 L2CP Processing Requirements in Table 8 of MEF 45 [69]		
MEF EPL Option 2 L2CP Processing Recommendations in Table 9 of MEF 45[69]		
Protection (via redundant cSCTP on a different physical port of the same CE or different CE at cSUI, and on a different VM at cSI)	1:1or 1+1	
L2 Ethernet SOAM attributes [25]		
Maintenance Entity Group (MEG) Id		
Maintenance End Point (MEP) Id		
MEP Level		
L3 attributes if interface is L3		
IPv4 Subnet Address		
IPv6 Subnet Address		
DSCP Mapping		
Bandwidth Profile	CIR	
	CBS	
	EIR	
	EBS	

[6] cSUI Id and cSI Ids are included to identify cSUI and cSI that cSCTP is related to. The cSUI-cSCTP and cSI-cSCTP relationships maybe represented via association in the information model instead of an attribute of the cSCTP object.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Protection (via redundant cSCTP on a different port of the same CE or different CE providing the cSUI, and on a different VM of the application entity providing cSI)	1:1or 1+1	
LSP Label		
EXP Mapping		
Operational State		Enabled or Disabled
Administrative State		Enabled or Disabled
cSCTP Level Security		
Packet encryption	IPSec ESP	
	SSL VPN	
Connection Authentication	IPSec AH	
	TCP-AO	
Data confidentiality/privacy	Logical separation of cSTPs, limiting DoS and excessive re-source consumption via rate limiting	
Service Level Security	Rate limiting of DoS attacks and excessive resource consumption	

Table 6 : cSCTP Attributes

5.1.2 Dynamic Attributes

The following attributes are likely to be configured on-demand:

- Bandwidth Profile Parameters
- CoS Category
- PCP Mapping
- DSCP Mapping
- EXP Mapping
- cSCTP Protection
- L2CP Treatment
- IP subnet addresses
- Administrative state

5.1.3 Traffic Management

Traffic management applies to service frames or packets at cSCTP. The traffic management functionalities include bandwidth profile, policing, marking and traffic shaping per connection level at this termination point.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

For Ethernet L2 cSCTP, bandwidth profile parameters and algorithms defined for an EVC in MEF 10.3 [17] and MEF 41 [67] apply.

For IP networks, DSCP marking is used to mark packets that are processed according to the network policies for admission control, prioritization, mapping into classes of Integrated Services, or combinations of these techniques. In L2 Ethernet networks, both PCP and DSCP are used for traffic prioritization and coloring.

For MPLS networks, EXP field is used for marking [50]. Traffic engineering is further addressed in [77].

5.1.4 Fault Management

The fault management functions of cSCTP consist of fault management functions at L2 and L3 (if supported). These are including:

- AIS and RDI for connection failures
- Connection level MEP and MIP for Service OAM [25] for L2 interface
- CCM events
- MPLS OAM [52]

5.1.5 Performance Management

Service frames or packets of received, transmitted, and dropped of yellow and green colors [34,35] will be counted at cSCTP. The cSCTP will generate Threshold Crossing Alerts (TCAs) for delay, jitter and loss exceeding pre-set thresholds.

For L2 Ethernet interface, relevant connection level performance requirements in MEF15 [18], MEF35 [27] and MEF 35.0.1 [28] apply.

For L3 interface, IP Flow performance requirements in RFC 7012 [54] apply.

5.1.6 Protection

Protection of cSCTP can be provided by having a back-up cSCTP on another port of the same CE or another port of a different CE providing cSUI, and on another VM of the application entity providing the cSI. Depending on configuration, the protection can be 1:1 or 1+1.

5.1.7Security

Security capabilities of cSCTP needed during the establishment of a Cloud Service Connection (cSC) are:

- cSC Connection Authentication to prevent unauthorized access between the two cSCTP endpoints such as IPSec-AH
- cSC Connection Encryption to prevent eavesdropping, interception or a man-in-the-middle attack on an existing cSC using some form of packet encryption such as VPN

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

- Data confidentiality and privacy such as identity and access management, or Data Loss Prevention (DLP) at the network level
- Service Level Security against attacks such as DDoS
- Proper Management of cSCTP once the corresponding cSC is tore down, ensuring that the cSCTP is properly cleaned up:
  - OperationalState and AdminstrativeState are set to Disabled,
  - resources are released,
  - cSCTP Id is no longer valid , and
  - there is no collusion between newly generated cSCTP Ids and old sSCTP ids. This is necessary to prevent malicious cSC from reusing old, but not reclaimed cSCTP and in so doing, compromise cSI resources.

5.2 Cloud Service Connection (cSC)

The cSC is a cross connect between two or more cSCTPs. The cSC could be an EVC, LSP or IP VPN connection.

A cSC can support accessing multiple VMs via multiple sessions as depicted in Figure 17 where a virtual switch routes traffic to destination VM.

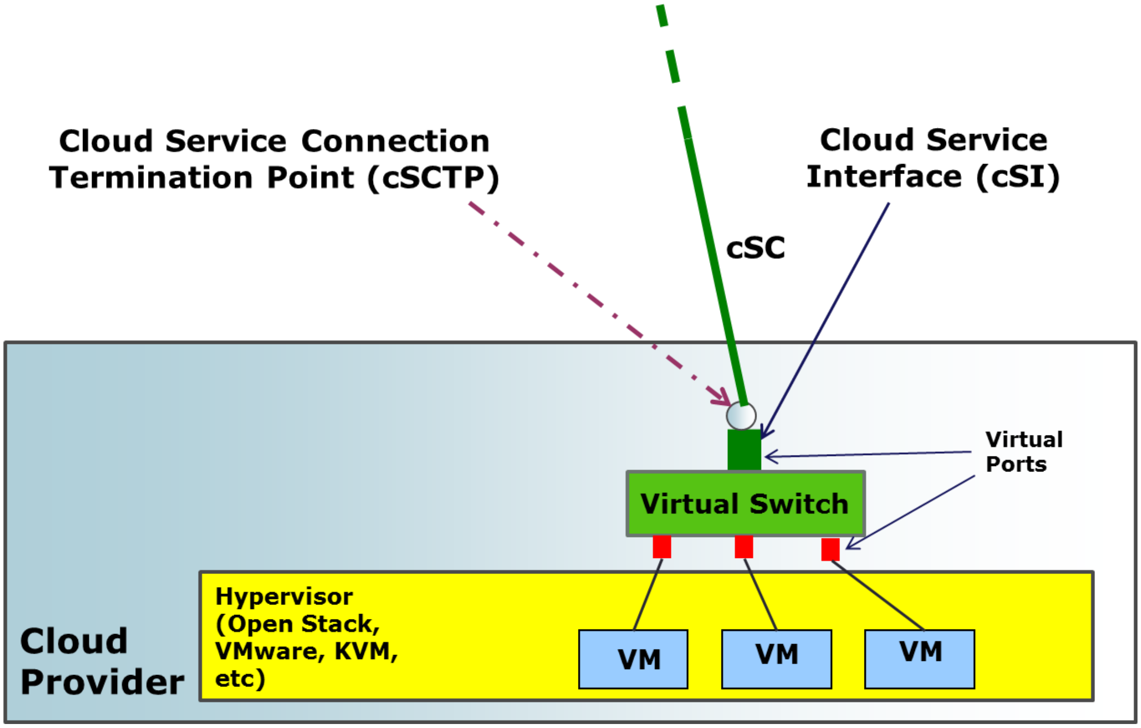

Cloud Service Connection Termination Point (cSCTP)
Cloud Service Interface (cSI)
cSC
Virtual Ports
Virtual Switch
Hypervisor (Open Stack, VMware, KVM, etc)
VM
VM
VM
Cloud Provider

Figure 17: Multiple VM sharing a cSC

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

5.2.1 Attributes

Possible attributes for the cSC are listed in Table 7.

cSC attributes		Descriptions and recommended values of attributes
cSC Id		Arbitrary text string to identify the cSC
List of associated cSCTP Ids[7]		
Overlay Network Attributes	VNI ID	
Type	Point-to-Point	
	Point-to-Multipoint	
	Multipoint-to-Multipoint	
Protection	1:1 or 1+1	cSC needs to be protected for path protection
L2 Ethernet connection attributes [71,47]		
MEF EVC Service attributes in Table 6 of MEF 6.2 [70]		
MEF EVC Service attributes of EPL in Table 9 of MEF 6.2 [70]		
MEF EVC Service attributes of EVPL in Table 12 of MEF 6.2 [70]		
MEF EVC Service attributes of EP-LAN in Table 15 of MEF 6.2 [70]		
MEF EVC Service attributes of EVP-LAN in Table 18 of MEF 6.2 [70]		
MEF EVC Service attributes of EP-Tree in Table 21 of MEF 6.2 [70]		
MEF EVC Service attributes of EVP-Tree in Table 24 of MEF 6.2 [70]		
MEF EVC Perfromance attributes and Parameters per CoS in Table 25 of MEF 6.2 [70]		
L3 connection attributes (if supported)	Service Level Objectives (SLOs)	Delay, jitter, loss
	MTU	
	Type	Point-to-Point, Multipoint-to-Multipoint, Rooted Multipoint
Connection Start Time		Specified in seconds in Coordinated Universal Time (UTC).
Connection Start Interval (Start Interval parameter to indicate the acceptable interval after the Start Time during which the service attribute modifications can be made.) [80]		Specified in seconds in UTC

[7] cSCTP Ids are included to identify termination points associated with this cSC. This cSC-cSCTP relationship may be rep-resented via association in the information model instead of an attribute of the cSC object..

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Connection Duration		Specified in days, minutes or seconds.
Connection Period		Specified in daily, weekly or monthly
Operational State		Enabled or Disabled
Administrative State		Enabled or Disabled
Billing Options	Monthly, Hourly	

Table 7: cSC Attributes

5.2.2 Dynamic Attributes

The following attributes are likely to be configured on-demand:

- List of cSCTPs
- Connection Start Time
- Connection End Time
- Administrative State
- Maximum Frame Size or MTU
- Service Level Objectives (SLOs)

5.2.3 SLOs

SLOs defined in MEF23.1 [47] apply here whether the cSC is an EVC, LSP or IP VPN connection.

5.2.4 Fault Management

CCM and Link Trace capabilities to identify L2 EVC failures, Internet Control Message Protocol (ICMP) Ping for IP VPN failures, and MPLS Ping and Traceroute for LSP failures are needed.

5.2.5 Performance Management

Periodic delay, jitter, and loss measurements are needed.

For L2 Ethernet cSC, performance management requirements in MEF 35 [25] apply.

For L3 cSC, IP Flow performance requirements in RFC 7012 [54] apply.

5.2.6 Protection

The cSC protection can be achieved via a redundant cSC following the same path or a different path. The protection can be 1:1 or 1+1.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

5.2.7 Billing

The billing may depend on the cSC bandwidth parameters and the length of the usage.

5.3Cloud Service Provider Connection Termination Point (cSC-csp-TP)

The cSC may cross multiple Cloud Service Provider domains as depicted in Figure 18. Each domain will carry a segment of the cSC. The segment in each cSP domains called cSC-csp.

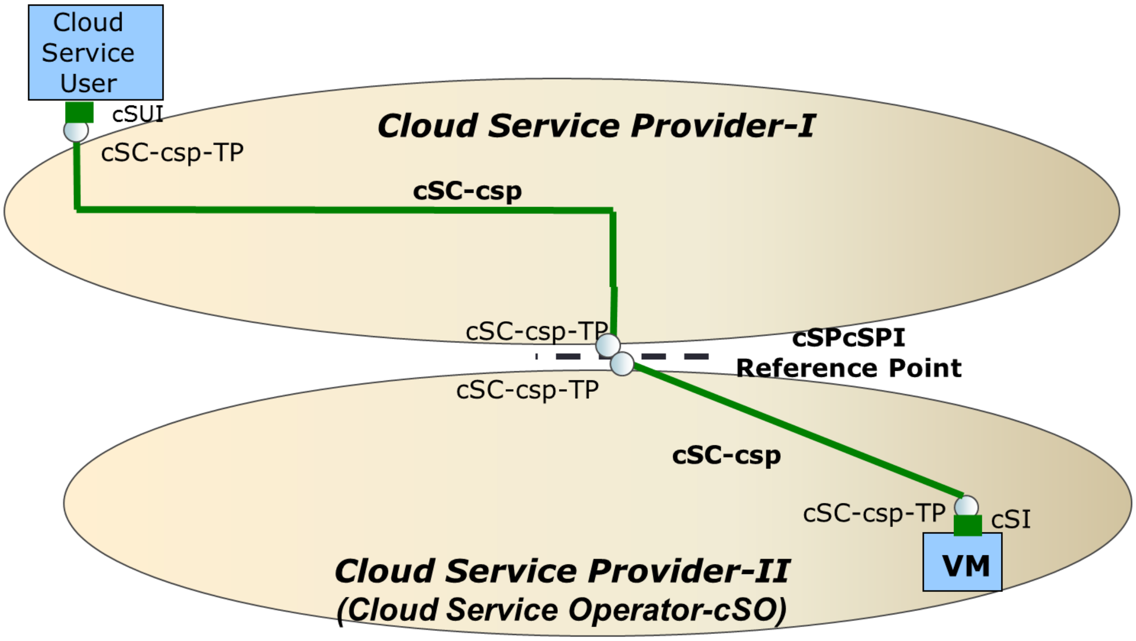


Figure 18: cSC-csp-TP, cSC-csp

The cSC-csp is between the termination point at cSUI or cSI which is cSC-csp-TP, and the termination point at cSPcSPI which is cSC-csp-TP.

For L2 Ethernet, the cSC-csp will be very similar to the Operator Virtual Connection (OVC) defined by MEF 26.1 [22]. Also the cSC-cp-TP is very similar to the OVC End Point [22].

5.3.1 Attributes

Cloud Service Provider Connection Termination Point (cSC-cp-TP) possible attributes are listed in Table 8.

cSC-cp-TP attributes	Require-mentsDescriptions and recommended values of attributes

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

cSC-csp-TP Id		Arbitrary text string to identify the cSC-csp-TP
cCScSPI Ids		
Overlay Network Attributes	Virtual Access Point (VAP) Id	
	NVE Interface Id	4 decimal digits
L2 Ethernet attributes[8]		
MEF OVC End Point per ENNI Service Attributes in Table 17 of MEF 26.1 [22]		
MEF OVC End Point per UNI Service Attributes in Table 18 of MEF 26.1 [22]		
MEF OVC L2CP Service Attributes for Access EVPL in Table 13 of MEF 45 [69]		
MEF OVC L2CP Service Attributes for Access EPL in Table 16 of MEF 45 [69]		
MEF OVC L2CP Service Attributes for UTA in Table 19 of MEF 45 [22]		
MEF OVC L2CP Service Attributes for vNID Case A in Table 24 of MEF 45 [69]		
OVC L2CP Service Attributes for vNID Case B in Table 27 of MEF 45 [22]		
Protection (via redundant cSC-csp-TP on a different port of the same cSPcSPI Gateway	1:1or 1+1	
L2 SOAM attributes [25]		
Maintenance Entity Group (MEG) Id		
Maintenance End Point (MEP) Id		
MEP Level		
Maximum Number of MEPs		
Maintenance Intermediate Point (MIP) Id		
L3 attributes if interface is L3		
IPv4 Subnet Address		
IPv6 Subnet Address		
DSCP Mapping		
Bandwidth Profile	CIR	
	CBS	
	EIR	
	EBS	
Protection (via redundant cSCTP on a different port of the same cSPcSPI Gateway	1:1or 1+1	
LSP Label		
EXP Mapping		
Operational State		Enabled or Disabled

[8] More attributes may be added after MEF OVC Services Definitions document is finalized.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Administrative State		Enabled or Disabled
Security		
Packet encryption	IPSec ESP	
	SSL VPN	
Connection Authentication	IPSec AH	
	TCP-AO	
Service Level Security	Rate limiting of DoS attacks and limiting excessive resource consumption	
Data confidentiality/privacy	Preventing eavesdropping between cSC-csp-TPs via logical separation.	

Table 8 : cSC-csp-TP Attributes

5.3.2 Dynamic Attributes

The following attributes are likely to be configured on-demand:

- Bandwidth Profile Parameters
- PCP Mapping
- DSCP Mapping
- EXP Mapping
- cSC-csp-TP Protection
- L2CP Treatment
- IP subnet addresses
- Administrative state

5.3.3 Traffic Management

Traffic management applies to service frames or packets at cSC-csp-TP. The traffic management functionalities include bandwidth profile, policing, marking and traffic shaping per connection level at this termination point.

For Ethernet L2 cSC-csp-TP, bandwidth profile parameters and algorithms defined for an EVC in MEF 10.3 [17] and MEF 41 [67] apply.

For IP networks, DSCP marking is used to mark packets that are processed according to the network policies for admission control, prioritization, mapping into classes of Integrated Services, or combinations of these techniques. In L2 Ethernet networks, both PCP and DSCP are used for traffic prioritization and coloring.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

For MPLS networks, EXP field is used for marking [50]. Traffic engineering is further addressed in [77].

5.3.4 Fault Management

The fault management functions of cSC-csp-TP consist of fault management functions at L2 and L3 (if supported). These are:

- •AIS and RDI for connection failures
- •Connection level MEP and MIP for Service OAM [25] for L2 interface
- •CCM events for L2 interface
- •MPLS OAM [52]

5.3.5 Performance Management

Service frames or packets of received, transmitted, and dropped of yellow and green colors [34,35] will be counted at cSC-csp-TP.

For L2 interface, relevant connection level performance requirements in MEF15 [18], MEF35 [27] and MEF 35.0.1 [28] apply here.

For L3 interface, relevant performance requirements in RFC 4293 [33], RFC 2697 [35] and RFC 2698 [34] apply.

5.3.6 Protection

The protection of cSC-csp-TP at cSPcSPI can be provided by having a back-up cSC-csp-TP at another port on the same cSPcSPI gateway. Depending on the configuration, the protection can be 1:1 or 1+1.

5.3.7 Security

Security capabilities of cSC-csp-TP needed during the establishment of an associated cSC segment are:

- •Connection Authentication to prevent unauthorized access or eavesdrop-ping between different cSCcpTPs such as IPSec-AH
- •cSC-csp Connection Decryption/re-Encryption if both the cSC-csp use different encryption technologies, ensuring that all segments of the cSC are encrypted to prevent eavesdropping, interception or a man-in-the-middle attack on an existing cSC using some form of packet encryption such as VPN
- •Data confidentiality and privacy such as identity and access management, or DLP at the network level
- •Service Level Security against attacks such as DDoS
- •Proper Management of cSC-csp-TPs once the corresponding cSC is tore down, ensuring that the cSCcpTPs are properly cleaned up:
  - o OperationalState and AdminstrativeState are set to Disabled,

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

o resources released,
o cSC-csp-TP Ids are no longer valid , and
o there is no collusion between newly generated cSCcpTP Ids and old sSC-csp-TP ids. This is necessary to prevent malicious cSC from reusing old, but not reclaimed cSC-csp-TP and in so doing, compromise cSPcScPI resources.

5.4 Cloud Service Provider Connection (cSC-csp)

The cSC-csp is a cross connect between two cSC-csp-TPs. The cSC-csp could be an OVC, LSP or IP VPN connection segment.

5.4.1 Attributes

The cSC-csp possible attributes are listed in Table 9.

cSC-csp attributes		Descriptions and Recommended Values of Attributes
cSC-csp Id		Arbitrary text string to identify the cSC-csp
cSC-csp-TP Ids associated with this cSC-csp		
Overlay Network Attributes	VNI ID	
Protection	1:1 or 1+1	
L2 Ethernet Connection attributes		
MEF OVC Services attributes in Table 5 of MEF 26.1 [22]		
MEF OVC CE-VLAN ID Preservation when All CE-VLAN IDs Map to the OVC at all of the UNIs Associated by the OVC in Table 6 of MEF 26.1 [22]		
MEF OVC CE-VLAN ID Preservation when not All CE-VLAN IDs Map to the OVC at all of the UNIs Associated by the OVC in Table 7 of MEF 26.1 [22]		
MEF OVC CE-VLAN ID Preservation when none of the OVC End Points are at UNIs in Table 8 of MEF 26.1 [22]		
OVC CE-VLAN CoS Preservation in Table 9 of MEF 26.1 [22]		
L3 Connection attributes		
	SLOs	Delay, jitter, loss and availability
	MTU	
	Type	Point-to-Point, Multipoint-to-Multipoint, Rooted-Multipoint
Connection Start Time		Measured in minutes
Connection End Time		Measured in minutes
Operational State		Enabled or Disabled

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Administrative State		Enabled or Disabled
Billing Options	Monthly, Hourly	

Table 9 : cSC-csp Attributes

5.4.2 Dynamic Attributes

The following attributes are likely to be configured on-demand:

- cSC-csp-TPs
- MTU or Maximum Frame Size
- CoS Category
- Connection End Time
- Administrative State
- SLOs

5.4.3 SLOs

SLO for cSC-csp needs to be defined and agreed between cSPs in order to meet the end-to-end SLOs of the given cSC.

5.4.4 Fault Management

CCM and Link Trace capabilities to identify L2 Ethernet OVC failures, Internet Control Message Proto-col (ICMP) Ping for IP VPN segment failures, and MPLS Ping and Traceroute for LSP failures are needed.

5.4.5 Protection

The cSC-csp can be protected via a back-up cSC-csp. The protection can be 1:1 or 1+1.

5.4.6 Performance Management

Periodic delay, jitter, and loss measurements are required.

For L2 Ethernet cSC-csp, performance management requirements in MEF 35 [27], MEF 35.0.1 [28], and MEF 35.0.2 [68] apply.

For L3 interface, IP Flow performance requirements in RFC 7012 [54] apply.

5.5 Cloud Carrier-Provider Connection Termination Point (cSC-cp-TP)

The cSC may cross multiple Cloud Carrier domain (s) and Cloud Provider domain (s) as depicted in Figure 19. Each domain will carry a segment of the cSC. The segment in the Cloud Carrier domain is called cSC-c. The segment in the Cloud Provider domain is called cSC-p.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

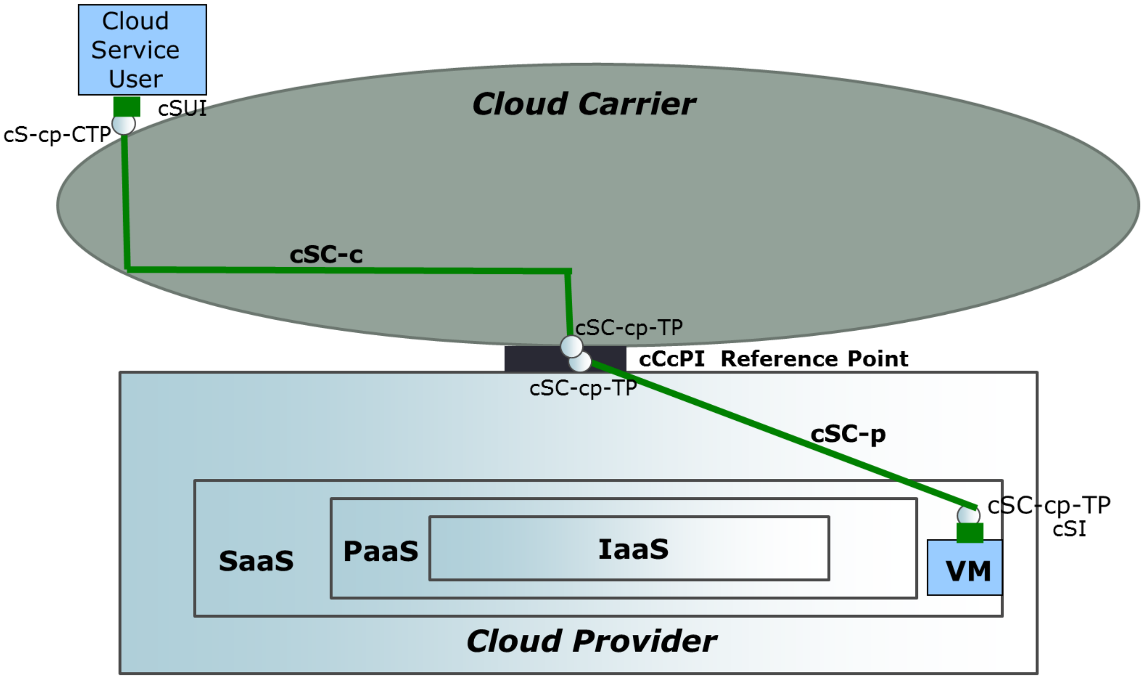


Figure 19: cSC-cp-TP, cSC-c, cSC-p

The cSC-c is between the termination point at cSUI which is cSC-cp-TP, and the termination point at cCcPI which is cSC-cp-TP. Similarly, the cSC-p is between the termination point at cSI which is cSC-cp-TP and the termination point at cCcPI which is cSC-cp-TP.

The cSC-c and cSC-p are expected to have very similar properties. For L2 Ethernet, both cSC segments will be very similar to the OVCs defined by MEF 26.1 [22]. The cSC-cp-TP is very similar to the OVC End Point for L2 Ethernet [22].

5.5.1 Attributes

Cloud Carrier-Provider Connection Termination Point (cSC-cp-TP) possible attributes are listed in Table 8.

cSC-cp-TP attributes	Descriptions and recommended values of attributes
cSC-cp-TP Id	Arbitrary text string to identify the cS-Ccp-TP
cCcPI Id[9]	
cSC-c Id	

[9] cSC Id, cSC-c Id, cSC-p Id, cCcPI Id can be associated with the cSC-cp-TP Id. They can be represented either by attributes or by associations.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

cSC-p Id		
cSC Id		
Overlay Network Attributes	Virtual Access Point (VAP) Id	
	NVE Interface Id	4 decimal digits
L2 Ethernet attributes		
MEF OVC End Point per ENNI Service Attributes in Table 17 of MEF 26.1 [22]		
MEF OVC L2CP Service Attributes for Access EVPL in Table 13 of MEF 45 [69]		
MEF OVC L2CP Service Attributes for Access EPL in Table 16 of MEF 45 [69]		
MEF OVC L2CP Service Attributes for UTA in Table 19 of MEF 45 [69]		
MEF OVC L2CP Service Attributes for vNID Case A in Table 24 of MEF 45 [69]		
OVC L2CP Service Attributes for vNID Case B in Table 27 of MEF 45 [69]		
Protection (via redundant cSC-cp-TP on a different port of the same CCcPI gateway	1:1or 1+1	
L2 SOAM attributes [25]		
Maintenance Entity Group (MEG) Id		
Maintenance End Point (MEP) Id		
MEP Level		
Maximum Number of MEPs		
Maintenance Intermediate Point (MIP) Id		
L3 attributes if interface is L3		
IPv4 Subnet Address		
IPv6 Subnet Address		
DSCP Mapping		
Bandwidth Profile	CIR	
	CBS	
	EIR	
	EBS	
Protection (via redundant cSC-cp-TP on a different port of the cCcPI gateway)	1:1or 1+1	
LSP Label		
EXP Mapping		
Operational State		Enabled or Disabled
Administrative State		Enabled or Disabled
Security		
Packet encryption	IPSec ESP	
	SSL VPN	

Connection Authentication	IPSec AH	
	TCP-AO	
Service Level Security	Rate limiting of DoS attacks and excessive resource consumption	
Data confidentiality/privacy	Prevent eavesdropping between cSC-cp-TPs via logical separation.	

Table 10 : cSC-cp-TP Attributes

5.5.2 Dynamic Attributes

The following attributes are likely to be configured on-demand:

- Bandwidth Profile Parameters
- PCP Mapping
- DSCP Mapping
- EXP Mapping
- cSC-cp-TP Protection
- L2CP Treatment
- IP subnet addresses
- Administrative state

5.5.3 Traffic Management

Traffic management applies to service frames or packets at cSC-cp-TP supporting L2 and above. The traffic management functionalities include bandwidth profile, policing, marking and traffic shaping per connection level at this termination point.

For Ethernet L2 cSC-cp-TP, bandwidth profile parameters and algorithms defined for an EVC in MEF 10.3 [17] and MEF 41 [67] apply.

For IP networks, DSCP marking is used to mark packets that are processed according to the network policies for admission control, prioritization, mapping into classes of Integrated Services, or combinations of these techniques. In L2 Ethernet networks, both PCP and DSCP are used for traffic prioritization and coloring.

For MPLS networks, EXP field is used for marking [50]. Traffic engineering is further addressed in [77].

5.5.4 Fault Management

The fault management functions of cSC-cp-TP consist of fault management functions at L2 and L3 (if supported). These are:

- •AIS and RDI for connection failures
- •Connection level MEP and MIP for Service OAM [25] for L2 interface
- •CCM events for L2 interface
- •MPLS OAM [52]

5.5.5 Performance Management

Service frames or packets of received, transmitted, and dropped of yellow and green colors [34,35] will be counted at cSC-cp-TP.

For L2 Ethernet interface, relevant connection level performance requirements in MEF15 [18], MEF35 [27] and MEF 35.0.1 [28] apply.

5.5.6 Protection

The protection of cSC-cp-TP at cCcPI can be provided by having a back-up cSC-cp-TP at another port on the same cCcPI gateway. Depending on configuration, the protection can be 1:1 or 1+1.

For L3 interface, relevant performance requirements in RFC 4293 [33], RFC 2697 [35] and RFC 2698 [34] apply.

5.5.7 Security

Security capabilities of cSC-cp-TP needed during the establishment of an associated cSC segment are:

- •Connection Authentication to prevent unauthorized access or eavesdrop-ping between different cSC-cp-TPs such as IPSec-AH
- •cSC-c to cSC-p Connection Decryption/re-Encryption if both the cSC-c and cSC-p use different encryption technologies, ensuring that all segments of the cSC are encrypted to prevent eavesdropping, interception or a man-in-the-middle attack on an existing cSC using some form of packet encryption such as VPN
- •Data confidentiality and privacy such as identity and access management, or DLP at the network level
- •Service Level Security against attacks such as DDoS
- •Proper Management of cSCcpTPs once the corresponding cSC is tore down, ensuring that the cSC-cp-TP are properly cleaned up:
  - o OperationalState and AdminstrativeState are set to Disabled,
  - o resources released,
  - o cSC-cp-TP Ids are no longer valid, and
  - o there is no collusion between newly generated cSC-cp-TP Ids and old cSC-cp-TP ids. This is necessary to prevent malicious cSC from reusing old, but not reclaimed cSC-cp-TP and in so doing, compromise cCcPI resources.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

5.6 Cloud Carrier Connection (cSC-c)

cSC-c is a cross connect between two cSC-cp-TPs of a Cloud Carrier. cSC-c could be an OVC, LSP or IP VPN connection segment.

5.6.1 Attributes

The cSC-c possible attributes are listed in Table 11.

cSC-c attributes		Definition and Requirements
cSC-c Id		Arbitrary text string to identify the cSC-c
cSC-cp-TP Ids associated with this cSC-c		
Overlay Network Attributes	VNI ID	
Protection	1:1 or 1+1	
L2 Ethernet Connection attributes		
MEF OVC Services attributes in Table 5 of MEF 26.1 [22]		
MEF OVC CE-VLAN ID Preservation when All CE-VLAN IDs Map to the OVC at all of the UNIs Associated by the OVC in Table 6 of MEF 26.1 [22]		
MEF OVC CE-VLAN ID Preservation when not All CE-VLAN IDs Map to the OVC at all of the UNIs Associated by the OVC in Table 7 of MEF 26.1 [22]		
MEF OVC CE-VLAN ID Preservation when none of the OVC End Points are at UNIs in Table 8 of MEF 26.1 [22]		
OVC CE-VLAN CoS Preservation in Table 9 of MEF 26.1 [22]		
L3 Connection attributes		
	SLOs	
	MTU	
	Type	Point-to-Point, Multipoint-to-Multipoint, Rooted-Multipoint
Connection Start Time		Measured in minutes
Connection End Time		Measured in minutes
Operational State		Enabled or Disabled
Administrative State		Enabled or Disabled
Billing Options	Monthly, Hourly	

Table 11 : cSC-c Attributes

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

5.6.2 Dynamic Attributes

The following attributes are likely to be configured on-demand:

- cSC-cp-TP
- CoS category
- Connection Start Time
- Connection End Time
- Administrative State
- SLOs
- MTU or Maximum Frame Size

5.6.3 SLOs

SLO for cSC-c needs to be defined between the cSP and the cC in order to meet end-to-end SLOs of the given cSC.

5.6.4 Fault Management

CCM and Link Trace capabilities to identify L2 Ethernet OVC failures, Internet Control Message Protocol (ICMP) Ping for IP VPN segment failures, and MPLS Ping and Traceroute for LSP failures are needed.

5.6.5 Performance Management

Periodic delay, jitter, and loss measurements are required.

For L2 Ethernet cSC-c, performance management requirements in MEF 35 [25] and MEF 35.0.1 [28] apply.

For L3 interface, IP Flow performance requirements in RFC 7012 [54] apply.

5.6.6 Protection

The cSC-c can be protected via a back-up cSC-c. The protection can be 1:1 or 1+1.

5.6.7 Billing

The billing may depend on the cSC-c bandwidth parameters and the length of the usage.

5.7 Cloud Provider Connection (cSC-p)

The cSC-p is a cross-connect between two cSC-cp-TPs of a Cloud Provider. The cSC-p could be an OVC, LSP or IP VPN connection segment.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

There may be no difference between attributes of cSC-p and cSC-c, other than their Ids. In order to have flexibility in the architecture, a different object is created.

5.7.1 Attributes

The cSC-p possible attributes are listed in Table 12.

cSC-p attributes		Definition and Requirements
cSC-p Id		Arbitrary text string to identify the cSC-c
cSC-cp-TP Ids associated with this cSC-p		
Overlay Network Attributes	VNI ID	
Protection	1:1 or 1+1	
L2 Ethernet Connection attributes		
MEF OVC Services attributes in Table 5 of MEF 26.1 [22]		
MEF OVC CE-VLAN ID Preservation when All CE-VLAN IDs Map to the OVC at all of the UNIs Associated by the OVC in Table 6 of MEF 26.1 [22]		
MEF OVC CE-VLAN ID Preservation when not All CE-VLAN IDs Map to the OVC at all of the UNIs Associated by the OVC in Table 7 of MEF 26.1 [22]		
MEF OVC CE-VLAN ID Preservation when none of the OVC End Points are at UNIs in Table 8 of MEF 26.1 [22]		
OVC CE-VLAN CoS Preservation in Table 9 of MEF 26.1 [22]		
L3 Connection attributes		
	SLOs	
	MTU	
	Type	Point-to-Point, Multipoint-to-Multipoint, Rooted-Multipoint
Connection Start Time		Measured in minutes
Connection End Time		Measured in minutes
Operational State		Enabled or Disabled
Administrative State		Enabled or Disabled
Billing Options	Monthly, Hourly	

Table 12 : cSC-p Attributes

5.7.2 Dynamic Attributes

The following attributes are likely to be configured on-demand:

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

•cSC-cp-TP
•CoS category
•Connection Start Time
•Connection End Time
•Administrative State
SLOs
MTU or Maximum Frame Size

5.7.3 SLOs

The SLO for a cSC-p needs to be defined and agreed between the cSP and the cP in order to meet the end-to-end SLOs of the given cSC.

5.7.4 Fault Management

CCM and Link Trace capabilities to identify L2 OVC failures, Internet Control Message Protocol (ICMP) Ping for IP VPN segment failures, and MPLS Ping and Traceroute for LSP failures are needed.

5.7.5 Protection

The cSC-p can be protected via a back-up cSC-p. The protection can be 1:1 or 1+1.

5.7.6 Performance Management

Periodic delay, jitter, and loss measurements are required.

For L2 Ethernet cSC-p, performance management requirements in MEF 35 [25], MEF 35.0.1 [28], and MEF 35.0.2 [68] apply.

For L3 interface, IP Flow performance requirements in RFC 7012 [54] apply.

6 Cloud Services

So far we have described entities and their requirements to support connectivity for cloud applications. This section describes Cloud Services and their possible attributes.

A cloud service can include application entities, cSC and associated resources, as well as just the application or just the connection.   For example, the connectivity service depicted in Figure 8 is a Cloud Service. Similarly, computing applications, computing resources and virtual network depicted in Figures 12, 13 and 14 collectively can form a Cloud Computing service or just the computing applications together with computing resources form a cloud service.

When a Cloud Service is an end-to-end service between external interfaces (i.e. cSUI, cSI, cCPI, cSPcSPI), it can include non-cloud and cloud resources or all cloud resources. For example, a

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

user may use non-cloud based NaaS or cloud based NaaS to access cloud computing applications. The cSP coordinates all resources acting as the single point of contact and provides a bill to the cloud user.

The services are grouped under NaaS, IaaS, PaaS, SaaS, CaaS and SECaaS for now. Given there is no consensus among various Standards Developing Organizations (SDOs) and Cloud Service Providers regarding to which service belongs to which service category, we will make an attempt to group services with similar characteristics. However, the grouping will have no effect on the requirements related to each service.

For example,

- Server, desktop, database and VLAN can be categorized as IaaS
- Development environment and test environment can be categorized as PaaS
- Business, consumer, network and communication applications can be categorized as SaaS and
- Virtual PBX, audio and video conferencing and telepresence can be categorized as CaaS

The characteristics and parameters of the cloud resources can be:

- Type of resources: CPU, memory, hard disk space, bandwidth
- Amount of resources
- Nature of the resources: dedicated, shared
- Timing of resources: scheduled or on-demand
- Duration of resources

The cSP negotiates the contract and monitors its realization in real-time. The monitoring encompasses the SLO contract definition, the SLO negotiation, the SLO monitoring, and the SLO enforcement. The contract may include price reductions and discounts that are applied when a cSP fails to meet the desired service parameters or does not fulfill an agreement. The resource usage may be tracked to align them with the billing rules agreed in the SLOs.

cSP provides a set of security services and mechanisms (e.g. IP address filtering, firewall, message integrity and confidentiality, private key encryption, dynamic session key encryption, user authentication and Service certification) to protect Cloud Services data and their operating environment from unauthorized use, policy/operation violation and intrusion.

Security requirements may include:

- Licensing: If a service uses a component that is licensed by CPU and a user deploys it in a cloud environment designed to launch new instances and request more resources as load increases, the user could easily exceed the CPU license limit. The user needs to know how its licenses affect its ability to scale.
- Processing requirements and memory locks: If the application is designed with multi-threaded code that allows processing to be split into small chunks, it is well-suited for use within the cloud. On the other hand, an application that is designed around single

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

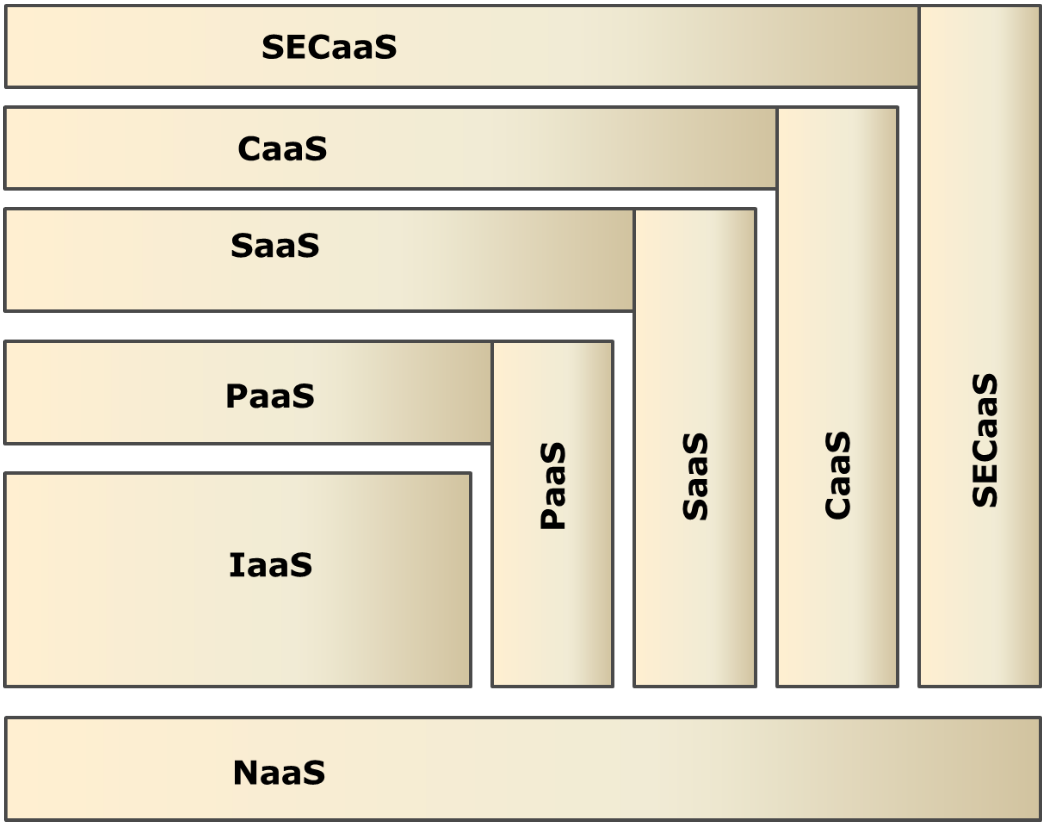
monolithic thread processing may not be able to take advantage of the distributed nature of the cloud.

- Communication protocol: Security mechanisms at the IP layer and lower layers below can protect the security of the transmitted data.
- Data Security: The service needs to provide security at the data storage, processing and transmission stages. . Data in transit needs to be protected either at the application or the transmission level. Most services choose Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols for protection at the transmission level. Server-to-server communications need to ensure the security from one cloud instance to another cloud instance.

In addition, the following features are likely to be offered by the Cloud Services;

- Committed or pay-as-you-go billing options
- Optional virtual machine management support
- Self-provisioning of server images and storage resources
- Multiple access methods for controlling user resources
- Built-in security and redundancy
- Virtualized infrastructure round-the-clock monitoring (24x7x365)

As depicted in Figure 20, it is possible to build 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, CaaS and SECaaS.



© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Figure 20: Possible hierarchy for building Cloud services

6.1 Attributes

Possible attributes that are likely to be common for Cloud Services are listed below.

Cloud Services		Descriptions and Recommended values of attributes
Resource	Virtual	Yes or No
	Physical	Yes or No
Network (i.e. NaaS)	Service Name	
	Bandwidth	
	Scheduled	
	Shared	
	Dedicated	
	On-Demand	
	Duration of Resource	
	IPv4/IPv6 Address, VLAN and MAC Filtering	
	NAT	
	Firewall	
	User Authentication	
	Encryption	
	Dynamic Scalability	
	Billing	
Infrastructure (i.e. IaaS)	Service Name	
	CPU	
	Memory	
	Hard Disk Space	
	Dedicated	
	Shared	
	Scheduled	
	On-Demand	
	Duration of Resource	
	Operating Systems	
	User Authentication	
	Encryption	
	Data Security	
	Dynamic Scalability	
	NaaS attributes	
	Billing	
Platform (i.e. PaaS)	Service Name	

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	CPU	
	Memory	
	Hard Disk Space	
	Dedicated	
	Shared	
	Scheduled	
	On-Demand	
	Duration of Resource	
	Operating Systems	
	User Authentication	
	Encryption	
	Dynamic Scalability	
	Data Security	
	NaaS attributes	
	Billing	
Software Service (SaaS)	Service Name	
	Licensing	
	On-demand Software Installation	
	NaaaS Attributes	
Communications (i.e. CaaS)	Service Name	
	Number of users	
	Licensed	
	Unlicensed	
	SLAs	
	Service Type	
	Data Security	
	Authentication Realm	
	NaaS attributes	
	Billing	
Security (i.e. SECaaS)	Security Service Type[10]	
	Security function[11]	
	Billing	

Table 13 : Common Attributes for Cloud Services

6.2 NaaS

Network as a Service (NaaS) delivers assured, dynamic connectivity services via virtual, or physical and virtual service endpoints orchestrated over multiple operators' networks. Such ser-

[10] •Security Service Types are the application of functions to those objects to be secured, such as Infrastructure security that might include physical surveillance, Network Security that might include firewall function, and Data Security that might include encryption function.

[11] •Security functions are the software/hardware implementation of security measures, such as DDoS prevention, firewall and encryption.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

vices will 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[12].

NaaS characteristics can be summarized as;

- On-demand network configuration: cSP provides the network capability, which can be configured on demand by a cloud service user (cSU)
- Secure connectivity: cSP provides secure connectivity
- QoS-guaranteed connectivity: cSP provides connectivity according to the negotiated SLO
- Heterogeneous networks compatibility: Connectivity is supported through heterogeneous networks

It is the responsibility of NaaS provider, cSP, to maintain and manage the network resources. It is possible that cSP may not own NaaS, but provides coordination. NaaS offers network as a utility.

Possible NaaS services are;

- Load Balancing where each of the following option costs differently per month
  - Local: Balancing traffic among two or more servers in the same location where servers are added and removed in real-time within 50 msec
  - Global: Balancing traffic over a geographical region consisting of multiple locations where servers are added and removed in real-time within 50 msec.
  - High Availability Load Balancers: Load balancers are available with fail-over protection and automatic fallback.
- Application Performance Services to remove the roadblocks in the network to efficiently and securely deliver applications
- Domain Registration Services
  - Register or Transfer a domain name
  - Full Domain Name System(DNS) control
  - URL Forwarding
  - Email Forwarding
  - .COM
  - .NET
  - .ORG
  - .US
  - .INFO
- Geographically Redundant DNS
- Managed DNS: Anycast DNS at Unicast DNS, Failover DNS, Backup Mail Spooling, Outbound Simple Mail Transfer Protocol (SMTP)
- Enterprise DNS: High performance, 24x7 support and 100% DNS Uptime.
- Network Appliances: Hardware and software solutions to serve as routers, firewalls, VPN devices, and load balancers. Firewalls can;
  - protect individual servers with hardware firewalls provisioned on-demand;

[12] This NaaS description is the same as the NaaS description in [74].

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

    - ○protect multiple or all servers that share the same VLAN with a dedicated, hardware firewall;
    - ○ be high availability firewall, and or
    - ○ be advance firewall with security and redundancy
- Dual-Stack IPv4 and IPv6 Capable
- Network Link Upgrade
- Outbound Public Bandwidth depending on server size
- Inbound Public Bandwidth which is usually unlimited
- Private Network Bandwidth that is usually unlimited
- Public and Private Network Ports (100 Mbps -10Gbps)
- Security
    - 24x7 Onsite Security
    - Proximity and Biometric Access Control
    - Digital Security Video Surveillance

When dealing with a disaster, it is very likely that a user will have to modify network settings as the user is failing over to another site.

NaaS needs to be highly available and scalable DNS web service. It must be designed to give developers and businesses an extremely reliable and cost-effective way to route end users to their applications.

IP addresses can be dynamic such that they are static IP addresses designed for dynamic cloud computing. Unlike traditional static IP addresses, dynamic IP addresses enable users to mask instance or zone failures by programmatically remapping user public IP addresses to instances in a user account in a particular region. For Disaster Recovery (DR), a user can also pre-allocate some IP addresses for the most critical systems so that their IP addresses are already known before disaster strikes. This can simplify the execution of the DR plan.

DynamicLoad Balancing automatically distributes incoming application traffic across multiple cSP service instances. It enables users to achieve even greater fault tolerance in user applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. Just as users can pre-allocate dynamic IP addresses, users can pre-allocate a Dynamic Load Balancer so that its DNS name is already known, which can simplify the execution of user DR plan.

NaaS can provide methods for users to provision cSP resources in a cloud virtual network that the user defines. The users have complete control over their virtual networking environments, including selection of user owned IP address ranges, creation of subnets, and configuration of route tables and network gateways. This would enable users to create a VPN connection between the users' corporate datacenter and their cloud virtual network and leverage the cSP as an extension of the corporate datacenter. In the context of DR, users can use this virtual network to extend their existing network topology to the cloud.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

6.2.1 Attributes

Possible attributes of NaaS Cloud Services are listed below. Additional attributes are also listed in the following sections.

NaaS Attributes		Descriptions and Recommended Values of Attributes
Service Name		NaaS
Service Type		
EPL[13]	On-demand with SLOs	
EVPL	On-demand with SLOs	
EP-LAN	On-demand with SLOs	
EVP-LAN	On-demand with SLOs	
EP-Tree	On-demand with SLOs	
EVP-Tree	On-demand with SLOs	
E-Access [21,58]		
IPv4 VPN		
IPv6 VPN		
Label-Only-Inferred-PSC (Per Hop Behavior Scheduling Class) LSPs (L-LSP) [79]		
EXP-Inferred-PSC LSPs (E-LSP) [79]		
Load Balancing (on-demand)		
	Local	
	Global	
	High Availability Load Balancing	
Dynamic Load Balancing (LB)	DLB automatically distributes incoming application traffic across multiple cSP service instances. User can pre-allocate user Dynamic Load Balancer so that its DNS name is already known, which can simplify the execution	

[13] If NaaS is an EPL, EVPL, EP-LAN, EVP-LAN, EP-Tree, or EVP Tree, then attributes recommended for interfaces, termination points, and connections associated with these services in section 5 apply.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	of the DR.	
Domain Registration Service	.COM	
	.NET	
	.ORG	
	.US	
	.INFO	
	Register or Transfer a domain name	
	Full DNS control	
	URL Forwarding	
	Email Forwarding	
Managed DNS	Unicast DNS	
	Anycast DNS	
	Failover DNS	
	Enterprise DNS requiring high performance, 24x7 support and 100% DNS Uptime	
	Geographically Redundant DNS	
	Backup Mail Spooling	
	Outbound SMTP	
Network Appliances	Firewalls	
	Routers	
	VPN Device	
IPv4 and IPv6 Capable Dual Stack		
Outbound Public Bandwidth		
Inbound Public Bandwidth		
Server-to-Server Bandwidth		
Upgradable Private Network Port		100Mbps-10Gbps
Upgradable Public Network Port		100Mbps-10Gbps
Dynamic IP Addresses	Dynamic IP addresses enable masking instance or Availability Zone failures by programmatically remapping user public IP addresses to instances in user account in a particular region. For Disaster Recovery (DR), some IP addresses can be pre-allocated for the most critical systems so that their IP addresses are already known before	

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	disaster strikes.	
Overlay Network Services		
PBB/PBT[75]	Pt-Pt	
	Pt-Mpt	
	Mpt-Mpt	
VXLAN [37]	List of Virtual Tunnel End Points (VTEPs)	
Security	24x7 Onsite Security	
	Proximity and Biometric Access Control	
	Digital Security Video Surveillance	

Table 14 : NaaS Cloud Service Attributes

6.3 IaaS

The capability provided to the consumer [2] 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, IaaS cP configures, deploys and maintains computing, storage and networking resources to user. Also, 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.

A Customer Portal is could be provided to access the infrastructure. An API is needed to reduce human intervention for system management and total cost of operation.

6.3.1 Cloud Computing

Cloud Computing is being able to provision computing and storage resources on-demand, specifically storage and virtual servers that IT can access on demand. IT can create virtual datacenters from commodity servers, enabling IT to stitch together memory, I/O, storage, and computational capacity as a virtualized resource pool available over the network.

Servers are the key elements of cloud computing [43]. They can be:

- Bare Metal Servers (single processor, dual processor, or quad processor)
- High Performance Computing

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

- Mass Storage Servers storing large amounts of data in solid state disks, hard disks, optical disks, or tapes
- Dedicated Rack
- Virtual Servers: They can be deployed on multi-tenant or single-tenant hosts as local or SAN storage. Portable storage can be added. Payment could be by the hour or month. Integration and migration between bare metal and virtual can be performed. Users can customize their server configuration of computing cores, RAM, and storage, on host servers without oversubscription.
    - Cores (1-8 virtual CPUs)
    - RAM in GB
    - Storage in GB
    - Disk I/O up to ~35,000 4K random read input/output operations per second (IOPS) and ~35,000 4K random write IOPS
- Redundant access links to servers

Hardware selection and upgrade are common features of cloud computing. They are:

- RAM Upgrade/ month
- Local Disk Upgrade
- Drives (SCSI, SATA Hard Drive, Solid State Drives (SSD),   )
- HW Controller
- Redundant Power Supplies

The core of Cloud Computing services is flexible compute, storage and network capacity, which can be adjusted up or down based on user demand. Within minutes, a user can create computing instances, which are virtual machines over which the user has complete control [42]. In the context of DR, this ability to rapidly create virtual machines that a user can control is critical.

Machine Images (MIs) can be preconfigured with operating systems and some application stacks. A user can also configure his/her own MIs. In the context of DR, a user should own his/her MIs configured and identified so that they can be launched as part of the recovery procedure. Such MIs should be preconfigured with the operating system of choice plus appropriate pieces of the application stack.

Reserved instances are especially relevant to DR and help to ensure that the capacity is available to user when required.

Availability Zones are distinct locations that are engineered to be insulated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same region. By launching instances in separate Availability Zones, a user can protect his/her applications from the failure of a single location. Regions consist of one or more Availability Zones.

VM Import feature enables user to import virtual machine images from user’s existing environment to Cloud Provider instances.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Compute as a service may get quick, secure access to virtual infrastructure, servers and storage without costs, time and installation requirements of adding physical hardware. Unlimited computing capacity can be offered while a user provides and manages the operating system, database and application. To manage the service, a user can choose either Graphical User Interface (GUI) or Application Programming Interfaces (APIs). There may be no upfront fees or term commitments. The user pays only for what she/he uses. The service may include the following:

- Portal Interface and API,
- Built-in security features, and
- Choice of operating system templates such as Windows or Linux.

Each customer may be limited to a number of VMs, for example 100 VMs, where VMs may be grouped into one or more Virtual Data Centers (VDCs), each with an individual firewall policy.

Once a user provisions computing resources, the user can scale infrastructure on demand by adding more resources where and when needed. When the flood of activity is over, the user can reduce capacity using a web portal.

Video applications may have variable volume or demand additional provisions for security and reliability. A user can go online and turn up server capacity for its video generation software in minutes on demand.

6.3.1.1 Attributes

Possible attributes for the Cloud Computing Services are listed below.

Cloud Computing Services		Descriptions and Recommended values of attributes
Service Name		Cloud Computing
Servers	Dedicated rack	
	Bare metal servers	Single processor, dual processors, quad processors, …
	High Performance Computing, with protected SSD storage	
	Mass Storage Servers in GB or TB	floppy disks, hard disks, optical disks, or tapes
	Redundant Power Supplies	
	RAM in GB	
	Number of VMs supported	
Virtual Servers	Single-tenant host	
	Multi-tenant host	
	Cores	1,2,3,4,5,6,7,8,..vCPU
	RAM in GB	

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	Storage in GB	SAN storage, local storage, portable storage
	Disk I/O	Number of random read&write IOPS
	Storage location	
	VM Mobility for importing VMs in user environment to cP environment.	
	Number of VMs supported per VDC	
	Number of VDCs	
	Time Interval to create a VM	
	Time Interval to move a VM	
Operating System Templates to create operating system instances on virtual servers		
Maximum Data Transfer	Per Month	GB or TB
	Per Day	GB or TB
Network Bandwidth	Inbound	
	Outbound	
HW Upgrade	RAM	
	Local Disk	
	Drives	SCSI, SATA, …
	HW Controller	
	Power Supplies	
Security	Firewall	
SLO	Delay	
	Jitter	
	Loss	
	Availability	
NaaS attributes		

Table 15 : Cloud Computing Services Attributes

6.3.2 Storage Services

Storage Services can be

- Simple Storage Service providing highly durable storage infrastructure designed for mission-critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities within a region;
- Dynamic Block Store Service (DBS) [64] providing the ability to create point-in-time snapshots of data volumes. Such snapshots can be used as the starting point for new DBS volumes, and to protect data for long-term durability. Once a volume is created, it can then be

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

attached to a running service instance. DBS Volumes provide off-instance storage that persists independently from the life of an instance;
•Import/Export Service for moving of large amounts of data into and out of a Cloud Provider (cP) using portable storage devices for transport. The cP transfers user data directly onto and off of storage devices by using NaaS. For data sets of significant size, Import/Export could be often faster than Internet transfer and more cost effective than upgrading connectivity. Users can use Import/Export to migrate data into and out of buckets or into DBS snapshots.

A cP may employ a storage gateway enabling seamless migration of data to and from between cloud storage and on-premises applications. The storage gateway stores volume data locally in the user's infrastructure and in cP. This enables existing on-premises applications to seamlessly store data in the cost-effective, secure, and durable storage infrastructure while preserving low-latency access to this data.

The storage options can be:

- **Memory** to provide rapid access to data such as file caches, object caches, in-memory databases, and RAM disks.

- **Message Queues** to provide temporary durable storage for data sent asynchronously between computer systems or application components.

- **Storage area network (SAN)**—Block devices (virtual disk logical unit numbers) on dedicated SANs providing the highest level of disk performance and durability for both business-critical file data and database storage. It can be used like a physical hard drive, typically by formatting it with the file system of user choice and using the file I/O interface provided by the instance operating system.

- **Direct-attached storage (DAS)**—Local hard disk drives or arrays residing in each server providing higher performance than a SAN, but lower durability for temporary and persistent files, database storage, and operating system (OS) boot storage than a SAN.

- **Network attached storage (NAS)** providing a file-level interface to storage that can be shared across multiple systems. NAS tends to be slower than either SAN or DAS.

- **Databases** such as a traditional SQL relational database, a NoSQL non-relational database, or a data warehouse where the underlying database storage typically resides on SAN or DAS devices, or in some cases in memory.

- **Backup and Archive** for data retained for backup and archival purposes which are typically stored on non-disk media such as tapes or optical media, which are usually stored off-site in remote secure locations for disaster recovery. There could be a limit on single archive and total amount of data in GBytes, Terabytes or Petabytes.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

- **Durable[14] Reduced Availability (DRA) storage buckets** [64] can be introduced to have lower costs and lower availability, but are designed to have the same durability as Simple Storage buckets.

DRA storage is appropriate for applications that are particularly cost-sensitive, or for which some unavailability is acceptable. For example:

- Data backup where high durability is critical, but the highest availability is not required and
- Batch jobs to recover from unavailable data, for example by keeping track of the last object that was processed and resuming from that point upon re-starting.

Cloud storage allows users to enable DRA at the bucket level. User can specify DRA storage at the time of bucket creation.

If a user wants to move data from a Simple Storage to a Durable Reduced Availability Storage bucket, the user needs to download the data from the Simple Storage bucket to his/her computer and then upload it to the Durable Reduced Availability bucket.

A cP can provide a highly durable storage infrastructure designed for mission-critical and primary data storage where objects are redundantly stored on multiple devices across multiple facilities within a region.

6.3.2.1 Attributes

Possible attributes for Cloud Storage Services are listed below.

Storage Services		Descriptions and Recommended values of attributes
Service Name		Storage Service
Simple Storage	Memory	In GBytes
	Message Queues	
	SAN	
	DAS	
	NAS	
	Database Type	SQL or non-SQL
	Backup and Archive	
Dynamic Block Storage	Memory	In GBytes
	Message Queues	
	SAN	
	DAS	

[14] Durability measures the length of a product's life. When the product can be repaired, estimating durability is more complicated. The item will be used until it is no longer economical to operate it. This happens when the repair rate and the associated costs increase significantly.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	NAS	
	Database Type	SQL or non-SQL
Import/Export	SAN	
	DAS	
	NAS	
	Backup an Archive	Single archive in in GB, TB, Petabytes, or DRA buckets
NaaS attributes		
Availability		
Billing	Memory size	
	Storage size	
	Database type	SQL or non-SQL
	Backup	
	Length of usage	
NaaS attributes		

Table 16 : Storage Service Attributes

6.3.3 Databases

A database service can be set up, operated, and scaled a relational database (RDS) in the cloud. RDS can be used either in the preparation phase for DR to hold critical data in a running database already, and/or in the recovery phase to run the production database.

A simple database can be a highly available, flexible, non-relational data store that offloads the work of database administration. It can also be used in the preparation and the recovery phase of DR. Users can also install and run their choice of database software on cP and can choose from a variety of leading database systems.

Deployment automation, post-startup software installation/configuration processes, and tools can be used in the cP domain. This can be helpful in the recovery phase to create the required set of resources in an automated fashion.

Database Cloud Services may be described as:

- Dedicated database instances with a cP database software
- Full administrative access via SSH, SQL Developer, Datapump, SQL*Plus and other tools
- Network Access using any type of network connectivity, including SQL*Net, JDBC, and other drivers to access user dedicated instances.
- Choice of database storage in GB or TB such as 5GB, 10GB, 20GB, 50GB, 1TB, etc.
- Software development environment running on an Oracle database such as Oracle Application Express (APEX) [77]
- Data access using RESTful Web Services
- Simple Database with no SQL*Net access or administrative control

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

The Database cloud services may be categorized as Basic, Managed or Premium:

- Basic:
  - Preconfigured database software
  - Managed by customer
  - Full administrative access
- Managed:
  - Basic management by cP
  - Automated backup
  - Point-in-time recovery available
  - Administrative access
- Premium Managed:
  - Managed offering above
  - Optional Data Guard or Active Data Guard
  - Pluggable database utility services
  - Flexible upgrade options

The Basic service level is customer managed. Managed and Premium Managed are managed by the cP providing full customer access. Resources are Dynamic such that the user can add or remove compute resources, memory or storage as needed.

Lifecycle Management can be also provided by flexible control of databases for production or test cloning, plus simple storage management on virtual machine instances.

The security for database services may have its own unique set of security rules.

6.3.3.1 Attributes

Possible attributes for the Cloud Database Services are listed below.

Database Services		Descriptions and Recommended values of attributes
Service Name		Database Service
Basic	Dedicated DB Instance with an ID	Preconfigured software
	Storage Size	5GB, 10GB, 20GB, 40GB, 50GB, 100GB, 1TB
	Security	
	Add/remove compute resources (i.e. memory or storage)	
Managed	Dedicated DB Instance with an ID	Preconfigured software

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	Storage Size	5GB, 10GB, 20GB, 40GB, 50GB, 100GB, 1TB
	Add/remove compute resources (i.e. memory or storage)	
	Automated Backup	
	Point-in-time recovery	
	Security	
	Redundant Site	
	Redundant Zone	
Premium	Dedicated DB Instance with an ID	Preconfigured software
	Storage Size	5GB, 10GB, 20GB, 40GB, 50GB, 100GB, 1TB
	Add/remove compute resources (i.e. memory or storage)	
	Automated Backup	
	Point-in-time recovery	
	Security	
	Data Guard	
	Upgradability	
	Redundant Site	
	Redundant Zone	
Availability		
Billing	Service type	
	Memory size	
	Storage size	
	Database type	
	Backup	
	Length of usage	
NaaS attributes		

Table 17 : Cloud Database Service Attributes

6.3.4 Disaster Recovery (DR)

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Disaster recovery is recovering from a failure that has a negative impact on business continuity or finances. This could be hardware or software failure, a network outage, a power outage, physical damage to a building like fire or flooding, human error, or some other significant disaster.

Two parameters are important for DR services:

- **Recovery time objective (RTO)** which is the duration of time and the service level to which a business process must be restored after a disaster (or disruption) to avoid unacceptable consequences associated with a break in business continuity.

- **Recovery point objective (RPO)** that describes the acceptable amount of data loss measured in time. For example, if the RPO was 1 hour, after the system was recovered, it would contain all data up to a point in time that is prior to 11:00 AM because the disaster occurred at noon.

In the preparation phase of DR, data migration and durable storage need to be considered. When reacting to a disaster, it is important to either quickly commission compute resources to run user system in the Cloud Provider domain or to orchestrate the failover to already running resources in Cloud Provider domain.

The Cloud User can choose the most appropriate location for the selected disaster recovery site, in addition to the site where the user system is fully deployed. A Cloud Carrier may have multiple regions where the selected recovery site can be chosen to be different.

6.3.4.1 Attributes

Possible attributes for Cloud DR Service are listed below.

Database Recovery Services		Descriptions and Recommended values of attributes
Service Name		Database Recovery Service
Resources	Memory Size	
	Storage Size	
	Bandwidth	
RTO		
RPO		
Redundant Zone		
Redundant Site		
NaaS attributes		
Availability		
Billing	Memory size	
	Storage size	
	Bandwidth	
	Length of usage	

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Table 18 : DR Service Attributes

6.4 SECaaS

Security services such as Connectivity security, Application Security, or Content Security, can be provided by a cSP to cloud consumers. Such services are referred as Security as a Service (SECaaS).

With Security as a Service (SECaaS), a consumer does not manage or control the underlying security transport negotiation, encryption, detection algorithms, threat intelligence or network inspection, but has control over the selection of security solutions and scope with respect to their data and network.

SECaaS can be;

- Security of Storage Services with managed authorized access and customized Data Leakage Prevention technologies
- NaaS security provided through network traffic data inspection and filtering, DDoS and other intrusion attack vector protection
- Threat Intelligence where attack vectors are detected and propagated through cSP for mitigation
- Traffic cleaning, where consumer network traffic that would not normally utilize the cSP is routed expressly for SECaaS

Security around data storage services must allow consumer fine control of Network Access Control List (ACL) for modification and accessibility of data stored in cSP. Additional security is provided by audit tracking of data access or modification, along with data leakage technologies applied to the network access between cloud users and cSP.

Network traffic between over a cSC is subject to protection from attack and intrusion vectors. cSP can provide the traffic inspection and intrusion/attack blocking via combination of traditional firewall/security appliances, alongside virtual security solutions provided by Network Functions Virtualization (NFV). Both content inspection and packet inspection technologies should be utilized to provide high security.

The cSUI allows the consumer to tailor the security offerings for their intended use of cSP services. For example a SaaS provider with a CDN would focus security on intrusion and attack vectors while an Email Service may focus on AntiSpam technologies.

The cSP may provide the service where security events and responses are utilized to gather threat intelligence and react in a manner to protect the consumer services. Should an attack or intrusion be detected, an automatic response to isolate the attack vector, or continue to provide the service through alternate infrastructure can be taken.

SECaaS may provide network security functions through cSC set up for delivery of security functions by the cSP, regardless of whether the consumer traffic would normally access the cSP.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Selection of routing or tunneling technologies to establish the cSC and security services is performed at cSUI.

6.4.1 Attributes

Possible attributes for the SECaaS are listed below.

SECaaS		Descriptions and Recommended values of attributes
Service Name		SECaaS
Content Security	Authentication Realm[15]	
	Content Filtering	
	Anti-spam	
	Anti-malware	
	Data Encryption algorithm & key strength	
	DLP (Data Leakage Prevention) Rules	
	Access Audit	
Connectivity Security	Firewalling	
	Packet Inspection	
	DDoS Prevention	
	Transport Layer Encryption	
	Security Analytics	
	Threat Remediation	
	Application classification	
	Usage Control and Rate limiting	
NaaS Attributes		
Billing	Service type	
	Number of end points secured	
	Bandwidth secured	
	Length of usage	

Table 19 : SECaaS Attributes

[15] Authentication Realm is a scheme that defines how authentication is accomplished. For example, a user/device can be authenticated according to the credentials in a relational Database, a Radius server, or a PKI certificate, biometric/finger printing etc.

6.5 PaaS

By Platform as a Service (PaaS) [2], 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.

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. For example, AppScale allows a user to deploy some applications written for Google App Engine to their own servers, providing data-store access from a standard SQL or NoSQL database. Similarly Mobile PaaS (mPaaS) is formed by the Yankee Group for mobile users. 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. As a fully managed application platform for running and consolidating software applications and databases in the cloud, PaaS includes:

- A virtualized, scalable infrastructure of application and database servers
- Performance, reliability and security of the network
- Network, server and storage infrastructure management
- 24x7x365 infrastructure monitoring and support
- Built-in redundancy and security of Data Centers

Since business changes are unpredictable, users need a way to quickly modify applications in response. A web-based platform as a service portal can help to:

- Access and manage user application environment from nearly anywhere
- Quickly adapt forms and fields within the application template
- View activity reports to identify improvement areas

6.5.1 Attributes

Possible attributes for the PaaS are listed below.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

PaaS		Descriptions and Recommended values of attributes
Service Name		PaaS
Supported Programming Languages	List of Languages	
Database		
Support of multiple Operating Systems	List of OSSs	
Servers		
Security		
NaaS attributes		

Table 20 : PaaS Attributes

6.6 SaaS

The capability provided to the consumer via SaaS [2] 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 via customer portal, and licensed and billed monthly. Open-source and enterprise 32 and 64-bit operating system software options from various vendors are available. Below are a few examples of vendors and operating systems that could be installed:

- Microsoft
- RedHat
- CentOS
- Debian
- FreeBSD
- Ubuntu
- Vyatta Network
- Cloud Linux
- Parallels®
- cPanel®
- Server Virtualization Software such as VMWare ESX and ESXi, Citrix Xenserver, Citrix CloudPlatform, Parallels Virtuozzo, Microsoft Hyper-V
- Security Software such as McAfee Total Protection, McAfee Anti-Virus, Microsoft Windows Firewall, McAfee Host Intrusion Protection, Nimsoft Monitoring, APF Software Firewall
- Database Software such as Microsoft SQL Server (2000, 2005, 2008, 2012), MySQL, Cloudera Hadoop, MongoDB, Basho Riak
- Control Panel Software such as cPanel/WHM with Fantastico, RVSkin and Softaculous, Parallels Plesk Panel

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

6.6.1 Attributes

Possible attributes for the SaaS are listed below.

SaaS		Descriptions and Recommended values of attributes
Service Name		SaaS
On-demand software installation	Operating System Software	RedHat, Microsoft, FreeBSD
	Server Virtualization Software	
	Database Software	
	Control Panel Server	
	Security Software	
Licensing		
NaaS attributes		

Table 21 : SaaS Attributes

6.6.2 CDN

In Cloud Content Delivery Network (CDN) service, user content is distributed to a worldwide network of edge servers, therefore, users can access the content from a server near them. The content travels a shorter distance, ensuring faster load times.

Large objects are delivered to many users with sustained high data transfer rates. And if user traffic fluctuates, the service automatically adjusts as demand increases or decreases.

User content can be placed onto Cloud Object Storage and then CDN enables the content. The user then visits a CDN site and requests files from the nearest edge server. The edge server delivers a local, cached copy or pulls one from Cloud Object Storage, the origin server. The object's Time-to-Live (TTL) will expire at intervals the user defines such as 24 hours. If the TTL has expired when the next request is made, the file is again retrieved from Cloud Object Storage. The content is cached once again by the edge servers and the time-to-live (TTL) restarts.

6.6.2.1. Attributes

Possible attributes for the Cloud CDN Service are listed below.

CDN Services	Descriptions and Recommended values of attributes

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

Service Name		CDN
TTL in seconds		0, 1, 10, …..
Static Content		
Dynamic Content		
HTTP Cookies		
Cache Behavior	Origin server name	
	Connection protocol	
	Minimum TTL	
	Cookies	
	Trusted Signer	
Media transcoding	Prepare & optimize media for on-demand streaming	
Guaranteed Uptime (Availability)		
Support of multiple active CDNs		
Automatic Failover		
NaaS attributes		

Table 22 : Cloud CDN Service Attributes

6.6.3 Email Service

Email delivery can be basic as well as highly reliable and scalable on demand:

- Basic
  - SMTP Relay
  - SMTP/web API
  - Event API
  - Parse API
- Advanced
  - Basic capabilities
  - Highly Reliable
  - Intelligent (spam report, blocks, invalid addresses, unsubscribes, etc)
  - Rate Limits
  - Spam filter testing
  - Dedicated API address
  - Real-time analytics reporting
  - Automated Email reporting
  - Unsubscribe tracking
  - Open tracking
- Enterprise
  - Digital Transcoding
  - Message Queue and Notification Service

The service can be casual email service as well as business service. Emails can be archived with certain security capability.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

6.6.3.1 Attributes

Possible attributes for the Cloud Email Service are listed below.

Email Service		Descriptions and Recommended values of attributes
Service Name		Email Service
Basic (or Casual)	SMTP Relay	
	Calendar	
	Contacts	
	Basic Security	
Advanced	SMTP Relay	
	Calendar	
	Contacts	
	Anti-spam protection	
	Anti-virus protection	
	Invalid Address Protection	
	Archived with EAS-256	
	Rate Limiting	
	24x7x365 support	
Enterprise	SMTP Relay	
	Calendar	
	Contacts	
	Anti-spam protection	
	Anti-virus protection	
	Invalid Address Protection	
	Archived with EAS-256	
	Rate Limiting	
	24x7x365 support	
	Digital Transcoding	
	Message Queue and Notification (to send emails to large audiences)	
SLO	Delay	
	Loss	
	Availability	
Scalability		
NaaS attributes		

Table 23 : Cloud Email Service Attributes

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

6.7 CaaS

Real-time services such as Virtual PBX, voice and video conferencing systems, collaboration systems and call centers can be considered as Communication as a Service (CaaS). CaaS features can be:

- Business voice continuity avoiding missing a call even when disaster strikes
- Unlimited inbound, local and domestic long distance
- Fixed Mobile Convergence which removes the distinctions between fixed and mobile networks, providing a superior experience to customers by creating seamless services using a combination of fixed broadband and local access wireless technologies to meet their needs in homes, offices, other buildings and on the go
- 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
- Easy call management and feature editing through Microsoft Outlook, Internet Explorer or Firefox
- Fully managed and hosted
- Point-to-point or multipoint Video Calling
- Point-to-point or multipoint Voice Calling
- Point-to-point or multipoint voice and video conferencing
- Mobile application support allowing free download for both iOS and Android platforms
- Professional voice recording service for user greetings and other messages recorded by an industry-leading voice talent
- Bring your own device (BYOD) capabilities
- SLAs including quality of service and availability such as next business day replacement of phones for equipment maintenance of virtual PBX service
- Dynamic security policy including authentication, media encryption, and access control
- Scalability

6.7.1 Attributes

Possible attributes for the CaaS are listed below.

CaaS Services		Description and recommended values of attributes
Service Name		CaaS
Dynamic Call Transfer		
Video Call		
Voice Call		
Video Conferencing	Point-to-Point	
	Multipoint	
Voice Conferencing	Point-to-Point	

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	Multipoint	
Audio and Video Conferencing simultaneously	Point-to-Point	
	Multipoint	
Unified Messaging (email, voice mail, fax, and text-to-speech that can be accessed via mobile device, email client, web interface, or dual-tone multi-frequency signaling (DMTF) telephone)		
Instant Messaging (IM)		
Presence		
IVR		
Voice Recording		
Video Recording		
Multi-site routing		
Tele-presence		
DR Service		
Fixed Mobile Convergence		
Emergency Services	Citizen-to-Authority calls such as 911	
	Authority-to-Citizen announcements such as tsunami warning	
	Emergency Traffic Prioritization	
Scalability	Number of users	
	Number of Class of Services	
	Number of Sites	
SLA	Delay	
	Jitter	
	Loss	
	Availability	
Security		
NaaS attributes		
Billing		

Table 24 : CaaS Attributes

6.8 Operations, Administration, Maintenance, Provisioning, Troubleshooting (OAMPT) for Cloud Services

In previous sections, we have defined interfaces and connections of Cloud Services, provided examples of their associated attributes and OAMPT functions.

The objective in this section is to describe OAMPT functions and OAMPT common attributes for Cloud Services that can be standardized and tested. List of possible attributes are left for a later phase of this document.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

6.8.1 Provisioning

Provisioning and Configuration can be categorized as rapid provisioning, resource changing, monitoring and reporting. Rapid provisioning is automatically deploying cloud systems based on the requested service/resources/capabilities. Resource changing is adjusting configuration/resource assignment for repairs, upgrades and joining new nodes into the cloud.

Automated customer notifications for order confirmations and payments are needed.

Systems associated with services need to be maintained as well. These functions include:

- Automated OS Reloads
- Remote Reboot & Console Access
- Image Import/Export

6.8.2 Performance Management

Performance management is to perform periodic measurements for interfaces, connections and servers; generating notifications for threshold crossings; and generating performance reports.

Monitoring and accessing performance reports are needed:

- Monitoring SLOs
- Host Ping and Statistics availability for 24x7
- Email/Ticket Notification for threshold crossing

6.8.3 Fault Management

Fault management comprises discovering and monitoring physical and virtual resources; monitoring cloud operations; and generating events and performance reports, including

- Notification for failures and
- Automated customer notifications for ticket updates and scheduled maintenance.

Some of the events can be listed as;

- Service Outage
- Incorrect Recovery
- Network misconfiguration
- Clusters collapsed
- Upgrade event
- Some servers offline
- Maintenance
- A datacenter (DC) offline

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

- Bad cross-DC re-mirroring
- DCs went down
- Power failure
- x% machines of a DC offline
- Bad failover
- All user apps in degraded states
- Network failure
- Late failover
- Global service interruption
- System overload
- Overheated DC
- Broken failover mechanism
- Global outage

6.8.4 Billing

As described in previous sections, multiple actors are likely to be involved in providing a Cloud Service. Billing will be issued from the cSP to cloud users. Below are the possible attributes that are likely to be part of a bill.

Billing		Description and recommended values of attributes
Billing Actor		Free form
Billed Actor		Free form
Billed Account #		Numeric Only
Instance Id	Circuit Id, VM, Server or storage ID	Free form
Billing Method		
Fixed	Time based in monthly	
	Bandwidth based in Kbps, Mbps or Gbps	
	Storage Capacity based in MB, GB or TB	
Usage Based	Time based in minutes or hours	
	Bandwidth based in Kbps, Mbps or Gbps	
	Storage Capacity based in MB, GB or TB	
Class of Services	Multiple	Low, Medium, High
	Single	Low, Medium or High
Circuit Id		Free form

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

VM Id		Free form
Server Id		Free form
Storage Id		Free form
Server	VM	quantity of VMs
	CPUs	1, 2, 4, 8, 16…
	RAM	
	Diversity – Include device Id to be diverse from	Physical Same Site or Geographically Separate Sites
Storage	Method	RAID 1, 2, 3, 4, 5
	Capacity	
	Diversity – Include device Id to be diverse from	Physical Same Site or Geographically Separate Sites
Authentication Method	RADIUS	
	Other	
Security Features	Firewall	
	NAT	
	D-DOS Detection	
Interface	Diversity – Include interface Id to be diverse from	
	Ethernet	
	DOCSIS	
	EPON	
	GPON	
	MPLS	
	IP	
	OTN	
	WDM	
	SONET/SDH	
Enterprise IPv4-addr		
Enterprise IPv6-addr		
Enterprise VLAN Id		
Start_time		dd/mm/yyyy HH:MM:SS
Stop_time		dd/mm/yyyy HH:MM:SS
Usage Bandwidth Data for each CoS – Low, Medium, High	Bytes TX	KB, MB, GB, TB
	Bytes RX	KB, MB, GB, TB
	Total Bytes	KB, MB, GB, TB
	Bits TX	Kb, Mb, Gb, Tb
	Bits RX	Kb, Mb, Gb, Tb
	Total Bits	Kb, Mb, Gb, Tb
Usage Stored Data	Bytes TX	KB, MB, GB, TB

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

	Bytes RX	KB, MB, GB, TB
	Total Bytes	KB, MB, GB, TB

Table 25 : Billing Attributes

6.8.5Testing

Procedures for verifications of attributes for each interface and connection, and performance of application related to Cloud Services before using the service are necessary.

For L2 Ethernet interfaces and connections, the procedures in MEF 9 [6], MEF19 [19], MEF25 [20], MEF27 [23], MEF34 [26] and MEF37 [29] apply.

6.9. Service Availability

Monthly Uptime (i.e. monthly availability) for a Cloud Service is expected to be at least 99.999% for business services. Monthly Uptime Percentage measurements may exclude downtime resulting directly or indirectly from more than one Availability Zone in which user is running an instance, within the same region, is “Unavailable” to user.

Unavailable means that all of user running instances have no external connectivity or all of the user attached volumes perform zero read write I/O with pending I/O in the queue, or other resources involved in a specific Cloud Service are unavailable.

References

[1] M. Toy, “Cable Networks, Services, and Management”,   J. Wiley-IEEE Press, 2014.

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

[3] International Telecommunications Union, Telecommunication Standardization Sector (ITU-T) Focus Group (FG) Cloud Technical Report (TR), version 1.0, February 2012

[4] IEEE Std 802.3-2008 IEEE Standard for Information technology-Telecommunications and information exchange between systems—Local and metropolitan area networks-Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and Physical Layer specifications

[5] CableLabs, DOCSIS 3.1 Physical Layer Specification DOCSIS PHY v3.1 CM-SP-PHYv3.1-I01-131029, 2013.

[6] CableLabs, DOCSIS 3.0 Physical Layer Interface Specification DOCSIS PHY v3.0 (CM-SP-PHYv3.0-I11-13-0808), 2013.

[7] IEEE Std 802.3ah.-2004: IEEE Standard for Information technology. Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

[8] 802.3av-2009 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 3: CSMA/CD Access Method and Physical Layer Specifications Amendment 1: Physical Layer Specifications and Management Parameters for 10 Gb/s Passive Optical Networks (10G EPON)

[9] ITU-T G.984.1 (03/2008) Digital sections and digital line system – Optical line systems for local and access networks Gigabit-capable passive optical networks (GPON): General characteristics

[10] ITU-T G.694.1 (02/2012) Transmission media and optical systems characteristics Characteristics of optical systems Spectral grids for WDM applications: DWDM frequency grid

[11] ITU-T G.694.2, WDM applications: CWDM wavelength grid, 12/03.

[12] ITU-T G.705 Characteristics of plesiochronous digital hierarchy (PDH) equipment functional blocks, 10/00.

[13] ITU-T G.774.02 Synchronous digital hierarchy (SDH) configuration of the payload structure for the network element view, 02/01.

[14] MPLS PVC User to Network Interface Implementation Agreement, 2003

[15] ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks, 11/2013.

[16] MEF 9 Abstract Test Suite for Ethernet Services at the UNI, October 2004.

[17] MEF 10.3 Ethernet Services Attributes Phase 3, October 2013.

[18] MEF 15 Requirements for Management of Metro Ethernet Phase 1 Network Elements, November 2005.

[19] MEF 19 Abstract Test Suite for UNI Type 1, April 2007.

[20] MEF 25 Abstract Test Suite for UNI Type 2 Part 3 Service OAM, May 2009.

[21] MEF 33 Ethernet Access Services Definition, January 2012.

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

[23] MEF 27 Abstract Test Suite For UNI Type 2 Part 5: Enhanced UNI Attributes & Part 6: L2CP Handling, May 2010.

[24] MEF 28 External Network Network Interface (ENNI) Support for UNI Tunnel Access and Virtual UNI, October 2010.

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

[26] MEF 34 ATS for Ethernet Access Services, February 2012.

[27] MEF 35 Service OAM Performance Monitoring Implementation Agreement, April 2012.

[28] MEF 35.0.1 SOAM PM Implementation Agreement Amendment, October 2013.

[29] MEF 37 Abstract Test Suite for ENNI, January 2012.

[30] IEEE Std. 802.1Q-2011, Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks (PDF; 6.0 MiB). ISBN 978-0-7381-6708-4.

[31] RFC4577: E. Rosen, et all, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs), June 2006,

[32] RFC 4659: J. De Clercq, BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN, September 2006

[33] RFC 4293: S. Routhier, Ed. Management Information Base for the Internet Protocol (IP), April 2006.

[34] RFC2698: J. Heinanen, et al., A Two Rate Three Color Marker, September 1999

[35] RFC 2697: J. Heinanen, et al.; A Single Rate Three Color Marker, September 1999

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

[36] RFC4122 P. Leach, et al., A Universally Unique IDentifier (UUID) URN Namespace

[37] M. Mahalingam, et all, IETF Draftdraft-mahalingam-dutt-dcops-vxlan-09.txt VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, April 2014

[38] RFC7365: Marc Lasserre, et al., Framework for DC Network Virtualization, October, 2014.

[39] D. Black, et. al., An Architecture for Overlay Networks (NVO3), draft-ietf-nvo3-arch-01.mht, October 2013.

[40] ETSI GS NFV 001 v1.1.1 (2013-10) Network Functions Virtualisation (NFV): Use Cases

[41] https://www.opennetworking.org/component/search/?searchword=oam&searchphrase=all&Itemid=101

[42] Amazon EC 2, http://aws.amazon.com/ec2/

[43] Cloud Servers, http://www.softlayer.com/cloud-servers

[44] http://www.vmware.com/products/

[45] https://wiki.io.comcast.net/display/PI/Comcast+Cloud

[46] https://www.openstack.org/software/openstack-compute/

[47] MEF 23.1 Class of Service Phase 2 Implementation Agreement

[48] MEF 6.1.1 Layer 2 Control Protocol Handling Amendment to MEF 6.1

[49] MPLS & Frame Relay Alliance Technical Committee, MPLS PVC User to Network Interface Annex B: MPLS Proxy Admission Control Protocol Implementation Agreement, October 2004

[50] RFC5462: L. Andersson, et al.; Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field, February 2009

[51] MEF 16 Ethernet Local Management Interface

[52] RFC 6427: G. Swallow, et al.; MPLS Fault Management Operations, Administration, and Maintenance (OAM), November 2011.

[53] IETF Draft: H. Asai, et al,; Management Information Base for Virtual Machines Controlled by a Hypervisor, draft-ietf-opsawg-vmm-mib-00.txt, February 10, 2014

[54] RFC 7012, B. Claise,et al., Information Model for IP Flow Information Export (IPFIX), September 2013.

[55]

[56] MEF 32 Requirements for Service Protection Across External Interfaces, July 2011.

[57] MEF 12.2 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer, May 2014.

[58] MEF 4 Metro Ethernet Network Architecture Framework Part 1: Generic Framework, May 2004.

[59] MEF 43 Virtual NID (vNID) Functionality for E-Access Services, April 2014.

[60] RFC 4732 M. Handley, et al., Internet Denial-of-Service Considerations, November 2006

[61] RFC2474, K. Nichols, et al., Definition of the Differentiated Services Field (DS Field)

[62] in the IPv4 and IPv6 Headers, December 1998

[63] RFC 5505, D. Thaler, et al., Principles of Internet Host Configuration, May 2009

[64] RFC 5286, A. Atlas, et al., Basic Specification for IP Fast Reroute: Loop-Free Alternates, September 2008.

[65] https://developers.google.com/storage/docs/durable-reduced-availability

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.

[66] http://aws.amazon.com/ebs/

[67] ISO/IEC 8802-2:1998, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 2: Logical link control.

[68] MEF Draft, Carrier Ethernet Services for Cloud Implementation Agreement, July 2014.

[69] MEF 41 Generic Token Bucket Algorithm, October 2013.

[70] MEF 35.0.2 Service OAM Performance Monitoring Implementation Agreement Amendment 2, February 2014.

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

[72] MEF 6.2 Ethernet Service Definitions Phase 3, August 2014.

[73] RFC4090, P. Pan, et. al., Fast Reroute Extensions to RSVP-TE for LSP Tunnels, May 2005

[74] ITU-T M.3100, Generic network information model, 4/2005.

[75] RFC 2863, K. McCloghrie, et. al., The Interfaces Group MIB, June 2000

[76] MEF NaaS Management Vision Paper Draft, September 2014.

[77] IEEE 802.1Qay-2009: Provider Backbone Bridge Traffic Engineering

[78] http://www.oracle.com/technetwork/developer-tools/apex/overview/index-155186.html

[79] RFC3270, F. Le Faucheur, et al., Multi-Protocol Label Switching (MPLS) Support of Differentiated Services, May 2002.

[80] ITU-T G.709/Y.1331, Interfaces for the optical transport network Recommendation, 02/2012.

[81] ITU-T Y.3500, Cloud Computing Information technology . Cloud computing Overview and Vocabulary, 8/2014.

[82] RFC 6428, D. Allan, et al., Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile, November 2011.

© The Cloud Ethernet Forum 2014. Any reproduction of this document, or any portion thereof, shall contain the following statement: "Reproduced with permission of the Cloud Ethernet Forum." No user of this document is authorized to modify any of the information contained herein.