Technical Specification

OCC 1.0

OCC 1.0 Reference Architecture with SDN and NFV Constructs

August, 2015

Disclaimer

Table of Contents

List of Figures

List of Tables

List of Contributing Members

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

Contributing CEF member companies agreed to be listed:

Avaya
Alcatel-Lucent
Verizon
Veryx

1.Introduction

The purpose of this document is to describe possible implementations of Cloud Services Architectures using Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) constructs.

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
cCcPI	Cloud Carrier Cloud Provider Interface	OCC 1.0 Ref. Arch.[1]
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).	OCC 1.0 Ref. Arch.[1]
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).	OCC 1.0 Ref. Arch.[1]
cC	Cloud Carrier (cC) is an intermediary that provides connectivity and transport between Cloud Providers and Cloud Consumers or between Cloud Providers.	OCC 1.0 Ref. Arch.[1]
cCcPI	Cloud Carrier Cloud Provider Interface	OCC 1.0 Ref. Arch.[1]
CoS	Class of Service	MEF 10.3 [14]
CoS ID	Class of Service Identifier	MEF 23.1 [22]
cP	Cloud Provider is an entity that is responsible for making cloud applications available to Cloud Consumers (Cloud Service Users).	NIST Special Publication 500-291 [13]
cSC	Cloud Service Connection	OCC 1.0 Ref. Arch.[1]
cSC-c	Cloud Carrier Connection	OCC 1.0 Ref. Arch.[1]

cSC-p	Cloud Provider Connection	OCC 1.0 Ref. Arch.[1]
cSC-cp	The segment of cSC within the boundaries of a Cloud Service Provider where cSC crosses multiple Cloud Service Providers	OCC 1.0 Ref. Arch.[1]
cSI	Cloud Service Interface (cSI) is the interface of a Cloud Service application supporting entity of a Cloud Provider such as VM.	OCC 1.0 Ref. Arch.[1]
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.	OCC 1.0 Ref. Arch.[1]
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.	OCC 1.0 Ref. Arch.[1]
cSCTP (Cloud Service Connection Termination Point)	A logical entity that originates or terminates cSC at a logical user or machine interface.	OCC 1.0 Ref. Arch.[1]
cSI	Demarcation Point between Cloud Service Providing entity such as a server or VM, and Cloud Service Provider.	OCC 1.0 Ref. Arch.[1]
cSPcSPI	Cloud Service Provider Cloud Service Provider Interface	OCC 1.0 Ref. Arch.[1]
cSC-c	Cloud Carrier Connection	OCC 1.0 Ref. Arch.[1]
cSC-p		
cSC-csp	Cloud Service Provider Connection	OCC 1.0 Ref. Arch.[1]
cSC-csp-TP	Cloud Service Provider Connection Termination Point	OCC 1.0 Ref. Arch.[1]
cSC-cp-TP	Cloud Carrier-Provider Connection Termination Point	OCC 1.0 Ref. Arch.[1]
cSC-p	Cloud Provider Connection	OCC 1.0 Ref. Arch.[1]

cSUI	Demarcation Point between a Cloud Consumer and Cloud Service Provider.	OCC 1.0 Ref. Arch.[1]
DoS	Denial of Service	RFC4732
DSCP	Differentiated Service Code Point	RFC 2474 [17]
EMS	Element Management System	
ENNI	External Network Network Interface	MEF 4 [16]
EVC	Ethernet Virtual Connection	MEF 10.3 [14]
EPL	Ethernet Private Line	MEF 6.2 [19]
EVPL	Ethernet Virtual Private Line	MEF 6.2 [19]
Hypervisor	A software, firmware or hardware running on a server that enables creation of virtual machines and runs them.	OCC 1.0 Ref. Arch.[1]
ICMP	Internet Control Message Protocol	RFC 792 [23]
IPSec ESP	Internet Protocol Security Encapsulating Security Payload	RFC 4303 [24]
L2CP	Layer Two Control Protocol	MEF 10.3 [14]
E-Line	An Ethernet Service Type that is based on a Point-to-Point EVC.	MEF 6.2 [19]
E-LAN	An Ethernet Service Type that is based on a Multipoint-to-Multipoint EVC.	MEF 6.2 [19]
LAN	Local Area Network	IEEE 802-2 [18]
LSO	Life Cycle Orchestration	MEF 50 [21]
LSP	Label-switched Path	MPLS Architecture[29]
MAC	Media Access Control	IEEE802-2 [18]
NE	Network Element	Not Applicable
NFV	Network Functions Virtualization	Draft ETSI GS NFV-INF V0.3.1 [2]
NID	Network Interface Device	MEF 4 [16]
OSS/BSS	Operation Support System/Billing Support System	Not Applicable
PW ID	Pseudowire Identification	RFC 4447 [31]

REST API	Representational State Transfer Application Programming Interface	RFC 6690 [25]
SDN	Software-Defined Networking	ONF White Paper [10]
S-VLAN	Service VLAN (also referred to as Provider VLAN)	IEEE802.1Q [15]
TCP-AO	Transmission Control Protocol- Authentication Option	RFC5925 [26]
TCP SYN	Transmission Control Protocol Synchronize	RFC793 [27]
TLS	Transport Layer Security	RFC5246 [28]
UNI	User Network Interface	MEF 4 [16]
VM	Virtual Machine	OCC 1.0 Ref. Arch.[1]
VN	Virtual Network	Not Applicable
VNF	Virtualized Network Function	Draft ETSI GS NFV-INF 001 V0.3.12 [4]
VNIC	Virtual Network Interface Controller	Not Applicable

Table 1: Terminology and Acronyms

3. Summary of OCC 1.0 Architecture[1]

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

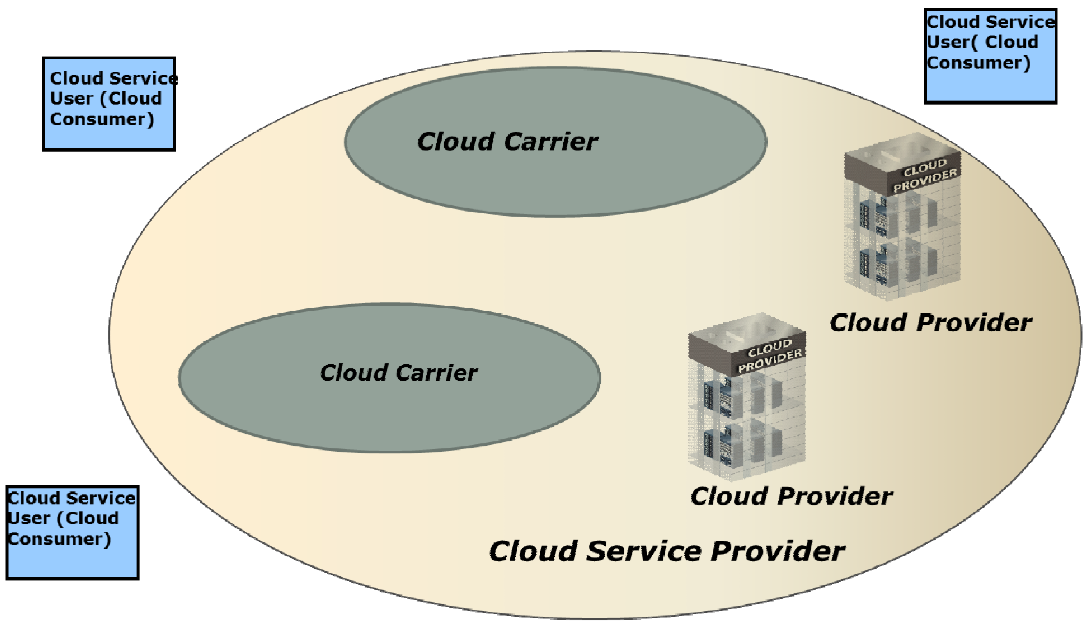


Figure 1: Cloud Service Actors

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 the demarcation point between the Cloud Service Provider and the Cloud Consumer.

When the Cloud Provider (cP) and the Cloud Carrier (cC) are two independent entities belonging to two different operators as depicted in Figures 3 and 4, 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.

[1] This section copies figures and text from OCC 1.0 Reference Architecture. The Reference Architecture takes precedence if there are differences.

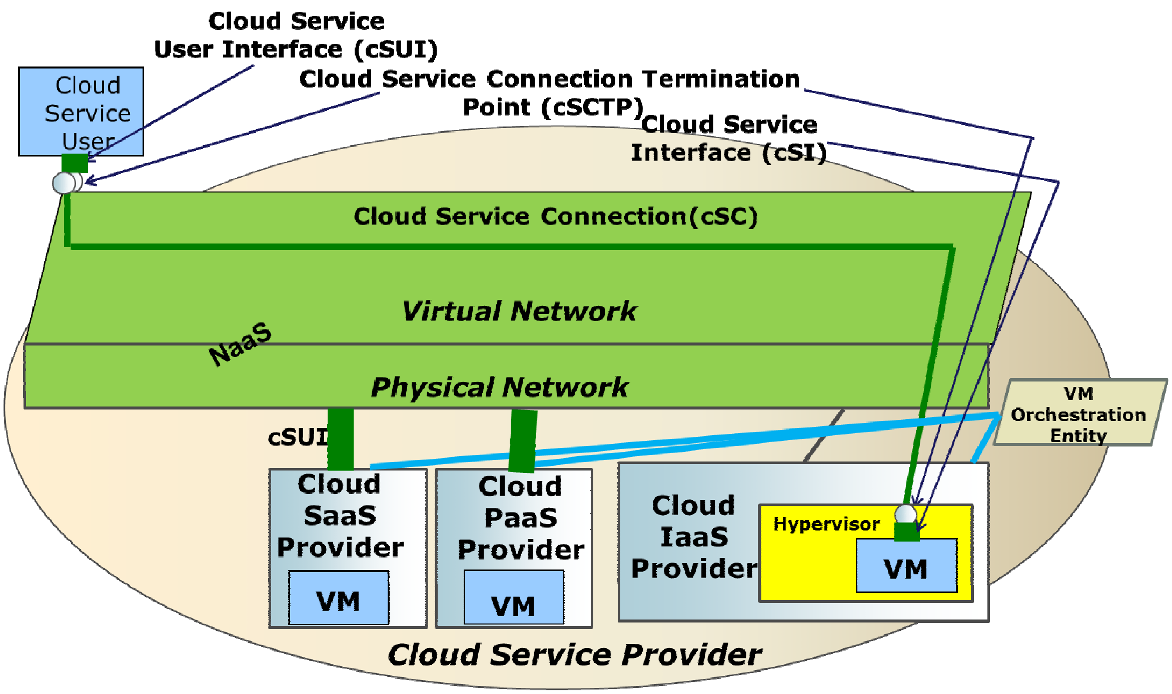


Figure 2: Cloud Service Provider access via the standard interface, cSUI.

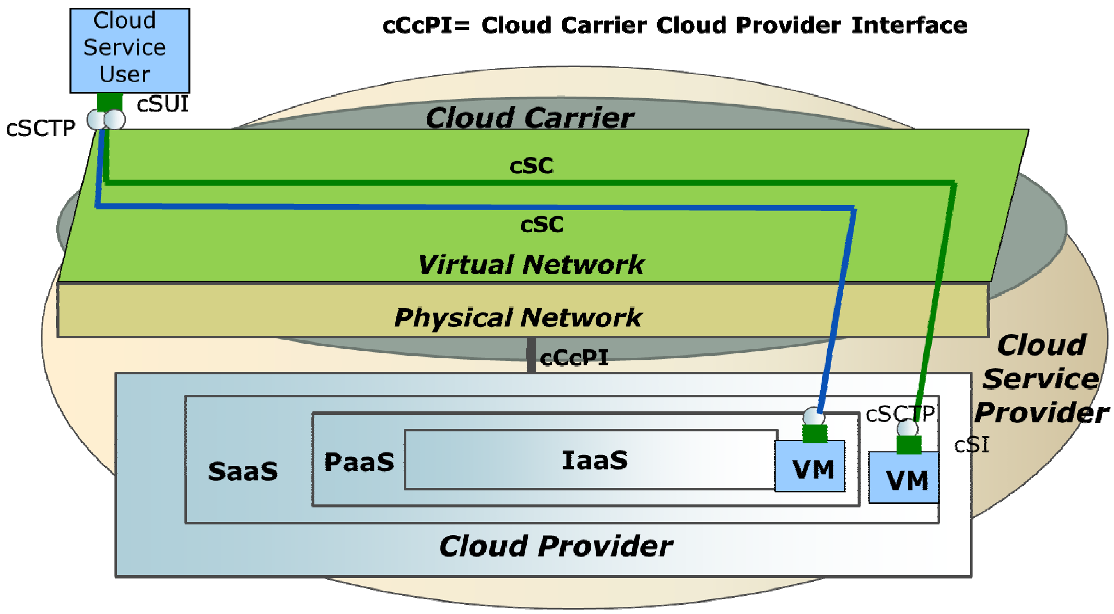


Figure 3: Cloud Provider and Cloud Carrier belong to two different Operators

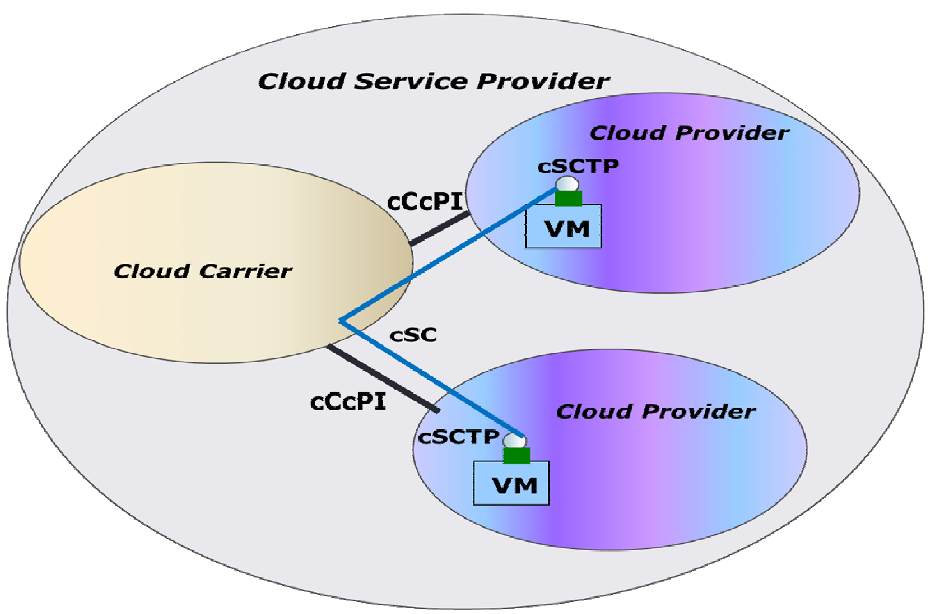


Figure 4: cSC between two Cloud Provider entities.

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 5 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)[2].

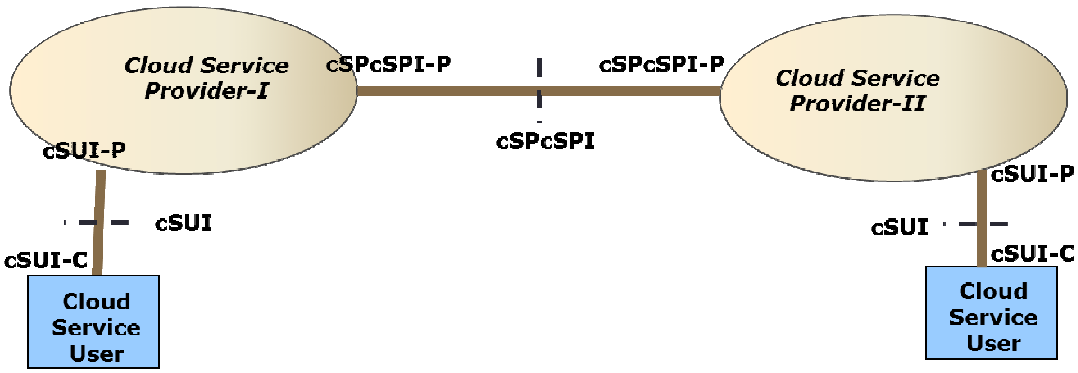


Figure 5: Two Cloud Service Providers collectively providing Cloud Services

So far we have identified interfaces between user and cSP, between cSPs, between cP and cC, between NaaS [1] and Cloud Service application supporting entity. The protocol stack at each interface that can be supported is depicted in Figure 6. Each of the protocol layer may be further decomposed into their data, control and management plane components.

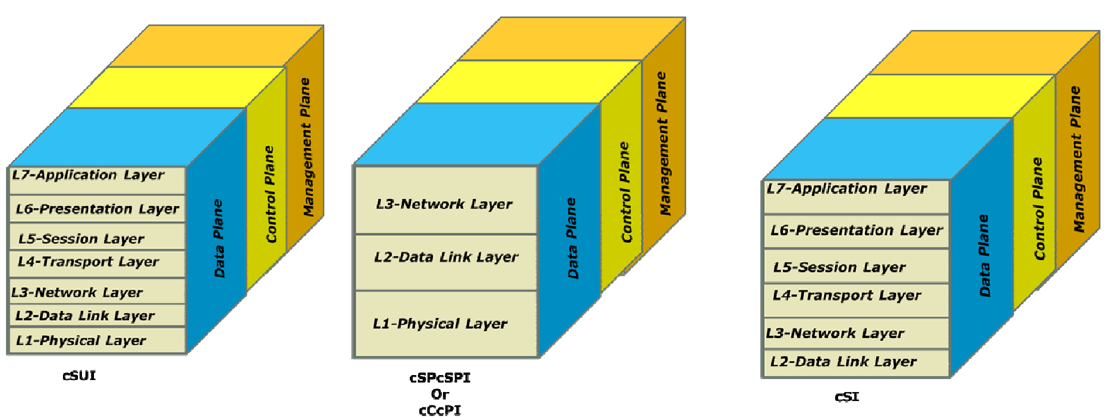


Figure 6 : Protocol Stacks that can be supported at external interfaces

2 cSO is a cSP that is not responsible from the end-to-end service. It can be cP or cC or an entity providing cloud applications in addition to cC and cP functionalities. It is possible that cSO may provide a bill for its part of the service, but this bill is not a bill for the end-to-end service that can be provided by the cSP.

The cSC provides connectivity 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 7 where a virtual switch routes traffic to a destination VM.

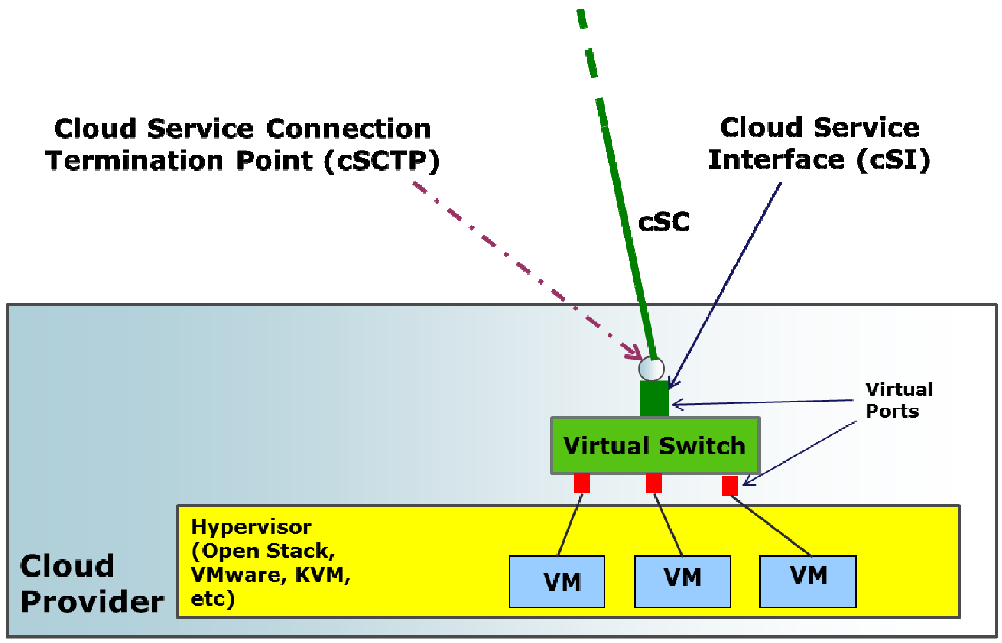


Figure 7: Multiple VM sharing a cSC

Furthermore, a VM may consist of multiple virtual network interface controllers (VNICs) where each VNIC can be identified by a soft MAC address, as depicted in Figure 8.

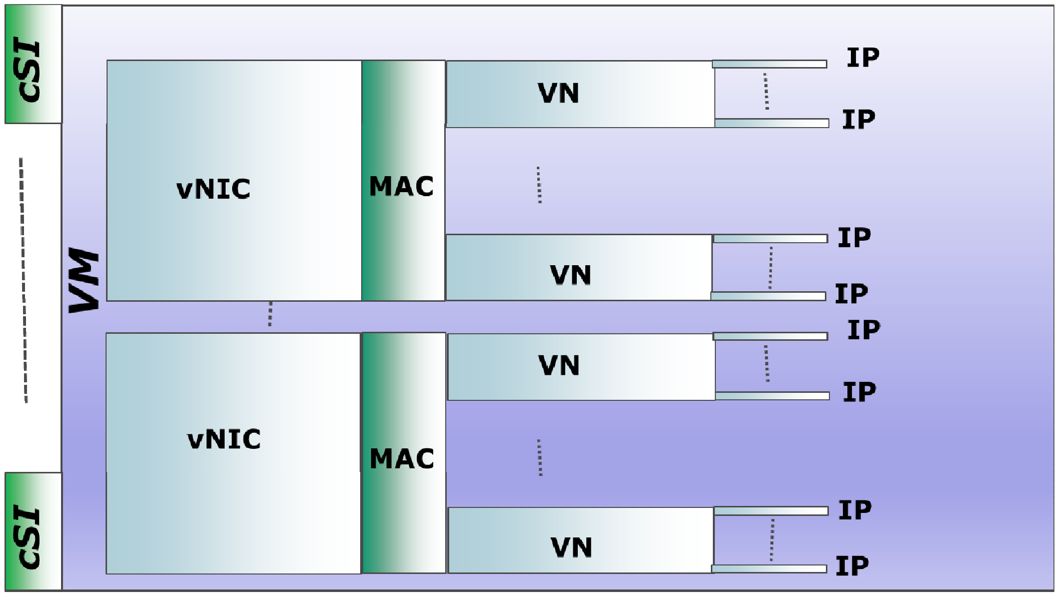
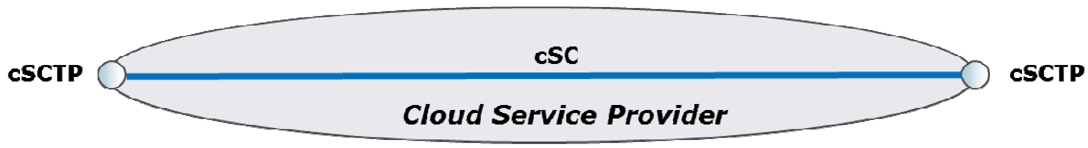
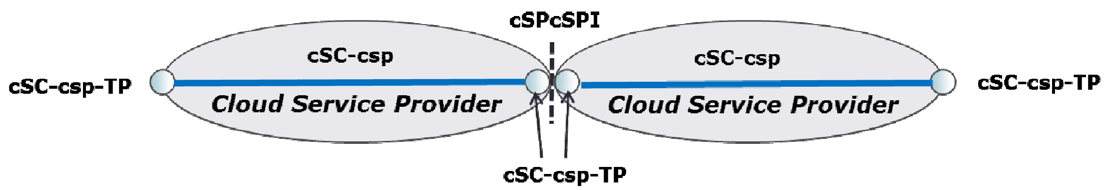


Figure 8: VM supporting multiple cSIs, virtual network interface controllers (vNICs), MACs, virtual networks (VNs) and IP addresses.

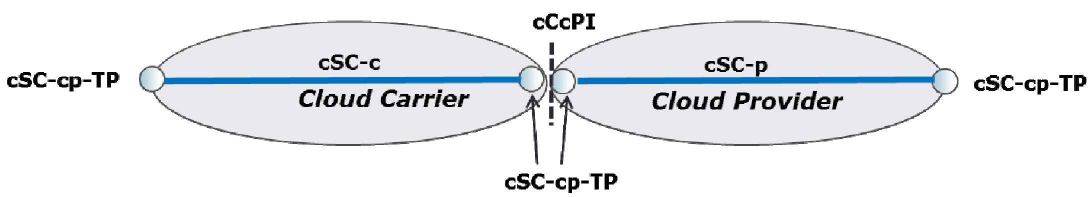
Cloud service connection types are depicted in Figure 9. The connection can be between two termination points of a cSP. If the connection crosses multiple cSPs, the connection segment within a cSP is called Cloud Service Provider Connection (cSC-csp). If the connection crosses a cP and cC, the connection segment within the cP is called Cloud Provider Connection (cSC-p) and the connection segment within the cC is called Cloud Carrier Connection (cSC-c).



(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 9: Cloud Service Connection Types

4. Summary of NFV Architecture

NFV [2, 3] divides the network into two layers, Network Hardware (or Infrastructure) and Virtual Network (or Virtual Network Function) as depicted in Figure 10 below. (Vn-Nf)/VN interface is identified as the virtual interface for the network. The E-Line and E-LAN services of MEF are being considered as examples of (Vn-Nf)/VN.

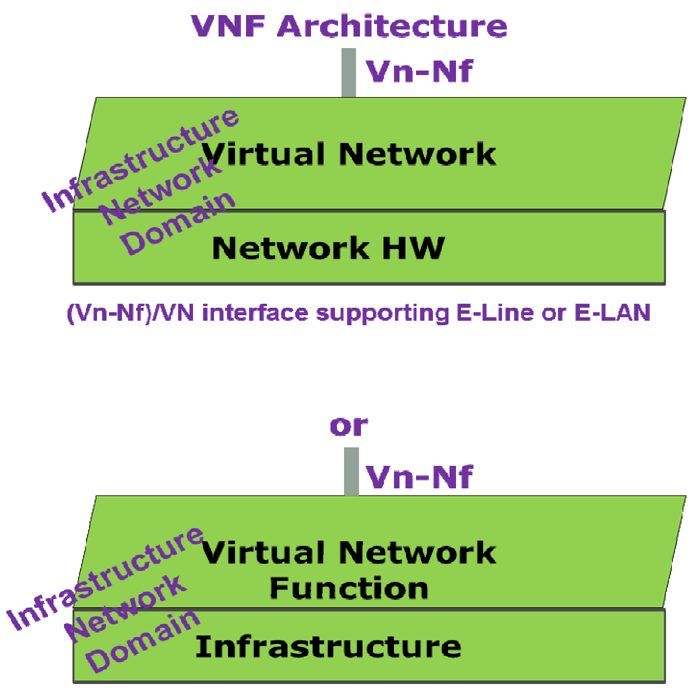


Figure 10: Network Layering and interface of NFV

NFV also identifies a VM interface [2] as (Vn-Nf)/VM or Vn-Nf-VM, which we call it as cSI. Given there is no description of (Vn-Nf)/VM in [2], we don't know if it is an equivalent of cSI.

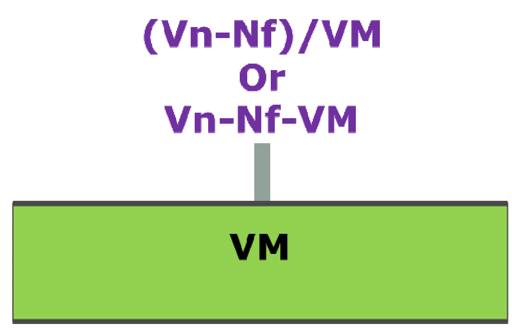


Figure 11: VM Interface

NFV identified an interface to hardware [4] as Vi-Ha and interface to Bare Metal OS as depicted in Figures 12 and 13. This interface can be a subset of cSUI or cCcPI or cSPcSPI.

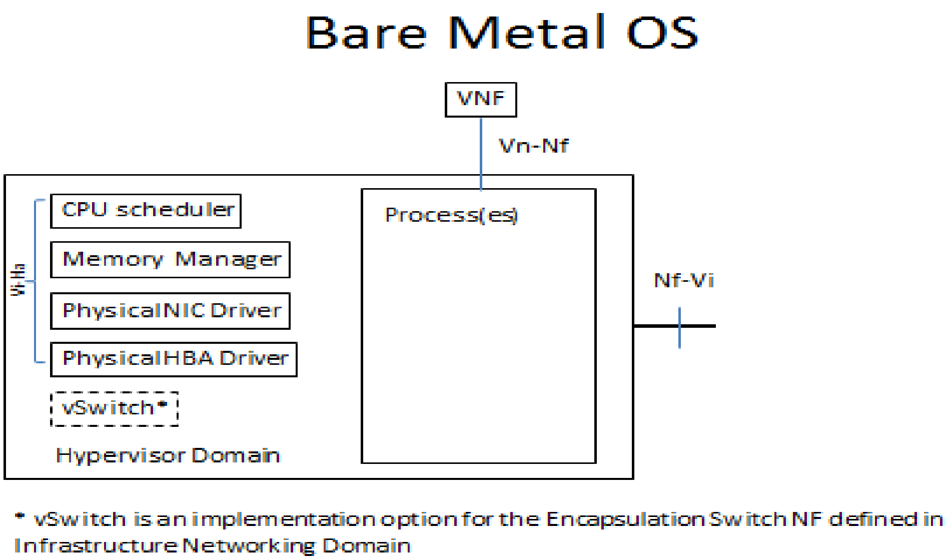


Figure 12: Bare Metal Server Interface [2]

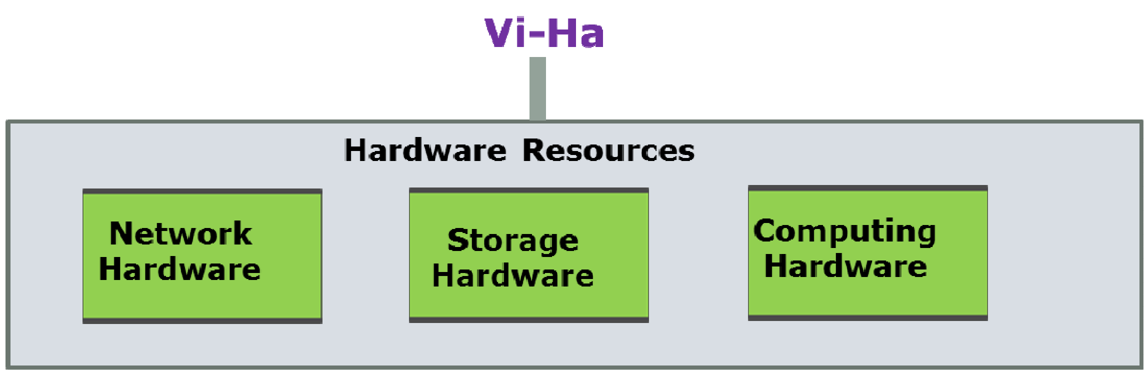


Figure 13: Bare Metal Server Interface [4]

NFV identifies SWA (Software Architecture)-1 interface [5] as depicted in Figure 14 to enable communication between various network functions within the same or different network service. They may represent data and/or control plane interfaces of the network functions (VNF, Physical Network Function-PNF). SWA-1 can be an equivalent of the virtual component of MEF UNI.

Figure 14: SWA-1 Interface

NFV identifies SW-5 interfaces which are an abstraction of all sub-interfaces between the NFV Infrastructure (NFVI) and the VNF, including VNF inter-switch connectivity services such as E-LAN, E-Line [5], as depicted in Figure 14.

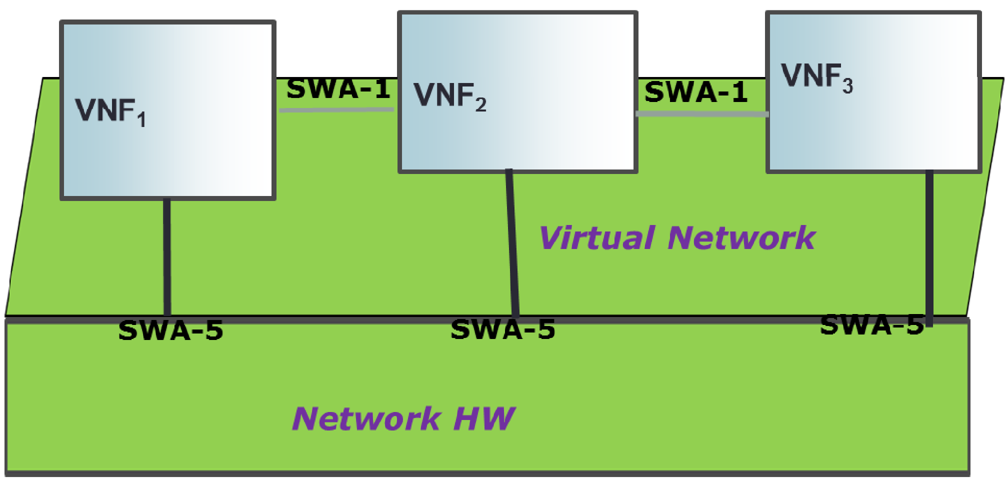


Figure 15: SWA-5 Interface

NFV divides functional blocks as Host Functional Block (HFB) and Virtualization Functional Block (VFB) [30] as depicted in Figure 16. The interface between HFB and VFB is called Container Interface which is the virtual interface between two containers.

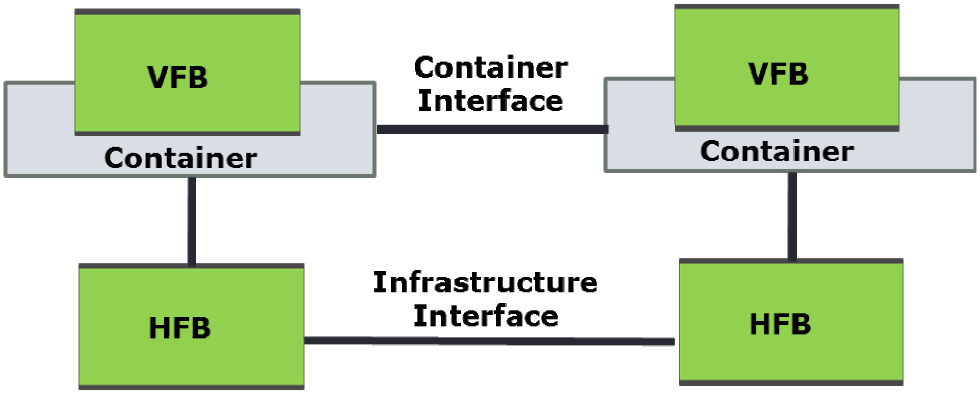


Figure 16: Container Interface

VNFs are managed by the "Management and Orchestration Function" [4] (Figure 17). The interaction of this orchestrator with Element Management System (EMS) and OSS/BSS [6] is depicted in Figure 18.

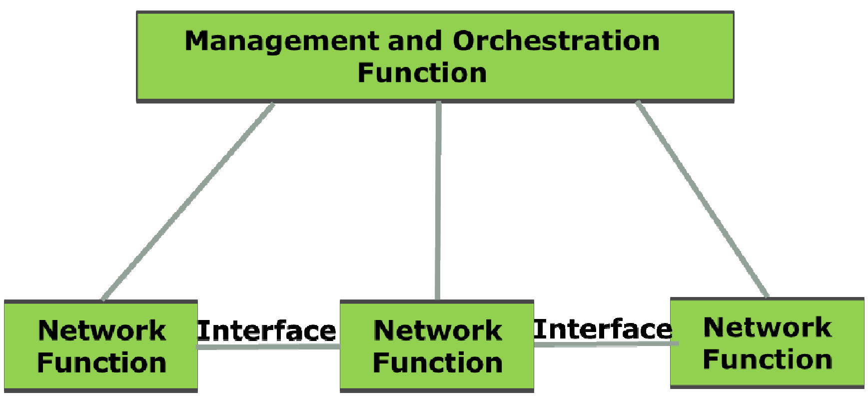


Figure 17: Management of Network Functions

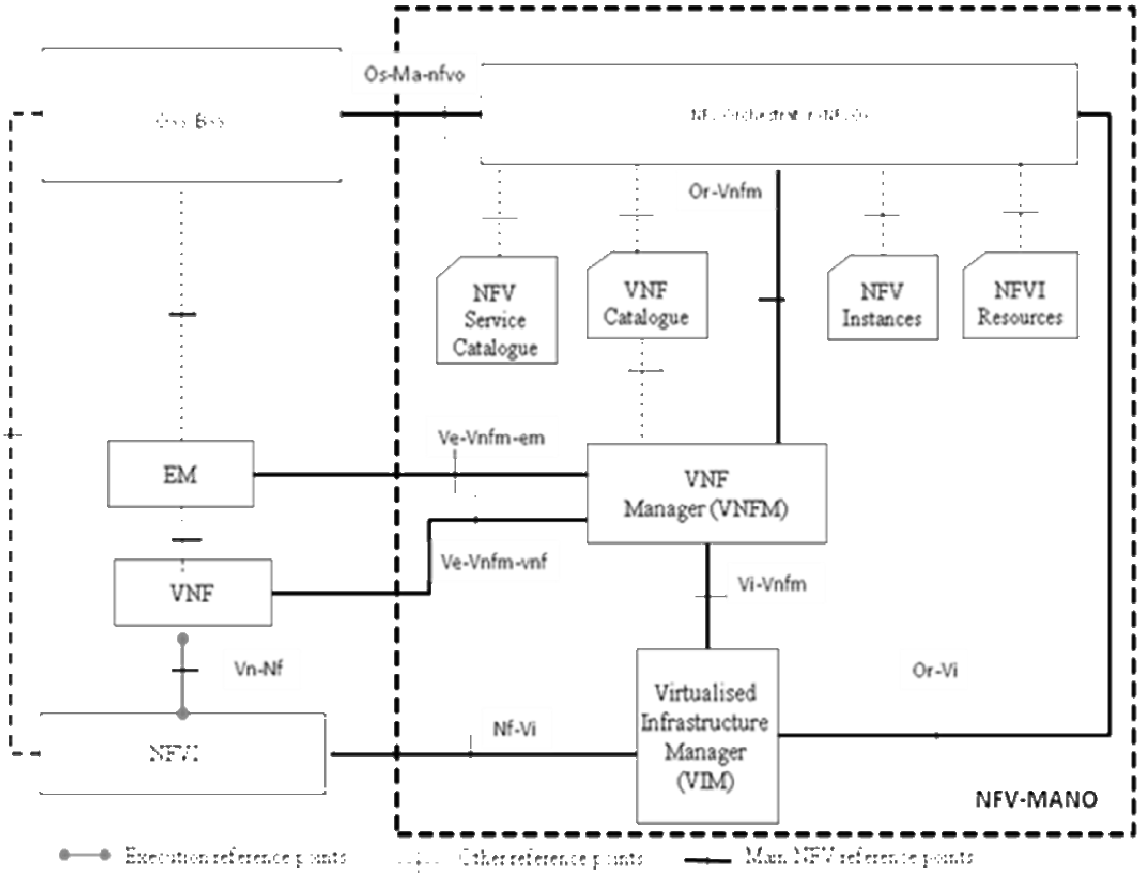


Figure 18: NFV Orchestrator interaction with EMS and OSS/BSS [6]

5. Mapping Between NFV and OCC Reference Architecture Constructs

Given there is no formal or informal descriptions of NFV interfaces in ETSI/NFV documents, it is very difficult to map the constructs. Table 2 and the following figures describe the recommended mappings between NFV and OCC architectural constructs.

	NFV Construct	OCC Construct
User Interface	(Vi-Ha)+(Vn-Nf)/VN	cSUI
VM Interface	(Vn-Nf)/VM	cSI
Container Interface	Container Interface	cSI
SWA-1	Software Architecture-1	cSI
Cloud Carrier-Cloud Provider Interface		cCcPI
Cloud Service Provider-Cloud Service Provider Interface		cSPcSPI
Connection between Users or between a	VNF Forwarding Graph	cSC

User and VM or between VMs		
Connection Termination Point		cSCTP

Table 2 : Mapping between OCC and NFV Constructs

NaaS and Cloud User interfaces to NaaS are depicted in Figure 19 using NFV constructs. Since cSUI represents both physical and logical components of NaaS, we map the cSUI to the combination of Vi-Ha and (Vn-Nf)/VN.

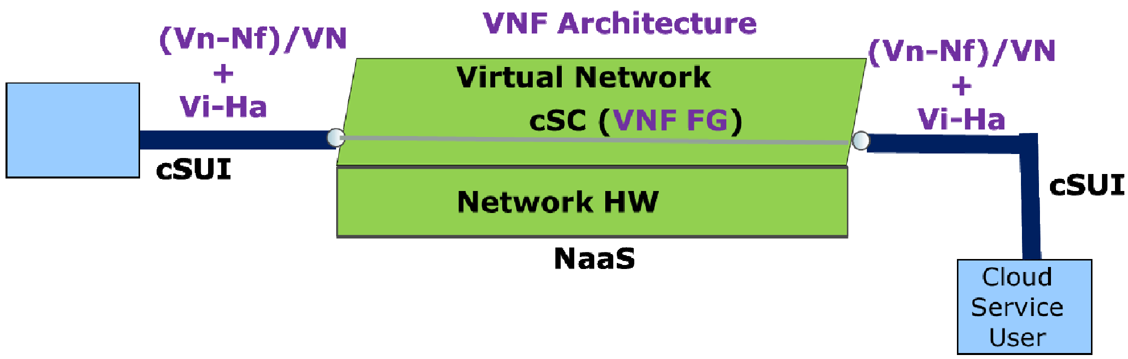


Figure 19: Cloud User Interface-NaaS architecture with NFV constructs

Cloud user access to bare metal servers over NaaS is depicted in Figure 20, using NFV constructs. As described in [1], bare metal servers can interface to NaaS using cSUI or cCcPI. We map this interface to the combination of Vi-Ha and SWA-5 since this interface can support both physical and logical components.

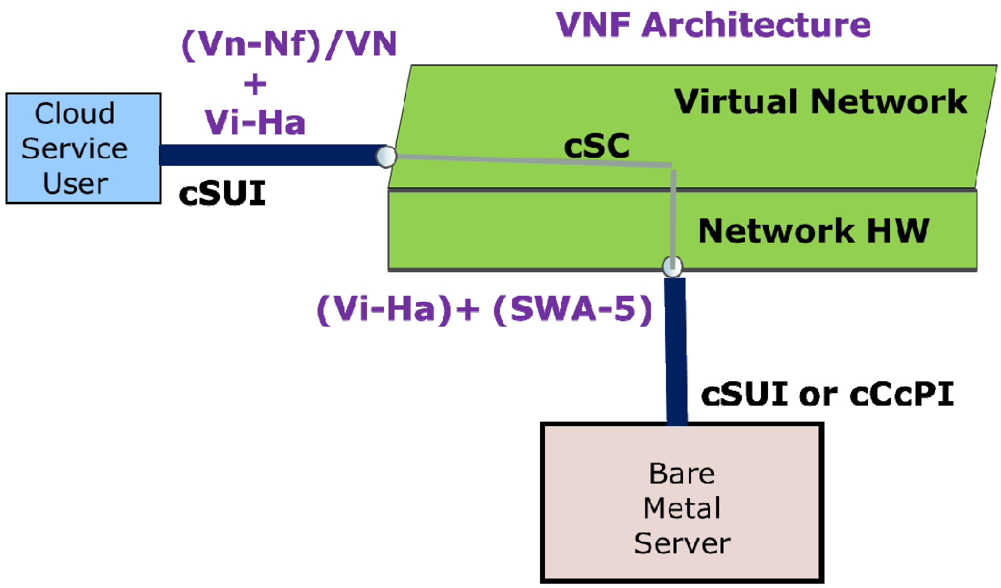


Figure 20: Bare Metal Server Interface and Naas

Cloud user access to VMs over NaaS is depicted in Figure 21, using NFV constructs. The functions of the cSI interface which is an equivalent of (Vn-NF)/VM ride over cCcPI. Although VNF forwarding may map to cSC, there is no concept of connection termination point in VNF. The End Point as depicted in [4] does not correspond to a connection termination point. The End Point is more like a device such as Customer Edge (CE) or an NE.

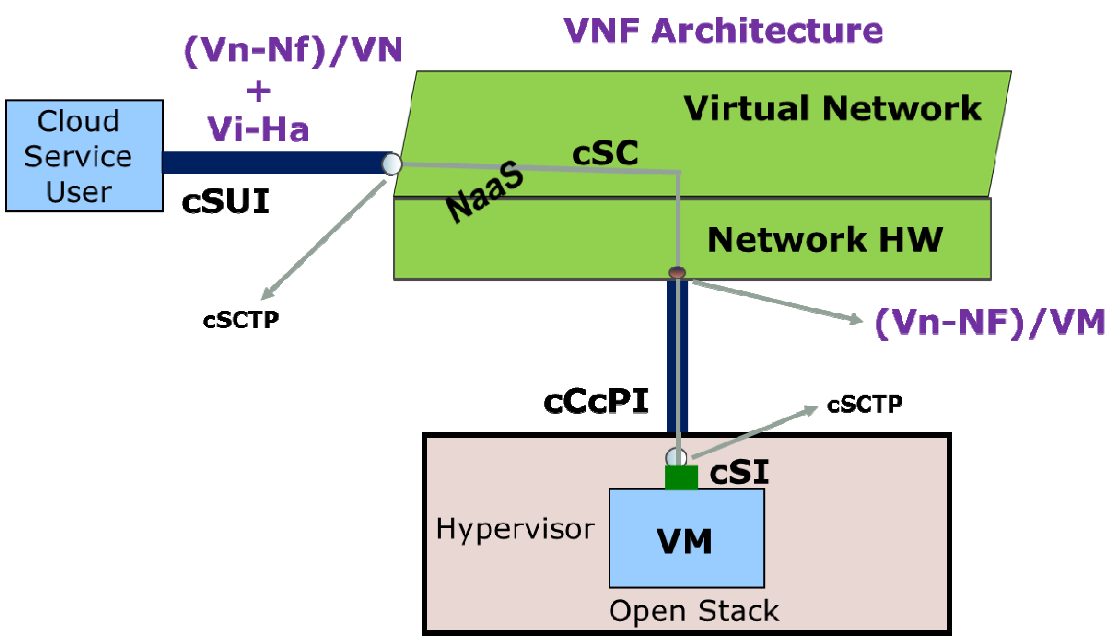


Figure 21: VM access over NaaS

6. Basic NFV Components of OCC Architecture

Neither NFV nor SDN architectures define necessary interfaces between a network and its user, between service providers, between a Cloud Provider and Cloud carrier. Furthermore they do not have connection and connection termination concepts as mentioned before. However, it is possible to build these Cloud Services components using VNFs and infrastructure components.

6.1. NFV Components of cSUI

VNF and infrastructure components of a point-to-point cSC and its cSCTPs in support of cloud services between two cSUIs are depicted in Figure 22.

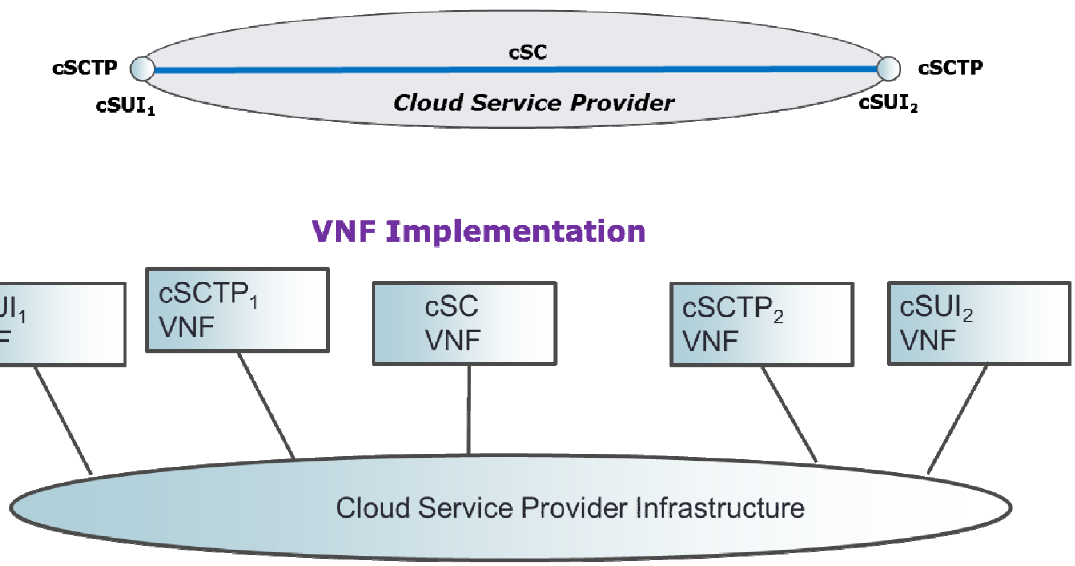


Figure 22: VNFs and Infrastructure for cSC and cSCTP

In Table 3, possible NFV and infrastructure components of cSUI are identified.

cSUI attributes	Descriptions and Recommended Values of Attributes	Component of VNF or Infrastructure or Both
cSUI Id	Arbitrary text string to identify cSUI	VNF

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].	VNF
NaaS Identifier			VNF
Physical Interface			
Ethernet if supported	speed, mode, physical medium		Infrastructure
	MAC Layer		Infrastructure
DOCSIS if supported	speed, mode, physical medium		Infrastructure
EPON if supported	speed, physical medium		Infrastructure
GPON if supported	speed, physical medium		Infrastructure
WDM if supported	speed, physical medium		Infrastructure
SONET/SDH if supported	speed, physical medium		Infrastructure
Optical Transport Network (OTN)	speed, physical medium		Infrastructure
Maximum Transmission Unit (MTU)		≥ 1522 bytes	Both
Connection Multiplexing		Yes or No	Both
Maximum number of Connection Termination Points(or End Points)			Both
L2 Ethernet configuration attributes			
MEF UNI Service attributes for Ethernet Private Services in Table 11 of MEF 6.2			VNF
MEF UNI L2CP Service Attributes for UTA in Table 18 of MEF 45			VNF
MEF UNI Service attributes in Table 4 of MEF 6.2			VNF
MEF UNI L2CP Service Attribute for vNID Case A in			VNF

Table 23 of MEF 45			
MEF UNI L2CP Service Attribute for vNID Case B in Table 26 of MEF 45			VNF
MEF UNI Service attributes for EPL in Table 7 of MEF 6.2			VNF
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EVPL in Table 10 of MEF 6.2			VNF
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EP-LAN in Table 13 of MEF 6.2			VNF
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EVP-LAN in Table 16 of MEF 6.2			VNF
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EP-Tree in Table 19 of MEF 6.2			VNF
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EVP-Tree in Table 22 of MEF 6.2			VNF
Other L2 Protocols such as Point-to-Point Protocol (PPP) and Point-to-Point Tunneling Protocol (PPTP) if supported			Both
L3 attributes if L3 protocol such as IP and/or MPLS is supported			Both
MPLS UNI attributes if MPLS is supported	LSP ID, Pseudo-wire (PW) ID, MTU, Ingress Bandwidth Profile,		Both

	Egress Bandwidth Profile, MPLS Link Down, MPLS Link Up, AIS, RDI, Lock Status		
IPv4 Address			VNF
DSCP Marking			VNF
IPv6 Address			VNF
IPv4 VPN[31]			VNF
IPv6 VPN [32]			VNF
L4 attributes if L4 protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Stream Control Transmission Protocol (SCTP) are supported			Both
L5 attributes if L5 protocols such as NFS, NetBios names, RPC and SQL are supported.			Both
L6 attributes if L6 protocols such as ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI are supported			Both
L7 attributes if L7 protocols/applications such as WWW browsers, NFS, SNMP, Telnet, HTTP, FTP are supported.			Both
Operational State		Enabled or Disabled	VNF
Admin State		Enabled or Disabled	VNF
Interface Level Security			
ACL (Access Control List) attributes			VNF
Packet Encryption	IPSec Encapsulating Security Payload (ESP) attributes		Both
	SSL VPN (Secure Sockets Layer Virtual Private Network)		Both
Connection Authentication			

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

Table 3 : VNF and Infrastructure Components of cSUI defined in [1]

6.2.NFV Components of cSC and cSCTPs

Table 4 and Table 5 identify possible NFV and infrastructure components of cSCTP and cSC.

cSCTP attributes		Descriptions and Recommended Values of Attributes	Component of VNF or Infrastructure or Both
cSCTP Id		Arbitrary text string to identify the cSCTP	VNF
cSUI Ids and cSI Ids[3]		Arbitrary string	VNF
cSC Id			VNF
Overlay Network Attributes	Virtual Access Point (VAP) Id		VNF
	NVE Interface Id	4 decimal digits	VNF
L2 Ethernet attributes			
MEF EVC per UNI Service attributes in Table 5 of MEF 6.2			Both
MEF EVC per UNI Service attributes for EPL Service in Table 8 of MEF 6.2			Both
MEF EVC per UNI Service attributes for EVPL Service in Table 11 of MEF			Both

[3] 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.

6.2			
MEF EVC per UNI Service attributes for EP-LAN Service in Table 14 of MEF 6.2			Both
MEF EVC per UNI Service attributes for EVP-LAN Service in Table 18 of MEF 6.2			Both
MEF EVC per UNI Service attributes for EP-Tree Service in Table 20 of MEF 6.2			Both
MEF EVC per UNI Service attributes for EVP-Tree Service in Table 23 of MEF 6.2			Both
MEF EPL Option 2 L2CP Processing Requirements in Table 8 of MEF 45			Both
MEF EPL Option 2 L2CP Processing Recommendations in Table 9 of MEF 45			Both
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		Both
L2 Ethernet SOAM attributes [25]			
Maintenance Entity Group (MEG) Id			VNF
Maintenance End Point (MEP) Id			VNF
MEP Level			VNF
L3 attributes if interface is L3			
IPv4 Subnet Address			VNF
IPv6 Subnet Address			VNF
DSCP Mapping			VNF
Bandwidth Profile	CIR		Both
	CBS		Both
	EIR		Both
	EBS		Both
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		Both
LSP Label			VNF

EXP Mapping			VNF
Operational State		Enabled or Disabled	Infrastructure
Administrative State		Enabled or Disabled	VNF
cSCTP Level Security			
Packet encryption	IPSec ESP		VNF
	SSL VPN		VNF
Connection Authentication	IPSec AH		VNF
	TCP-AO		VNF
Data confidentiality/privacy	Logical separation of cSTPs, limiting DoS and excessive resource consumption via rate limiting		Both
Service Level Security	Rate limiting of DoS attacks and excessive resource consumption		Infrastructure

Table 4 : VNF and Infrastructure Components of of cScTP defined in [1]

cSC attributes		Descriptions and recommended values of attributes	Component of VNF or Infrastructure or Both
cSC Id		Arbitrary text string to identify the cSC	VNF
List of associated cSCTP Ids[4]			VNF
Overlay Network Attributes	VNI ID	•	VNF
Type	Point-to-Point		VNF
	Point-to-Multipoint		VNF
	Multipoint-to-Multipoint		VNF
Protection	1:1 or 1+1	cSC needs to be protected for path protection	VNF
L2 Ethernet connection attributes [71,47]			
MEF EVC Service attributes in Table 6 of MEF 6.2			Both
MEF EVC Service attributes of EPL in Table 9 of MEF 6.2			Both
MEF EVC Service attributes of EVPL in Table 12 of			Both

[4] 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..

MEF 6.2			
MEF EVC Service attributes of EP-LAN in Table 15 of MEF 6.2			Both
MEF EVC Service attributes of EVP-LAN in Table 18 of MEF 6.2			Both
MEF EVC Service attributes of EP-Tree in Table 21 of MEF 6.2			Both
MEF EVC Service attributes of EVP-Tree in Table 24 of MEF 6.2			Both
MEF EVC Perfromance attributes and Parameters per CoS in Table 25 of MEF 6.2			Both
L3 connection attributes (if supported)	Service Level Objectives (SLOs)	Delay, jitter, loss	Both
	MTU		Both
	Type	Point-to-Point, Multipoint-to-Multipoint, Rooted Multipoint	VNF
Connection Start Time		Specified in seconds in Coordinated Universal Time (UTC).	VNF
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	VNF
Connection Duration		Specified in days, minutes or seconds.	VNF
Connection Period		Specified in daily, weekly or monthly	VNF
Operational State		Enabled or Disabled	Infrastructure
Administrative State		Enabled or Disabled	VNF
Billing Options	Monthly, Hourly		VNF

Table 5 : VNF and Infrastructure Components of cSC defined in [1]

6.3. NFV Components of cSI

VNF and infrastructure components of a point-to-point cSC and its cSCTPs in support of cloud services between a cSUI and a cSI are depicted in Figure 23.

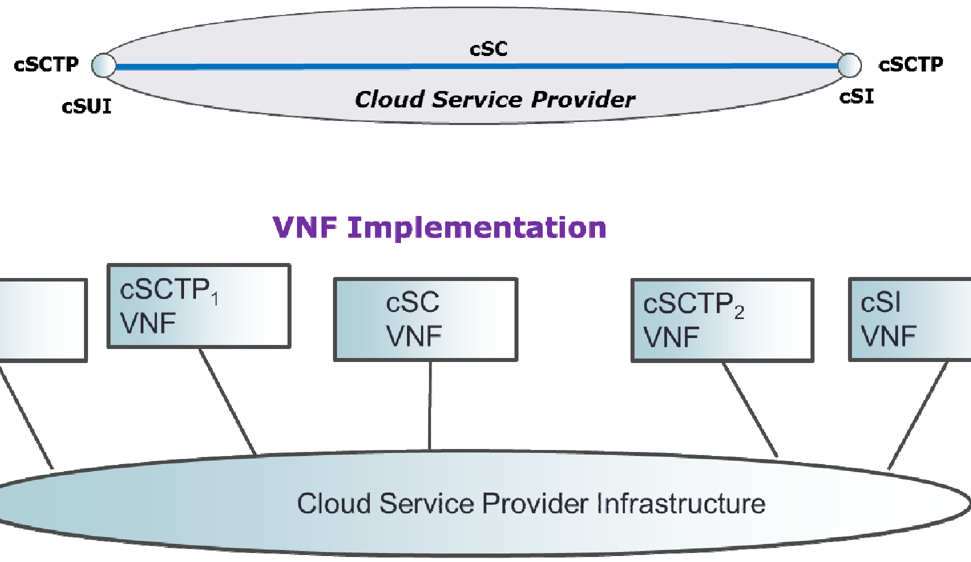


Figure 23: VNF and Infrastructure Components of cSC between cSUI and cSI

Table 6 identifies possible NFV and infrastructure components of cSI.

cSI attributes	Descriptions and Recommended Values of Attribute	Component of VNF or Infrastructure or Both
cSI Id	Arbitrary text string to identify cSI	VNF
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.	VNF
List of NaaS	List of NaaS employing this VM or server (i.e. application entity is shared or dedicated)	VNF
Interface Protection	1+1 or 1:1 or None	
Connection Multiplexing	Yes or No	
Maximum number of Connection Termination Points		Both
L2 Ethernet configuration attributes[17, 71, 66]		
MEF UNI Service attributes in Table 4 of MEF 6.2		Both
MEF UNI Service attrib-		Both

utes for EPL in Table 7 of MEF 6.2			
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EVPL in Table 10 of MEF 6.2			Both
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EP-LAN in Table 13 of MEF 6.2			Both
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EVP-LAN in Table 16 of MEF 6.2			Both
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EP-Tree in Table 19 of MEF 6.2			Both
MEF UNI Service attributes in Table 4 of MEF 6.2 MEF UNI Service attributes for EVP-Tree in Table 22 of MEF 6.2			Both
Other L2 Protocols such as Point-to-Point Protocol (PPP) and Point-to-Point Tunneling Protocol (PPTP) if supported			Both
VM Protection (if supported)	This would be redundant VM or redundant server or redundant resource offering the service		Both

VM Portability[5]		Yes or No	VNF
L3 attributes if L3 protocol such as IP and MPLS are supported			
MPLS UNI attributes [49] if MPLS is supported	LSP ID, PW ID, MTU, Ingress Bandwidth Profile, Egress Bandwidth Profile, MPLS Link Down, MPLS Link Up, AIS, RDI, Lock Status		Both
IPv4 Address			VNF
DSCP Marking			Infrastructure
IPv6 Address			VNF
IPv4 VPN			VNF
IPv6 VPN			VNF
NAT			VNF
L4 attributes if L4 protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and Stream Control Transmission Protocol (SCTP) are supported			VNF
General Ports	32111 (TCP)		VNF
	9427 (TCP)		VNF
PCoIP (PC over IP) Ports	50002(TCP/UDP)		VNF
	4172 (TCP/UDP)		VNF
RDP (Remote Desktop Protocol) Ports	3389 (TCP)		VNF
Connection server Ports	4001 (TCP)		VNF
L5 attributes if L5 protocols such as NFS, NetBios names, RPC and SQL are supported.			VNF
L6 attributes if L6 protocols such as ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI are supported			VNF
L7 attributes if L7 protocols/applications such as WWW browsers, NFS, SNMP, Telnet, HTTP, FTP are supported.			VNF
Operational State		Enabled or Disabled	Infrastructure
Admin State		Enabled or Disabled	VNF
Security			

[5] 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).

SSL (Secure Socket Layer) Termination	Terminating SSL traffic for services such as load balancer		VNF
ACL			VNF
Packet encryption	IPSec ESP (Encapsulating Security Payload)		Both
	SSL VPN		VNF
Connection Authentication	IPSec AH		VNF
	TCP-AO		VNF
Service Level Security	Rate limiting of DoS attacks and excessive resource consumption		Both
Data confidentiality/privacy	Prevent tenants from eavesdropping on each other via logical separation		VNF
Session Layer Security	REST API (Representational State Transfer Application Programming Interface) over SSL (Secure Sockets Layer) /TLS (Transport Layer Security)		VNF
	API keys		VNF
Billing	Recurring Charges		VNF
	Non-recurring Charges		VNF

Table 6 : VNF and Infrastructure Components of cSI defined in [1]

6.4.NFV Components of cSC Crossing two cSPs

VNF and infrastructure components of a point-to-point cSC crossing two cSPs and its cSCTPs in support of cloud services between two cSUIs are depicted in Figure 24.

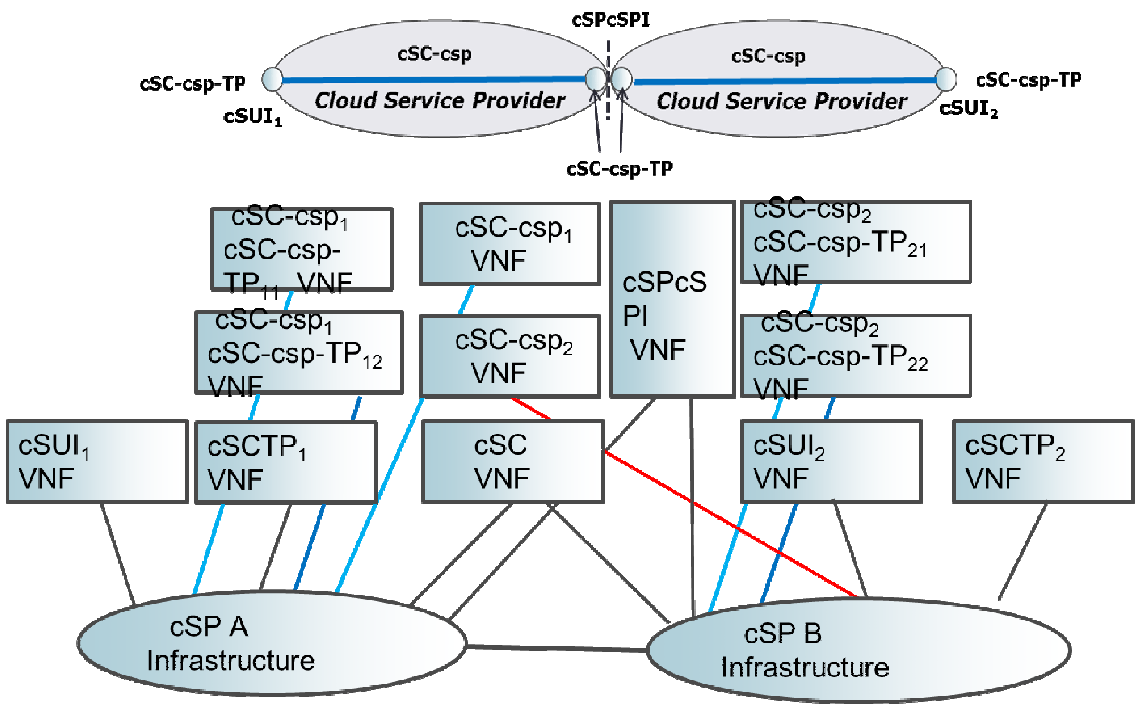


Figure 24: VNFs for cSC-csp and cSC-csp-TP

Table 7 identifies possible NFV and infrastructure components of cSPcSPI.

cSPcSPI attributes		Descriptions and Recommended Attribute Values	Component of VNF or Infrastructure or Both
cSPcSPI Id		Arbitrary text string to identify the cSPcSPI	VNF
Name of cSPs interfacing each other		Arbitrary text string to identify the cSP	VNF
Physical Interface			
L2 Ethernet			Infrastructure
	speed, mode, physical medium		
	MAC Layer		Infrastructure
DOCSIS if supported	speed, physical medium		Infrastructure
EPON if supported	speed, physical medium		Infrastructure
GPON if supported	speed, physical medium		Infrastructure

WDM if supported	speed, physical medium		Infrastructure
SONET/SDH if supported	speed, physical medium		Infrastructure
Optical Transport Network (OTN)			Infrastructure
MTU		$\geq$ 1522 bytes	Both
Connection Multiplexing		Yes or No	VNF
Maximum number of Connection Termination Points (or End Points)			VNF
L2 Ethernet configuration attributes[20,22]			
MEF ENNI Service attributes in Table 2 of MEF 26.1			Both
MEF ENNI L2CP Service Attributes for Access EPL in Table 17 of MEF 45			Both
MEF ENNI L2CP Service Attributes for UTA in Table 20 of MEF 45			Both
MEF ENNI L2CP Service Attributes for vNID Case A in Table 25 of MEF 45			Both
MEF ENNI L2CP Service Attributes for vNID Case B in Table 28 of MEF 45			Both
L2 Ethernet SOAM attributes [25]			
Maintenance Entity Group (MEG) Id			VNF
Maintenance End Point (MEP) Id			VNF
MEP Level			VNF
Maintenance Intermediate Point (MIP) Id			VNF
LAG MEG			Both
LAG Link MEG			VNF
Operator MEG			VNF
Other L2 Protocols such as Point-to-Point Protocol (PPP) and Point-to-Point Tunneling Protocol (PPTP) if supported			Both
L3 attributes if L3 protocol such as IP and MPLS are supported			
MPLS UNI attributes if MPLS is suported	LSP ID, PW ID, MTU, Ingress Bandwidth Profile, Egress Bandwidth Profile, MPLS Link Down, MPLS Link Up, AIS,		Both

	RDI, Lock Status		
Fast Reroute			Both
NAT			VNF
IPv4 Subnet Address			VNF
IPv6 Subnet Address			VNF
DSCP Marking			Infrastructure
IPv4 VPN [31]			VNF
IPv6 VPN [32]			VNF
Security between cSPs (if supported)			
ACL			VNF
Packet encryption	IPSec ESP		Both
	SSL VPN		VNF
Connection Authentication	IPSec AH		VNF
Service Level Security	Rate limiting of DoS attacks and excessive re-source consump-tion		Both

Table 7 : VNF and Infrastructure Components of cSPcSPI defined in [1]

Table 8 identifies possible NFV and infrastructure components of cSC-csp-TP.

cSC-csp-TP attributes		Descriptions and Recommended Val-ues of Attributes	Component of VNF or Infra-structure or Both
cSC-csp-TP Id		Arbitrary text string to identify the cSC-csp-TP	VNF
cCScSPI Ids			VNF
Overlay Network Attributes	Virtual Access Point (VAP) Id		VNF
	NVE Interface Id	4 decimal digits	VNF
L2 Ethernet attributes			
MEF OVC End Point per ENNI Ser-vice Attributes in Table 17 of MEF 26.1			Both
MEF OVC End Point per UNI Service Attrib-utes in Table 18 of MEF 26.1			Both
MEF OVC L2CP Service Attributes for Access EVPL in Table 13 of MEF 45			Both
MEF OVC L2CP Service Attributes for Access EPL in Table 16 of MEF 45			Both

MEF OVC L2CP Service Attributes for UTA in Table 19 of MEF 45			Both
MEF OVC L2CP Service Attributes for vNID Case A in Table 24 of MEF 45			Both
OVC L2CP Service Attributes for vNID Case B in Table 27 of MEF 45			Both
Protection (via redundant cSC-csp-TP on a different port of the same cSPcSPI Gateway	1:1or 1+1		Both
MEF OVC End Point per ENNI Ser-vice Attributes in Table 17 of MEF 26.1			Both
MEF OVC End Point per UNI Service Attrib-utes in Table 18 of MEF 26.1			Both
L2 Ethernet SOAM attributes [25]			VNF
Maintenance Entity Group (MEG) Id			VNF
Maintenance End Point (MEP) Id			
MEP Level			
Maximum Number of MEPs			VNF
Maintenance Intermediate Point (MIP) Id			VNF
L3 attributes if interface is L3			
IPv4 Subnet Address			VNF
IPv6 Subnet Address			VNF
DSCP Mapping			Both
Bandwidth Profile	CIR		Both
	CBS		Both
	EIR		Both
	EBS		Both
Protection (via redundant cSCTP on a different port of the same cSPcSPI Gateway	1:1or 1+1		Both
LSP Label			
EXP Mapping			
Operational State		Enabled or Disabled	
Administrative State		Enabled or Disabled	VNF
cSC-csp-TP Level Security			
Packet encryption	IPSec ESP		VNF
	SSL VPN		VNF
Connection Authentication	IPSec AH		VNF
	TCP-AO		VNF
Service Level Security	Rate limiting of DoS attacks and		VNF

	limiting excessive resource consumption		
Data confidentiality/privacy	Preventing eavesdropping between cSC-csp-TPs via logical separation.		Infrastructure

Table 8 : VNF and Infrastructure Components of cSC-csp-TP defined in [1]

7. Summary of Software-Defined Networking (SDN) Architecture

Software-Defined Networking (SDN) is defined by ONF as an emerging architecture that is dynamic, manageable, cost-effective, and adaptable [10]. This architecture decouples the network control and forwarding functions (Figure 25) enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.

Abstracting the control plane from the network elements allows network-platform-specific characteristics and differences that do not affect services to be hidden. In addition, applications can request needed resources from the network via interfaces to the control plane.

ITU keeps the ONF layer separation and adds orchestration between application layer and control layer as depicted in Figure 26 to provide automated control and management of network resources and coordination of requests from the application layer [11].

IETF also keeps the ONF layer separation (Figure 27) and adds a management plane which is responsible for monitoring, configuring, and maintaining network devices, in parallel to control plane.

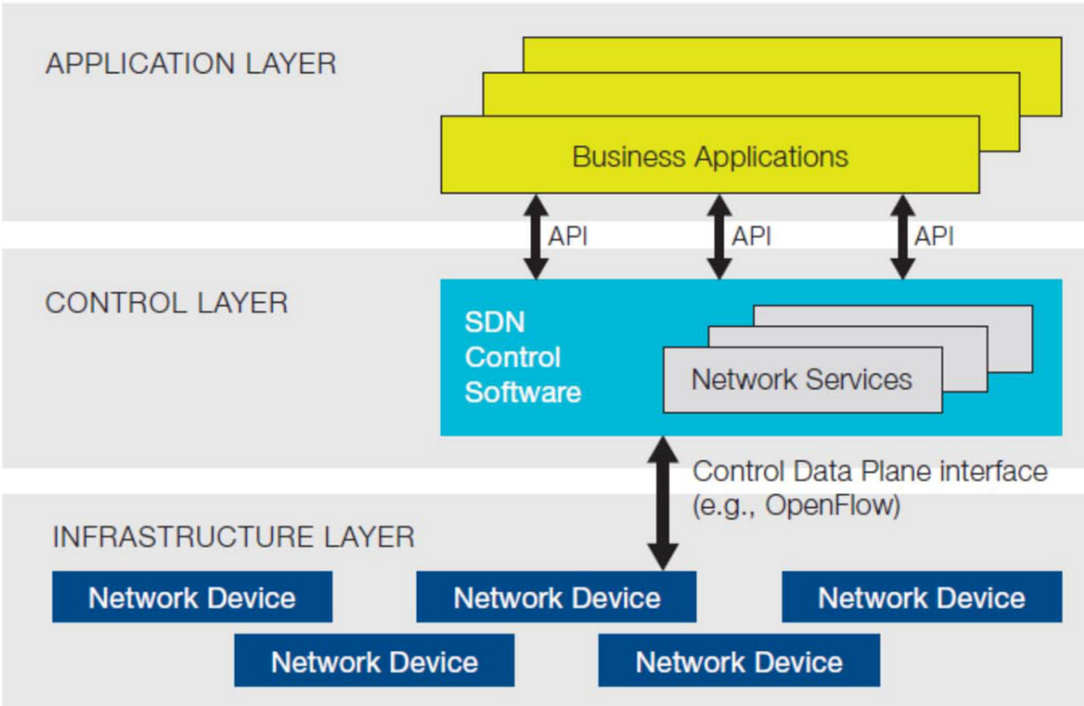


Figure 25: ONF SDN Architecture [10]

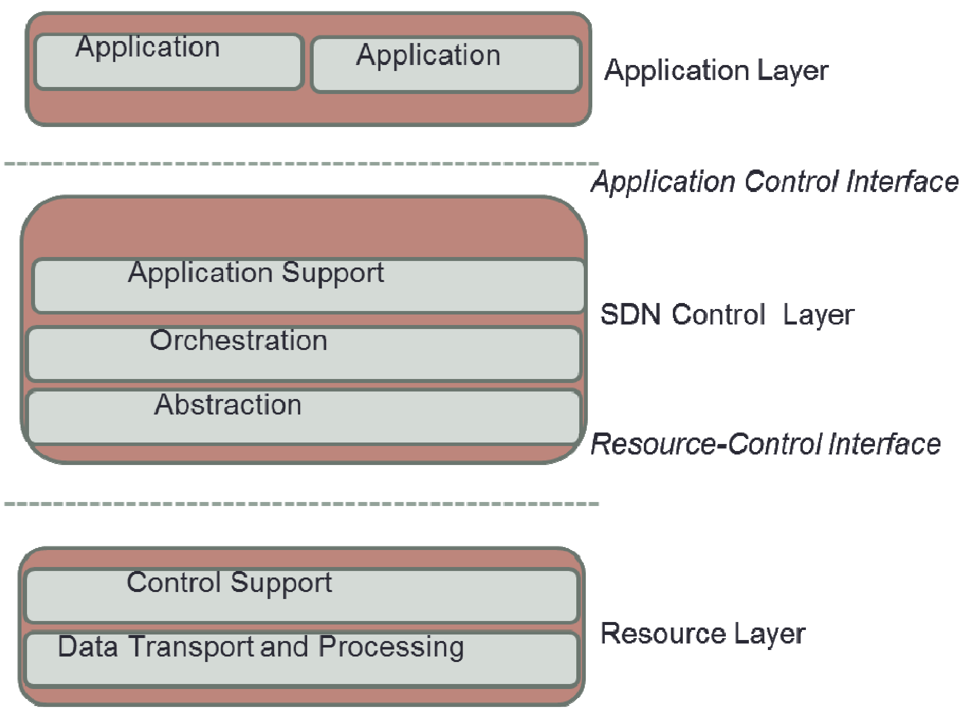


Figure 26: ITU SDN Architecture [11]

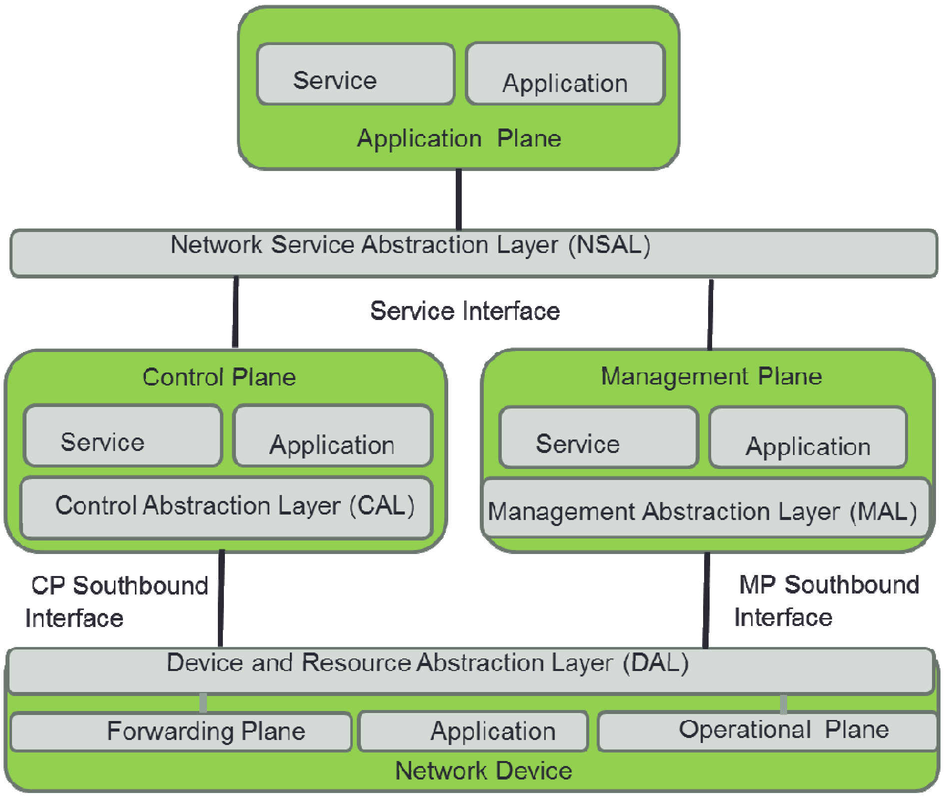


Figure 27: IETF SDN Architecture [12]

SDN building blocks are summarized in Figure 28. The application layer sits on top of services layers. The services layer interacts with an orchestrator which can interact with multiple controllers via a north bound API. The north bound interface between applications/services allows the applications to authenticate and learn of which objects they have authorization to manipulate, or to interact with objects belonging to controlling software. The SDN Orchestrator requests object models from each of the controlling software which is responsible for managing and manipulating them. The Southbound API provides abstraction for the controller to manage the devices in its domain.

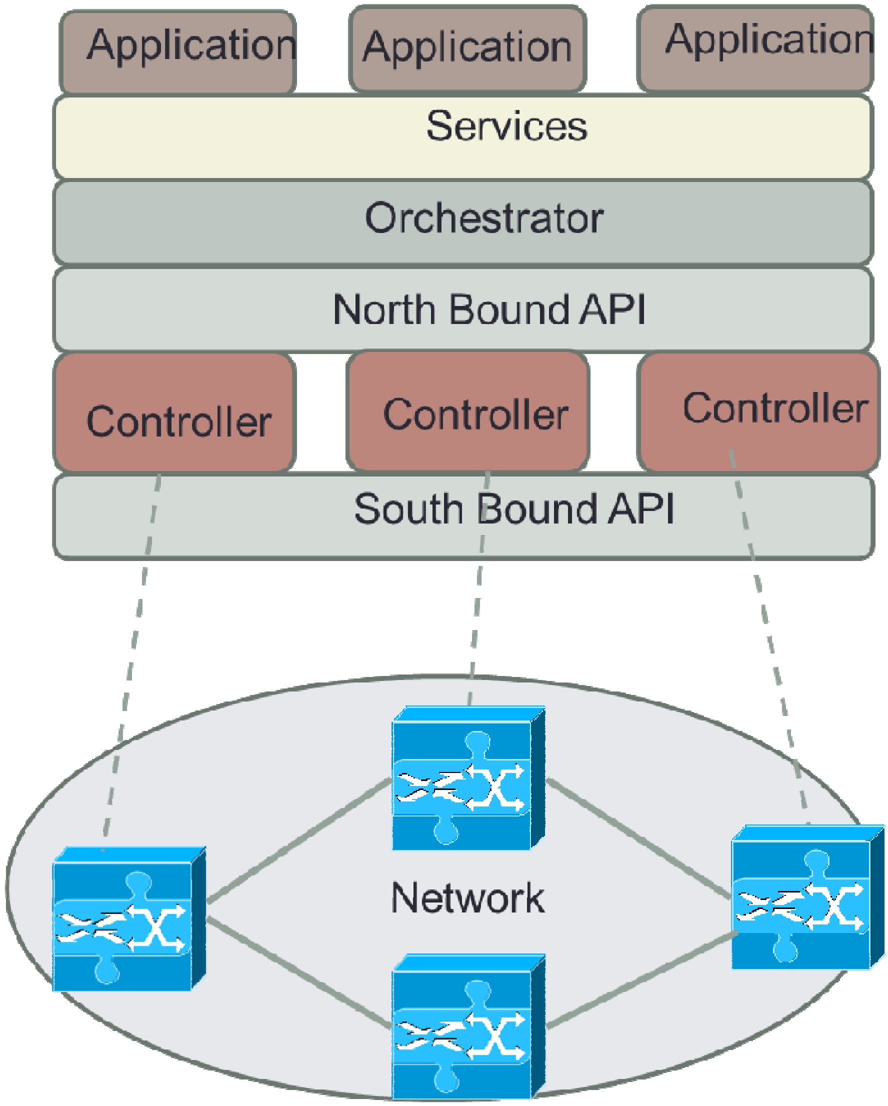


Figure 28: SDN Building Blocks [7]

8. OCC Management Architecture Basic Blocks

A high level management architecture is depicted in Figure 29 and Figure 30. Applications are expected to be mapped to services via a Cloud Services Catalog. For example, a voice call application between two users can be mapped to an Ethernet Virtual Private Line (EVPL) in H category [8]. Cloud Orchestrator configures the EVPL between two users by translating this request to appropriate commands to NFV Orchestrator and Controllers via “North Bound API”. The NFV Orchestrator is expected to perform service chaining of VNFs and infrastructure components associated with virtualized Network Elements (NEs) while Controllers automate provisioning of non-virtualized components of the network. It is possible to have non-SDN NEs in the network. They will be managed by Element Management Systems (EMSs).

The Cloud Orchestrator may perform Life Cycle Service Orchestration (LSO) as described in [9] for each service ordered and provisioned via User Portal and Operation Support System/Billing Support System (OSS/BSS). Some of the LSO functionalities are as depicted in Figure 31:

- Market Analysis and Product Strategy
- Service and Resource Design
- Launch products
- Marketing Fulfillment Response
- Sale Proposal and Feasibility
- Capture Customer Order
- Service Configuration & Activation
- End-to-End Service Testing
- Service Problem Management
- Service Quality Management
- Billing and Revenue Management
- Terminate Customer Relationship

In Figure 29, a Cloud Orchestrator performs Life Cycle Orchestration for Cloud services by a Cloud Service Operator. On the other hand, in Figure 30 where multiple operators are involved in providing cloud services, multiple Cloud Orchestrators might perform Life Cycle Orchestration. In this case, a Cloud Orchestrator of the Cloud Service Provider which is responsible from the end-to-end service [1] is expected to perform Life Cycle Orchestration end-to-end.

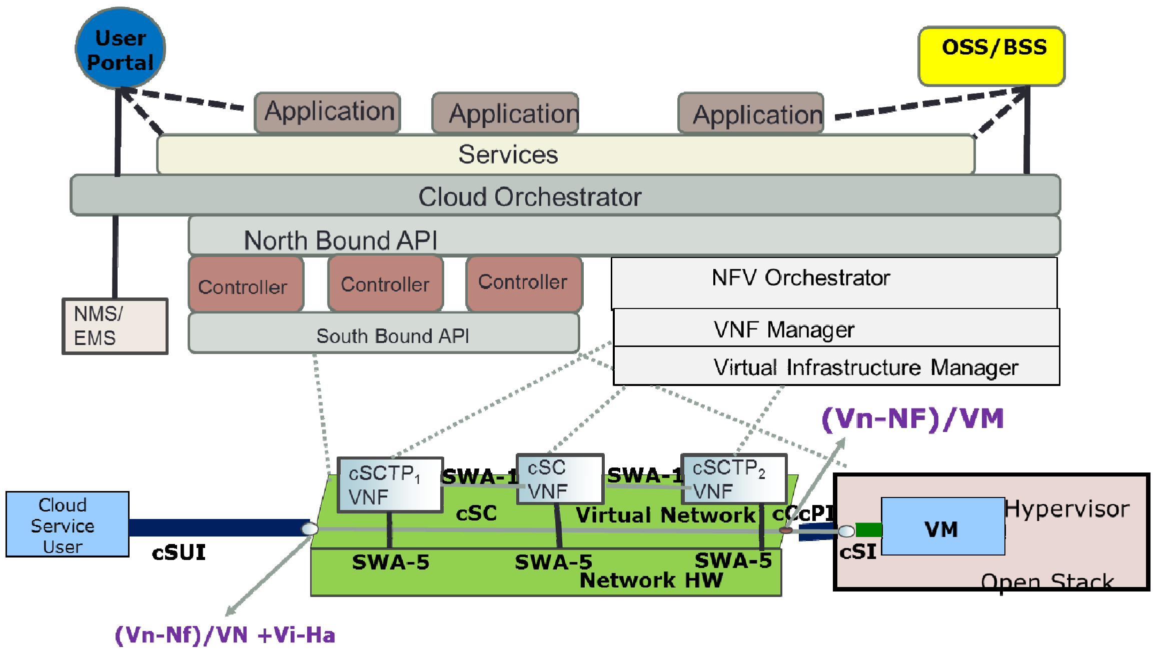


Figure 29: Cloud Services Management with Life Cycle Orchestration

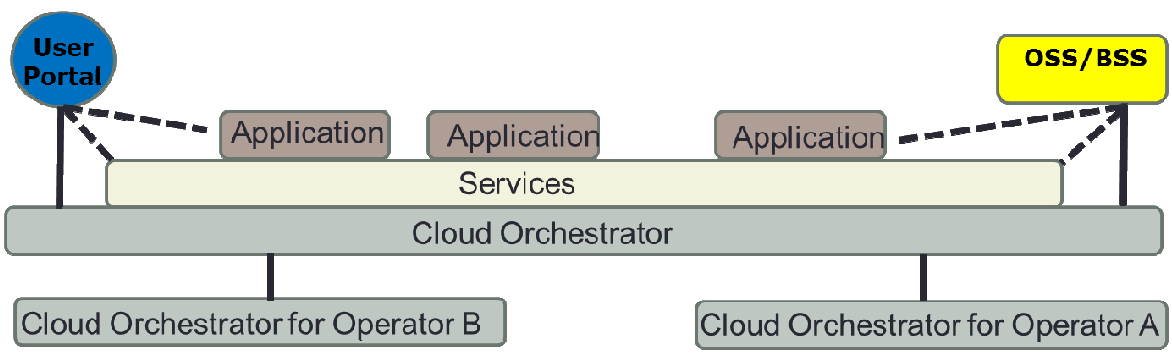


Figure 30: Management of Cloud Services provided by multiple Cloud Service Operators

The management architectures and distribution of management functionalities among layers in Figure 29 and Figure 30 are examples. Further architectural details need to be worked.

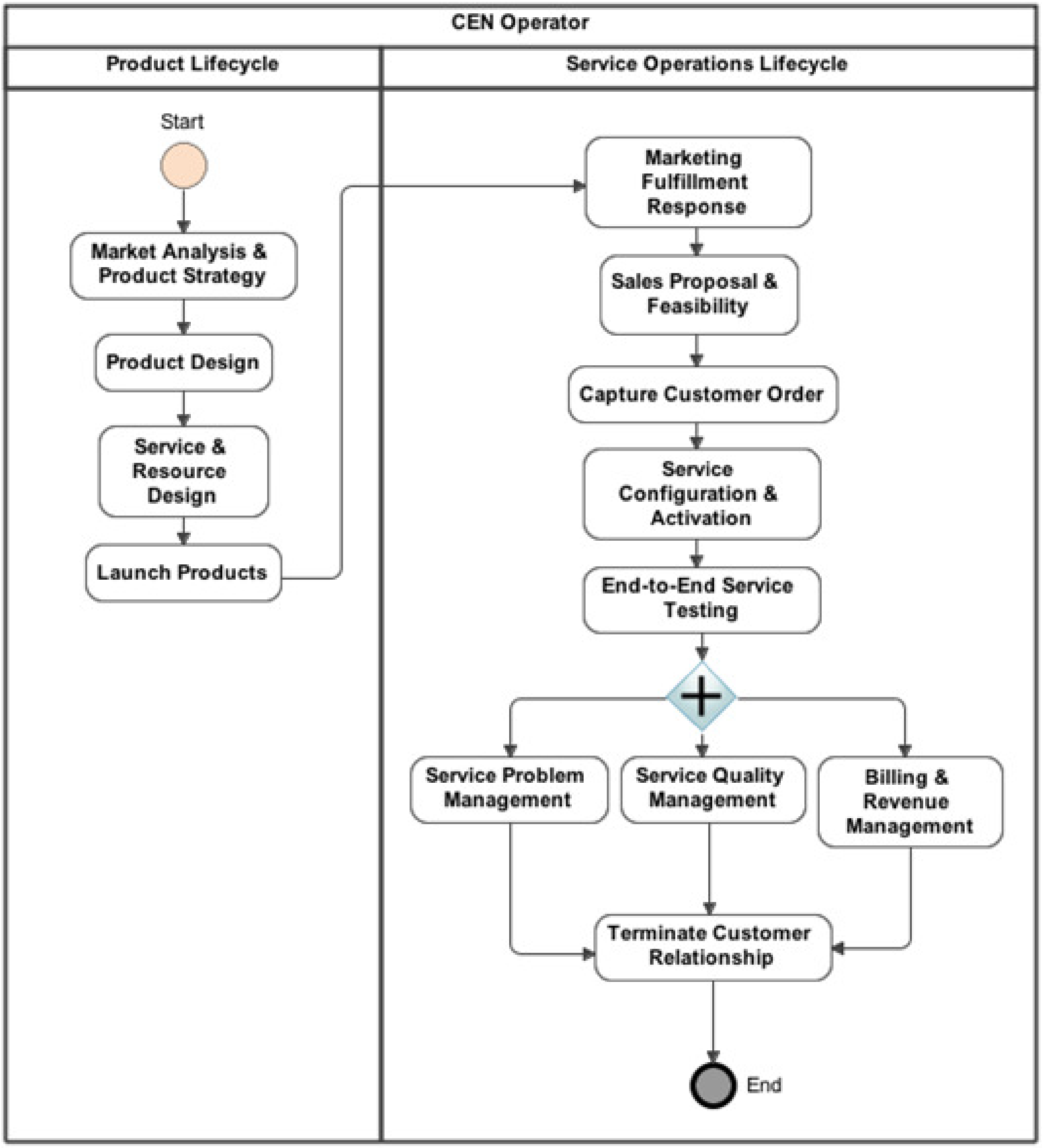


Figure 31: Product and Service Operations Lifecycle Stages [9]

References

[1] OCC, “OCC 1.0 Reference Architecture”, December, 2014.

[2] Draft ETSI GS NFV-INF V0.3.1 (2014-05), “Network Functions Virtualisation; Infrastructure Architecture; Architecture of the Hypervisor Domain”

[3] DGS NFV-INF003 V0.34 (2014-11-18), “Network Functions Virtualisation; Part 1:Infrastructure Architecture; Sub-Part 3: Architecture of Compute Domain”

[4] Draft ETSI GS NFV-INF 001 V0.3.12 (2014-11), “Network Functions Virtualisation; Infrastructure Overview”
[5] Draft ETSI GS NFV-SWA 001 v0.2.4 (2014-11), “Network Functions Virtualisation; Virtual Network Functions Architecture”
[6] ETSI GS NFV-MAN 001 v1.1.1 (2014-12), Network Functions Virtualisation (NFV); Management and Orchestration
[7] M. Toy. “Cable Networks, Services and Management”, J. Wiley-IEEE Press, 2015.
[8] MEF 23.1, Carrier Ethernet Class of Service – Phase 2, January 2012.
[9] MEF 50, Carrier Ethernet Service Lifecycle Process Model, December 2014.
[10] ONF (Open Networking Foundation), “Software-Defined Networking: The New Norm for Networks”, ONF White Paper, April 13, 2012.
[11] ITU-Y Y.3300, “Framework of software-defined networking”, 6/2014.
[12] RFC7426, “Software-Defined Networking (SDN): Layers and Architecture Terminology”, Januray 2015.
[13] National Institute of Standards and Technologies (NIST) Special Publication 500-291, NIST Cloud Computing Roadmap, July 2013
[14] MEF 10.3 Ethernet Services Attributes Phase 3, October 2013.
[15] 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.
[16] MEF 4 Metro Ethernet Network Architecture Framework Part 1: Generic Framework, May 2004.
[17] RFC2474, K. Nichols, et al., Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
[18] 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.
[19] MEF 6.2 Ethernet Service Definitions Phase 3, August 2014.
[20] MEF 23.1 Class of Service Phase 2 Implementation Agreement
[21] MEF 50, Carrier Ethernet Service Lifecycle Process Model, December 2014.
[22] MEF 23.1, Class of Service Phase 2 Implementation Agreement, January 2012.
[23] RFC 792, INTERNET CONTROL MESSAGE PROTOCOL, September 1981.
[24] RFC 4303, IP Encapsulating Security Payload (ESP), December 2005.
[25] RFC 6690, Constrained RESTful Environments (CoRE) Link Format, August 2012.
[26] RFC 5925, The TCP Authentication Option, June 2010.
[27] RFC 793, TRANSMISSION CONTROL PROTOCOL, September 1981.
[28] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008.
[29] RFC 3031, Multiprotocol Label Switching Architecture, January 2001.
[30] GS NFVINF 0007 v0.3.1 (2013-11-15), Network Function Virtualisation Infrastructure Architecture: Interfaces and Abstractions.
[31] RFC 4447, Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP), April 2006