Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: October 11, 2015

B. Khasnabish
ZTE (TX) Inc.
J. Chu
S. Ma
ZTE
N. So
Vinci Systems
P. Unbehagen
Avaya
M. Morrow
Cisco Sys. GmbH
M. Hasan
Cisco Systems
Y. Demchenko
Univ. of Amsterdam
Y. Meng
.

April 9, 2015

Cloud Reference Framework
draft-khasnabish-cloud-reference-framework-08.txt

Abstract

This document presents a cloud reference framework that intends to provide a basis for designing interoperable cloud services and their integration into existing open Internet and enterprise IT infrastructures.

In general, a cloud-based system utilizes virtualized computing / communications / storage resources and applications, and allows their combined provisioning as complex infrastructure services. In the emerging cloud-based virtualized infrastructures and services are provisioned on on-demand basis, and configured for specific customer needs or tasks.

The reference framework is based on the survey of the SDOs and WGs that are focusing on cloud-based systems and services (Cloud SDO, I-D.Khasnabish-cloud-sdo-survey), on-going standardisation activities and other research and developments in the cloud computing technology area. Both intra-cloud and inter-cloud reference frameworks are presented and the requirements to the general functional layers and components are discussed.

Status of this Memo

This Internet-Draft is submitted in full conformance with the

provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 11, 2015.

Copyright Notice

Table of Contents

1. Introduction

Clouds are emerging as a common way of provisioning virtualized infrastructure services that are provisioned on demand (and configured for specific customer needs or tasks). Current development of the cloud technologies demonstrate movement to developing Intercloud models, architectures and integration tools that could allow integrating cloud based infrastructure services into existing enterprise and campus infrastructures, on one hand, and provide common/interoperable environment for moving existing infrastructures and infrastructure services to virtualized cloud environment. More complex and enterprise oriented use of cloud infrastructure services will require developing new service provisioning and security models that could allow creating complex project and group oriented infrastructures provisioned on-demand and across multiple providers.

This document presents a general cloud reference framework that includes the proposed multilayer Cloud Services Model (CSM), including cross-layer functions such as Cloud Management Plane, and defines the Intercloud framework to address interoperability and integration issues in provisioning multi-domain multi-provider heterogeneous cloud based infrastructures and services.

The proposed CSM defines the basic functional layers to support the cloud based infrastructure services and applications virtualization, composition, delivery and operation. The CSM provides a basis for building Cloud Service Provider (CSP) internal infrastructure (or datacenter) that could also address inter-provider interoperability and cloud based services integration.

The proposed Intercloud Architecture Framework ICAF addresses a number of issues in ensuring interoperability of cloud infrastructures built using different cloud software stacks/platforms and provided by multiple providers. It should address Intercloud service control and management (under one cloud operator or integrator), Intercloud federation that should allow interoperability and integration of administratively independent cloud domains, and general inter-cloud services provisioning and operation.

The proposed in this document Intercloud Framework intends to provide a basis for inter-cloud infrastructures and services integration and interoperability that could span multiple providers, multiple management domains and include mutli-platform and multi-technology components/domains. The definition of the Intercloud Framework is based on previous experience of Internet community in building large scale interoperable telecommunication and Internet systems and uses best practices and recommendations from the wide range of industry

standards by IETF, OGF, ITU-T, TMF, DMTF and other standardisation bodies specifically oriented on cloud technologies.

The presented Cloud Reference Framework can be used to a) define requirements to the main cloud infrastructure functional elements and other components of the general Internet infrastructure to consistently support cloud services/infrastructure integration and operation, b) define the interfaces between the functional elements, and c) propose further standardisation.

It is important to mention that consistent definition of the general Cloud Services Model will provide a basis for seamless inter-cloud integration and operation.

The proposed cloud reference framework describes basic functions in different layers to support the virtualized applications and services interoperability, integration and operation. This reference framework can be used to standardize a) features of functional elements and b) the interfaces between the functions.

Basically, the cloud reference framework includes

- the following horizontal layers
  - User/Customer Side Services/Functions and Resources Layer(USL)
  - Access/Delivery Layer (ADL) hosting also Inter-Cloud functions
  - Cloud Service Layer(CSL)
  - Resource Control (Composition and Orchestration) Layer(RCL)
  - Resource Abstract and Virtualization Layer(RAVL)
  - Physical Resource Layer(PRL)
- Cross-layer functions including
  - Cloud Management Plane that supports the following functionality
    - Configuration management
    - Services registry and discovery
    - Monitoring, logging, accounting and auditing

+ Service Level Agreement (SLA) management (SLAM)

+ Security services and infrastructure management

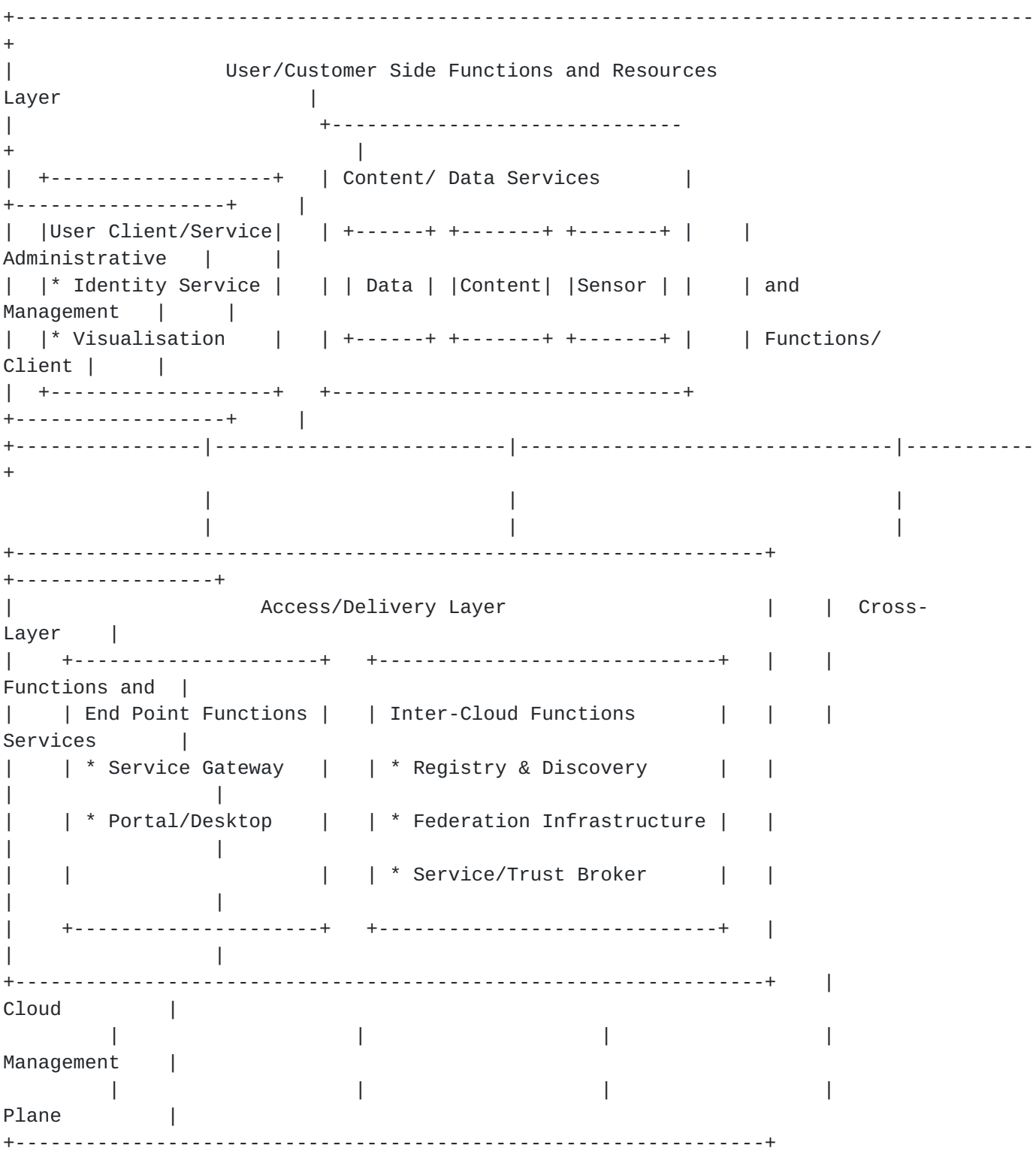
The Cloud Security Services Infrastructure works as another cross-layer service which task is to ensure normal operation of the cloud services, protect user data, and enforce security, access control (authentication and authorisation) and operational policies at all layers of the cloud services model. In clouds, security services also need to be provisioned on-demand together with the provisioned on-demand main cloud services. In this respect cloud security infrastructure should support consistent security context and security sessions management during the whole lifecycle of the provisioned cloud services. To perform this function it will use the services lifecycle management service as a part of the Cloud Management Plane functionality.

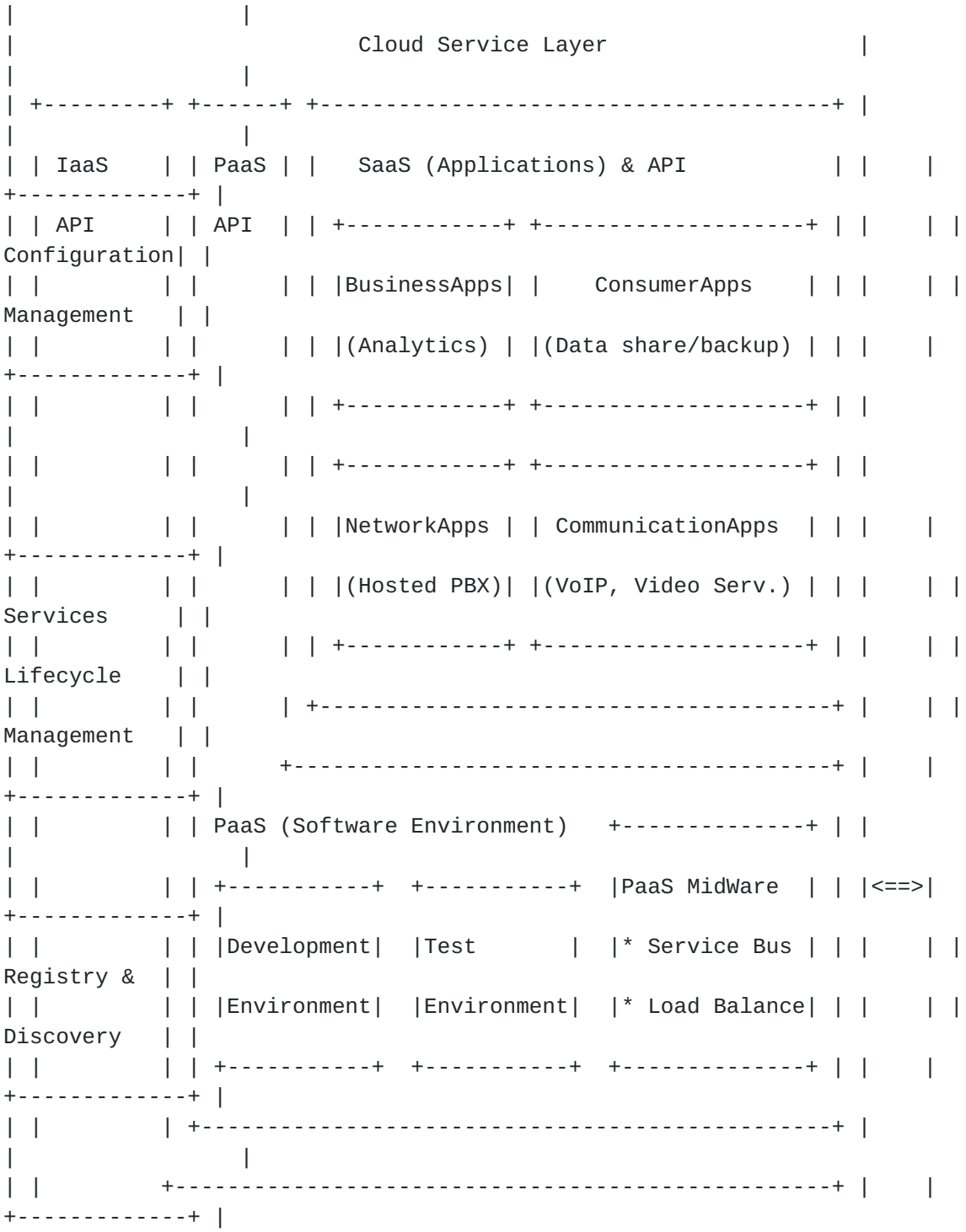
2. Terminology

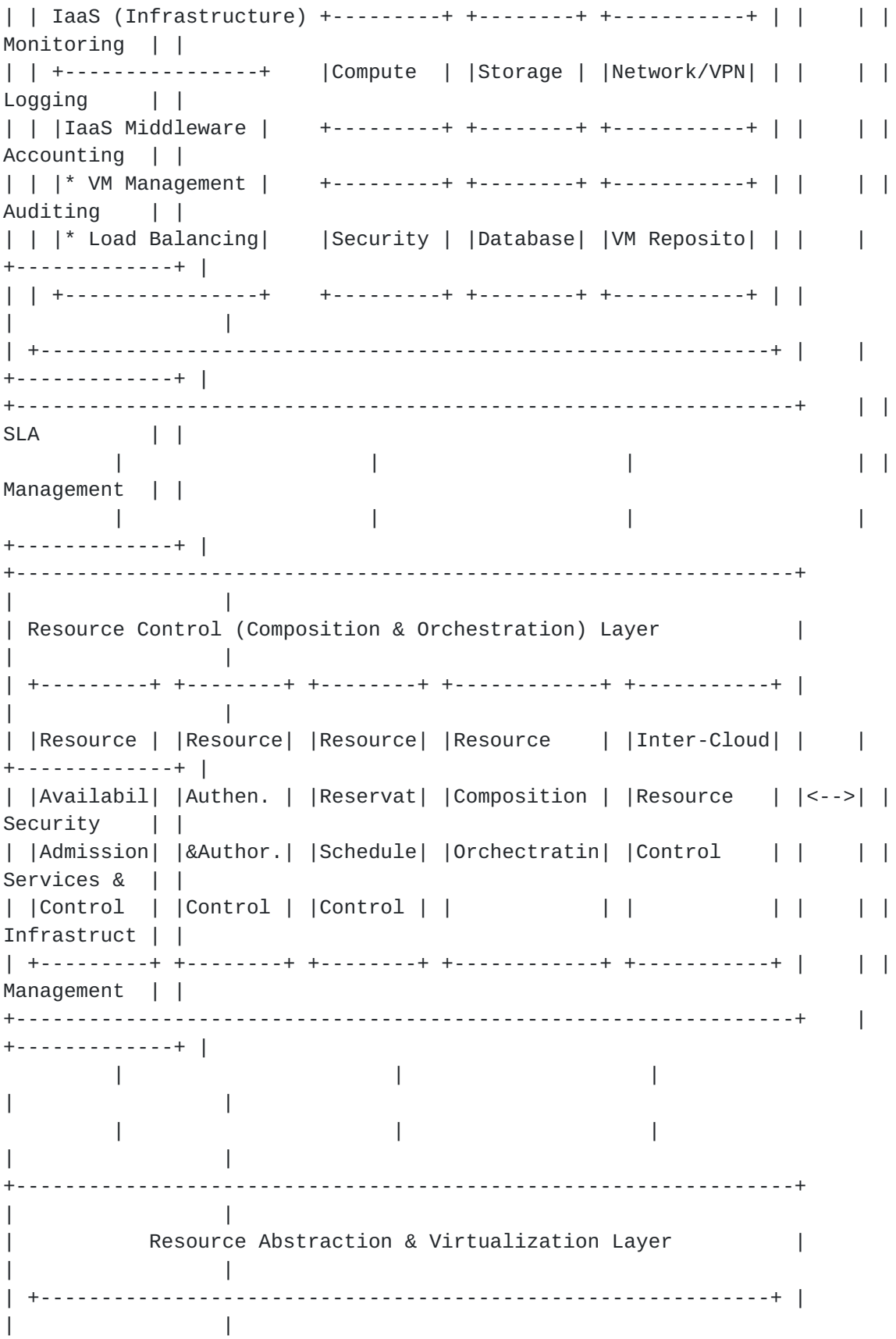
Clouds Discussion Archive:
http://www.ietf.org/mail-archive/web/clouds/current/maillist.html

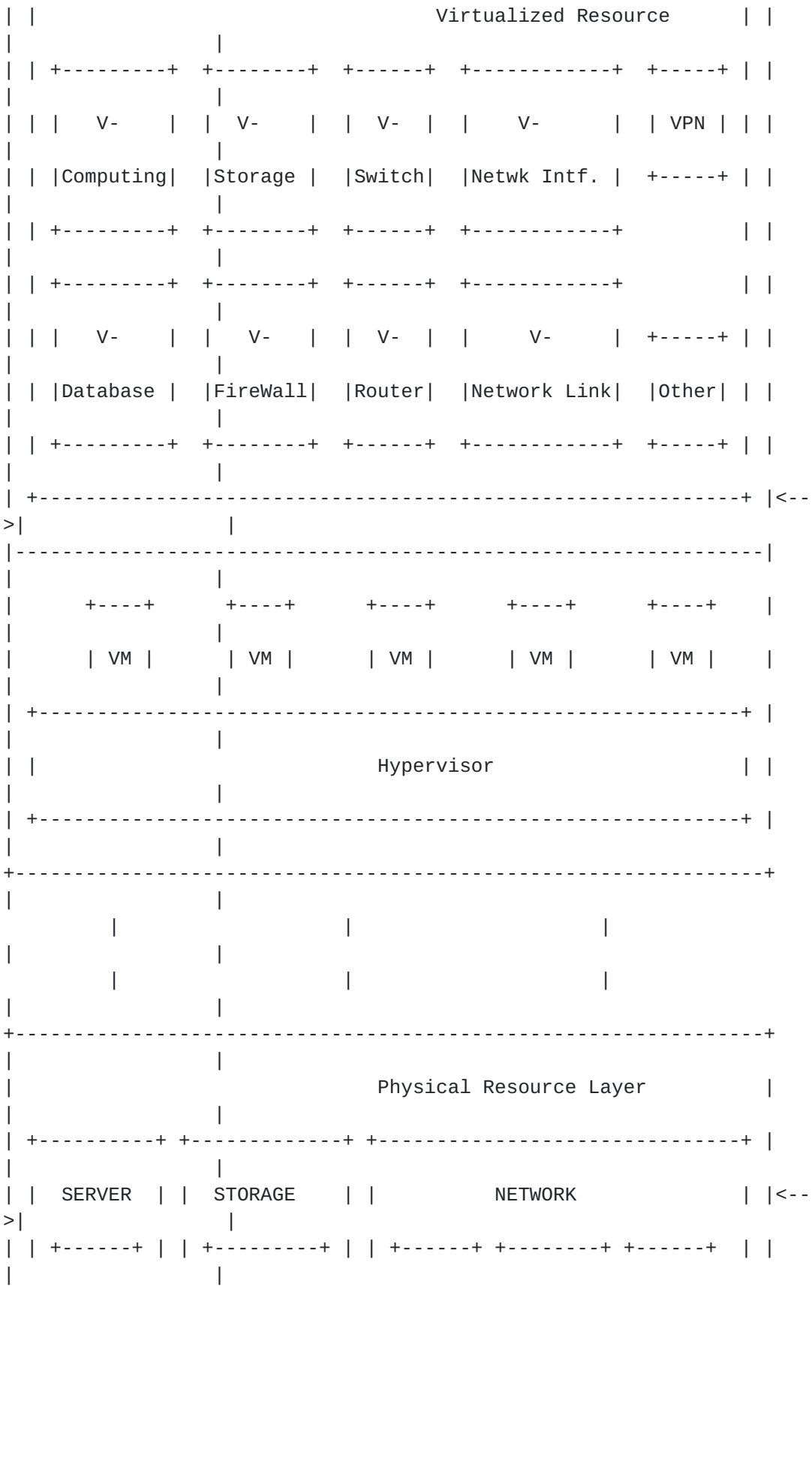
IETF Wiki Website for slides from Clouds bar BoFs:
http://trac.tools.ietf.org/area/app/trac/wiki/Clouds

3. Reference Cloud Services Model




Cloud Service Layer
IaaS
PaaS
SaaS (Applications) & API
API
API
BusinessApps
(Analytics)
ConsumerApps
(Data share/backup)
NetworkApps
(Hosted PBX)
CommunicationApps
(VoIP, Video Serv.)
PaaS (Software Environment)
PaaS MidWare
* Service Bus
* Load Balance
Development
Environment
Test
Environment
Configuration
Management
Services
Lifecycle
Management
Registry &
Discovery


IaaS (Infrastructure)
IaaS Middleware
* VM Management
* Load Balancing
Compute
Storage
Network/VPN
Security
Database
VM Reposito
Monitoring
Logging
Accounting
Auditing
SLA
Management
Resource Control (Composition & Orchestration) Layer
Resource
Availabil
Admission
Control
Authen.
&Author.
Control
Resourc
Reservat
Schedule
Control
Resource
Composition
Orchectratin
Control
Inter-Cloud
Resource
Control
<-->
Security
Services &
Infrastruct
Management
Resource Abstraction & Virtualization Layer


Virtualized Resource
V-Computing
V-Storage
V-Switch
V-Netwk Intf.
VPN
V-Database
V-FireWall
V-Router
V-Network Link
V-Other
VM
VM
VM
VM
VM
Hypervisor
Physical Resource Layer
SERVER
STORAGE
NETWORK

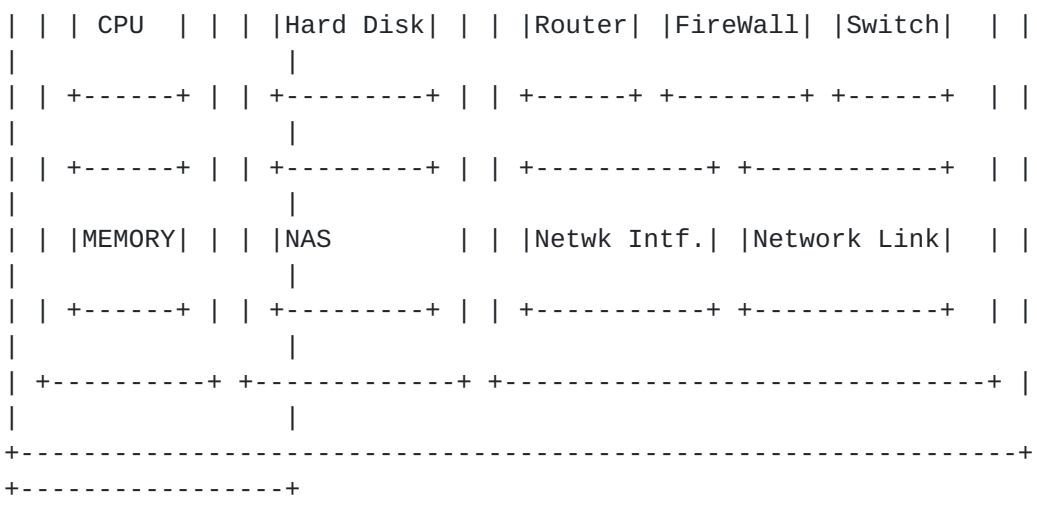


Figure 3.1. Cloud Services Model

3.1. HORIZONTAL/CSM LAYERS

3.1.1. Access and Service Delivery Layer (ASDL)

Access and Service Delivery Layer hosts functions and generally infrastructure components to deliver cloud based services to customers and their access by end users. In majority cases services delivery takes place over Internet but may also include dedicate network infrastructure provided by a third party network provider or so-called Cloud Carrier.

The ADL may include (but not limited to) the following functions:

- End-point functions that may include
  - User portal
  - Service gateways (such as distributed cache, CDN gateways, etc.)
- Intercloud functions that may include
  - Intercloud infrastructure to support cloud federation
  - Federated Identity providers that besides Identity Management functions may also include attribute provisioning and translation, trust management and Security Token Service
  - Cloud services registry and discovery

* Cloud brokering functions

* Trust brokering and management functions

End-point functions can be provided either Cloud Service provider themselves, in particular Cloud IaaS providers that typically have

globally distributed infrastructure, or third party service providers such as SDN providers, home access providers, network service providers, etc.

It is also foreseen that global Cloud Service providers will provide localized access and delivery services to distributed users based on their globally distributed infrastructure and existing datacenters and points of presence worldwide.

3.1.2. Cloud Services Layer

Cloud Service Layer defines the requirements of the basic functional entities based on the virtual resources needed to perform any tasks. The tasks are classified according to the 3 cloud services models IaaS, PaaS and SaaS. Some cloud services are illustrated as an example of applications like:

- Compute, storage, database, and VLAN/network for IaaS,
- Development environment and test environment for PaaS,
- Business, consumer, network and communication applications for SaaS.
- Cloud services middleware that is typically present in both IaaS and PaaS service layers and include load balancing, Service Bus for PaaS, and VM management for IaaS.

The requirements the basic functional entities provided include the following characteristics and parameters of the virtual resources:

- Type of resources: CPU, memory, hard disk space, bandwidth, latency, jitter, and so on
- Amount of resources
- Nature of the resources: dedicated vs. shared, transport media exclusions, and so on
- Timing of the resources: scheduled vs. on-demand
- Duration of the Resources

Cloud Services layer defines also interfaces: external cloud services interface that exposes cloud service to user or customer, and internal that links cloud services and underlying virtualized resources.

3.1.3. Resources Control (Composition and Orchestration) Layer (RCOL)

Resources Control Layer manages the virtual resources, ensuring that the resources are efficient, secure and reliable. With the interface of virtual resources, the layer integrates the resources as a whole supplied to upper layer. The layer has the following responsibilities:

- Resources composition and orchestration. The layer provides functionality to compose cloud resources, that are provisioned together as cloud services on-demand, from the available resource pool. Orchestration means providing inter-resources communication, synchronisation and coordination.

- Resource schedule control. The layer manages resources in form of resource pool. In a resource pool, the layer balances the virtual resources on a set of physical equipment to achieve higher hardware utilization. Virtual resources can be migrated between physical equipment if necessary, and also can be allocated according to user's priority grade.

- Inter-cloud resource control. Resources in a cloud can be shared with another cloud in some circumstances, so a cloud must control resources in other cloud, and supply cloud service to end users. End users have no need to know where the resources are from.

- Resource availability control. The layer supports fault-tolerance on resources. It can allocate another copy of resources as a backup, and switch over when some faults raised.

- Resource security management. Resources must be accessed and owned by the right user, there are several function modules to fulfill this responsibility, include resource admission control, resource authentication and authorization control

- Services Lifecycle Management. This functional component is needed to support resources provisioning process/staes for an instant cloud infrastructure or service.

3.1.4. Resources Abstraction and Virtualization Layer

Physical resources at the lowest level are the most complex to share among multiple users. There are several hardware details that don't need to visible to users, so we need a level of abstraction. In fact, these physical resources are abstracted first, next composed by the cloud management software (at composition and abstraction layer) and finally deployed as virtual resources on the virtualized physical resources. The function of resources abstraction and virtualization

layer is to convert physical resources to virtual resources. Virtual resources are contained in resource pool. Resources can be allocated to users from the resource pool, and released to resource pool when it's not needed.

Virtual resources are isolated from physical equipment, and have the following features:

- Have all features as physical resources, resource users can't distinguish the difference between them;
- Can be allocated and released on demand;
- Support heterogeneous physical equipment, and supply a consistency view of resources to users;
- Support resource mobility, virtual resource can move from one physical equipment to another seamlessly;

There are several types of resources, such as computing resource, storage resource, database, bandwidth and network. According to the type of resource, there are different methods to realize virtualization. The variety function modules for virtualization are contained in Resources abstraction and virtualization layer. The layer has the following responsibilities:

- Through the interface of physical equipment to manage physical resource, mapping the virtual resources to physical resource;
- Supply the interface to upper layer to manage and access virtual resources;
- Hide the details of physical equipment, mask the difference between physical equipment.

3.1.4.1. Networking Resources Layer

Networking (Resources) layer converts and communicates network (LAN/MAN/WAN) capabilities and capacities(such as Bandwidth, ports, Latency matrices, Jitter matrices, Availability, Restoration capabilities, etc) into a set of resource pools that can be understood and used by the above layers. The resource pools include

- Virtual Switch
- Virtual Router

- Virtual Firewall
- Virtual Network Interface
- Virtual Network Link
- VPN

3.1.5. Physical Resources Layer

Physical Resources Layer include

- CPU
- Memory
- Hard Disk
- Network Interface Card
- Network Link
  - Ports
  - Bandwidth

3.2. VERTICAL LAYERS

3.2.1. Cloud Management Plane

Cloud Management Plane provides monitoring and administration of the cloud network platform to keep the whole cloud operating normally, including the following functionalities:

- Configuration management and services lifecycle management
- Services Registry and discovery
- Monitoring, logging, accounting and auditing
- Service level agreement (SLA) Management (SLAM), and
- Security services/infrastructure management.

Key features of the Virtual System Management Layer include:

- Automatically deploying the cloud system based on the configuration data and policy

- Real-time monitoring and alerting of cloud status, resource usage and performance of cloud
- Reporting and charting of historical events and performance metrics
- Flexible IT management and operational status displays
- Authenticating/Authorizing the published cloud service registry
- Auditing the cloud environment to check whether its running smoothly
- Controlling the SLA implemented in the cloud system
- Maintenance concerned with performing repairs, upgrades and new nodes join into the Cloud
- Providing Security mechanism for the Cloud

Basically CML includes four Functions:

- Cloud Configuration Management
- Cloud Service Registry and Audit Management
- Cloud SLA Management
- Cloud Service Security Management

3.2.1.1. Cloud Configuration Management

Cloud Configuration Management (CCM) is responsible for establishing and maintaining the consistent performance of the Clouds system or product and its functional and physical attributes throughout its life-cycle. It mainly focuses on configuring the cloud system and retrieving the configuration information automatically. Requirements on Configuration Management are as follows:

- Provide efficient and reliable means to provision large amounts of configuration data. Current versions of provision configuration data are CLI, SNMP and NETCONF.
- Provide secure means to provision configuration data. The system must provide support for access control, authentication, integrity-checking, replay- protection and/or privacy security services.

- Provide means to send feedback information to the management system. Feedback information include configuration data confirmation, network status and monitoring information, specific events, etc.

- Provide expiration time and effective time capabilities to configuration data. It is required that some configuration data items be set to expire, and other items be set to never expire.

- Provide facilities to help in tracing back configuration changes

- Be flexible and extensible to accommodate future needs. Configuration management data models are not fixed for all time and are subject to evolution like any other management data model.

- Leverage knowledge of the existing SNMP management infrastructure, such as the knowledge of and experience with MIBs and SMI.

- Basically, the CM includes CM database, CM policy, system change management and version management.

- Related protocol: CLI, SNMP, NETCONF

3.2.1.2. Cloud Service Registry/Repository

Service Registry/Repository provides management and governance capabilities that enable the published cloud service to be authenticated in the cloud system and accessed by service client. It facilitates storing, accessing and managing service information, called service metadata, so that the cloud service can be easily published, selected, invoked, enriched, governed and reused.

Requirements on Service Registry/Repository are as follows:

- Publication and Discovery. The authorized service is published in the Cloud system, and you can keep an accurate record of the deployed services in your repository platform. The user can find the service from the repository platform using the service discovery engine. Cloud Service Registry/Repository is capable of a powerful query mechanism allows you to search and find the services that best fit the requirements of a given process.

- Service Information Retrieval. The service repository enables dynamic and efficient access to services information by enabling selection of services based on service metadata.

- Optimize service usage. Service manage capability enables management of service metadata, as well as service interactions,

dependencies and redundancies. You can classify services based on business objectives, manage policies for service usage and monitor how services are changed and versioned. This capability helps you optimize the use of services in cloud system by exchanging service metadata with runtime monitoring tools and operational data stores.

- Impact analysis. By maintaining relationships, Cloud Service Registry/Repository has extensive support for analyzing the impact of service introduction, deletion or alteration.

- Service life cycle. By creating user-definable entities and customizing the service life cycle, you can configure Cloud Service Registry/Repository precisely according to your business needs. You can easily implement best practices for service life-cycle management with the ability to promote services and life-cycle validations.

- Policy support. You can publish policies that apply to services stored in Cloud Service Registry/Repository. These policies help you institute best practices in your Cloud deployment.

- Governance profile. To help you get started easily and quickly, Cloud Service Registry/Repository provides a well defined service model that includes templates, associated life cycles, governance policies, a classification system, roles and perspectives.

3.2.1.3. Cloud Monitoring, Accounting and Audit Management (CMAAM)

Cloud Monitoring, Accounting and Audit Management (CMAAM) is to provide an agent through which cloud providers and authorized consumers automate the Audit, Assertion, Assessment, and Assurance of the cloud infrastructure (IaaS), platform (PaaS), and application (SaaS) environments to reduce the risk. A common interface and namespace can be used by the CAM to facilitate these audit functions.

Requirements on CMAAM are as follows:

- A well-defined objective and scope tied to quality compliance and risk management processes

- Establish clear policies, procedures, and metrics. Audit management should incorporate defined policies, procedures, and metrics as performance benchmarks. These elements should be reviewed periodically for continuous improvement.

- Integrate essential quality management processes. An effective audit management system should automate the entire audit process

and include integration of the following processes:

* Corrective and preventive actions

* Change control

* Non-conformance tracking and management

* Regulatory document/content management

* Custom reporting, analysis and analytics

* Training

* Compliance intelligence dashboard

3.2.1.4. Cloud SLA Management (C-SLAM)

SLA is a part of a service contract where the level of service is formally defined between Cloud service providers and Cloud customers. Within the terms of their contracts, the SLA will have a technical definition, typical terms as MTTF (Mean Time To Failures), MTTR (Mean Time To Repair), ABA (Abandonment Rate), ASA (Average Speed to Answer), TSF (Time Service Factor), FCR (First Call Resolution), TAT (Turn Around Time), Uptime Agreements, various data rates, etc.

C-SLAM is to control the usage and receipt of resources from and by third parties. The strategy of C-SLAM includes the negotiation of the contract and the monitoring of its realization in real-time. Thus, C-SLAM encompasses the SLA contract definition (basic schema within QoS parameters), the SLA negotiation, the SLA monitoring, and the SLA enforcement.

C-SLAM also needs to define rate reductions and discounts that are applied when a service provider fails to meet the desired service parameters or does not fulfill an agreement.

Requirements on C-SLAM are as follows:

o SLA template specification. when service provider publishes a new service, an SLA template which describes the contract type that goes with the resource usage will be specified. Such a template may be hard to define we propose to develop a skeleton of a template with the corresponding write-up procedure.

o Negotiation. Service client and service providers have to agree on the terms of the SLA binding them and also with the consequences to violations.

- Resource Optimization. When the SLA processes the service access request from the service client, it also has to keep in mind the optimization of the usage of resources, and the QoS guaranteed in the SLA.

- Monitoring. Once the cloud system has started providing access to its resources, it should monitor the operating resources. The monitored information is then used to prove the QoS agreed within the SLA being satisfied.

- Re-negotiation. Some party of the contract may wish to change the resource usage policy while the system is running, in order to comply with a change in external conditions. In order to keep the behaviour of the process continuous, the agreed SLA need adjust to assure the process vitality after migration and resource shortage.

- Evaluation. Besides the running information is interested by the managers and users, other data like contract violations or global statistics are also needed in order to verify the SLA. Evaluation is the process of analyzing the previously monitored information. An evaluation daemon may be proposed, based on the monitoring tools developed.

- Accounting. The use of a resource generates an accounting sheet which describes the resources used and aligns them with the billing rules agreed in the SLA. This is a base to draft the real financial exchange, which can be in disfavour of the provider in case of failure to comply with the compromised QoS. This subject is very sensible, and the development of tools for such themes should not be taken lightly.

C-SLAM service use languages and ontologies related to SLA and business processes management such as WSLA, TMF SLAM, Web Services Agreement, ITIL.

3.2.1.5. Cloud Security Services Management CSSM)

Security in clouds involve two types of security services: cloud platform security services managed by the Cloud Provider and security services that are run as a part of the cloud services or infrastructure provisioned to the customer that is managed by the customer themselves. Cloud Security Services (CSS) include 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 authorisation, service certification) to ensure normal cloud services operation and their protection against not authorised use, policy/ operation violation and intrusion..

Requirements on CSS are as follows

- Authentication and Authorisation. This is the main functionality of the CSSM to provided authentication of the request or requester and authorization of the service use or a specific action on the cloud resource. Authentication requires both Identity Provisioning and Management and key or trust management between two or three parties: Customer/requester, Cloud services or provider, and Identity Provider if it is a part of the Authentication infrastructure. Authorisation requires attributes and policy management. Attributes management can be a part of the Identity Management, and Policy management is typically a separate service of the security infrastructure.

- Policy management. Policy management includes functions for authorisation policies management, their distribution, and selection.

- Licensing. It is likely that cloud services are composed of many different components, most of which have some type of licensing agreement associated with them. The service composition and delivery process need to review individual services licensing agreements and determine if, or how, those licenses will be affected by deployment in a cloud. For example, if the service uses a component that is licensed by CPU number and it is deployed in a cloud environment designed to launch new instances and request more resources as load increases, there should be provided a control not to exceed particular CPU license limit. Cloud service implementation should provide license control when scaling applications.

- Processing requirements and memory locks. To make advantage of a parallel architecture on the typical cloud platform, the application must be designed with multi-threaded code that will allow processing to be split into small chunks,

- Communication protocol. The cloud is based on the Internet Protocol (IP), so for an service to be considered, it must use IP as its communication mechanism. While there are many protocols that can be run over IP, the IP layer can provide security mechanism to protect the security of the transmitted data.

- Data security. The service needs to provide security at the data storage, processing and transmission stages. Data at rest must be protected by the service, that is the service must provide a mechanism to protect the data stored in the cloud. Data in transit needs to be protected either at the service or the transmission level. Most services choose the transmission level

for protection and the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols are often used. Server to server communications need to ensure the security from one cloud instance to another cloud instance.

3.3. User/Customer Side Functions and Resources

It is also important to define the functions on the user or customer side that are typically involved into interaction and protocols with the services provided on clouds. Cloud services are often provided to customers (like company or university) to create their business or project specific services that will be delivered to the end users (like services consumers, buyers, students, etc.).

Considering generic cloud based services delivery chain (cloud provider) _ (customer or business) _ (consumer, end user) the following user/customer side functions can be defined:

- Identity service or user home organization authentication service that in general should be capable to support Single-Sign-On to cloud based services.

- Visualisation that represents a specific type of service delivery that in general needs to deliver a large volume of data to user location; visualization can be considered as a particular case for the general content delivery, and consequently can use CDN technologies.

- Administrative and management functions that are used to manage the provisioned cloud based services; majority of these management functions can be fulfill with the management interface (typically web based) provided by cloud services providers, but for more complex and Intercloud infrastructure services there will be a need for a special user-side management tool.

- Functions to manage content or data on the user side, in particular: cloud services may be created to process or manage user data; cloud services may produce content that needs to be stored at user side; cloud services may involve collecting data from the sensors in user premises or for user applications. Interacting with user content and/or data services may require interactive communication with the cloud services residing on cloud provider premises.

4. Inter-Cloud Framework

The inter-cloud interoperability and integration is motivated by a number of uses to provide multi-provider cloud services and infrastructures, multi-platform cloud services integration and traditional/legacy infrastructure services migration to clouds, and IT infrastructure services recovery or migration/move to a new location, platform, or service model.

A Cloud Service Provider (CSP) can offer services using one or more date centers (DCs). These DCs can provide virtualized compute, storage, and networking resources on on-demand basis to the Cloud Service Consumers (CSC). Therefore, the DC infrastructure does not necessarily need to be a static entity as in a traditional DC. The infrastructure resources can span multiple CSPs and the entity that is offered to the consumer can be referred to as the Infrastructure as a Service (IaaS).

With the IaaS, a CSC can acquire and release resources on on-demand basis.

We therefore define an Inter-Cloud as a interconnection of clouds where two or more cloud service providers (any combination of Service-Provider-owned, private, public, etc.) can collaborate. The objective of the collaboration is to dynamically distribute the workloads based on mutually agreed upon service level agreement (SLA).

The inter-cloud functions generically include the following groups of functions:

- Intercloud Users and Identities management
- Intercloud data store, replication, migration, access and management
- Intercloud business processes, workflows, workflow and SLA management

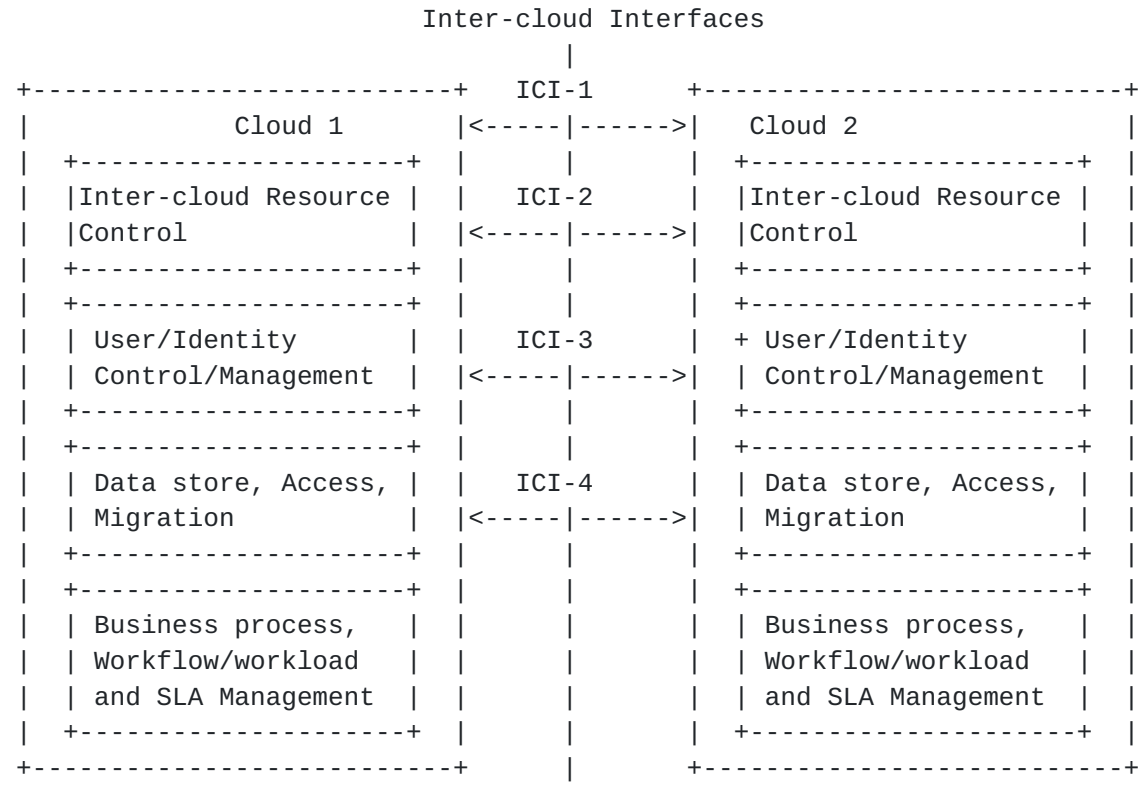


Figure 4.1. Inter-Cloud interfaces general view

4.1. Inter-Cloud Requirements

- ICF should support communication between cloud applications and services belonging to different service layers (vertical integration), between cloud domains and heterogeneous platforms (horizontal integration).

- ICA should provide a possibility that applications could control infrastructure and related supporting services at different service layers to achieve run-time optimization and required Quality of Service (QoS) (typically related to Intercloud control and management functions).

- ICA should support cloud services/infrastructures provisioning on-demand and their lifecycle management, including composition, deployment, operation, and monitoring, involving resources and services from multiple providers (this is typically related to service management and operations support functions).

- Provide a framework for heterogeneous inter-cloud federation

- Facilitate interoperable and measurable intra-provider infrastructures

- Explicit/Guaranteed intra- and inter-Cloud network infrastructure provisioning (as NaaS service model)

- Support existing Cloud Provider operational and business models and provide a basis for new forms of infrastructure services provisioning and operation

More specific Inter-cloud functional requirements may be articulated as follows:

- Provide a mechanism for resource search and discovery, to determine which serving cloud might have certain resources available (including a match making mechanism).

- Provide a mechanism to authenticate participating entities belonging to different cloud domains.

- Provide a mechanism for requesting, controlling, and releasing resources between two clouds.

- Provide a secure transport channel between the interconnecting entities.

- Provide end-to-end isolation to support multi-tenancy.

- Provide a mechanism for monitoring, assuring, and troubleshooting across the interconnection.

- Provide a mechanism for defining the monitoring metrics such as Delay-Jitter-Loss. This may be useful for monitoring a flow such as TCP/UDP between IP prefix and a destination address across the interconnection.

Following the above requirements, we define the following complimentary components of the proposed Intercloud Architecture:

(1) Intercloud Control and Management Plane (ICCMP) for Intercloud applications/infrastructure control and management, including inter-applications signaling, synchronization and session management, configuration, monitoring, run time infrastructure optimization including VM migration, resources scaling, and jobs/objects routing;

(2) Intercloud Federation Framework (ICFF) to allow independent clouds and related infrastructure components federation of independently managed cloud based infrastructure components belonging

to different cloud providers and/or administrative domains; this should support federation at the level of services, business applications, semantics, and namespaces, assuming necessary gateway or federation services;

(3) Intercloud Operation Framework (ICOF) which includes functionalities to support multi-provider infrastructure operation including business workflow, SLA management, accounting. ICOF defines the basic roles, actors and their relations in sense of resources operation, management and ownership. ICOF requires support from and interacts with both ICCMP and ICFF.

Intercloud Security Framework (ICSF) that provides a basis for secure operation of all components of the Intercloud infrastructure, including secure operation of the cloud federations. In this respect ICSF should provide a basis for integration of the security services between different CSM layers and all participating cloud service providers.

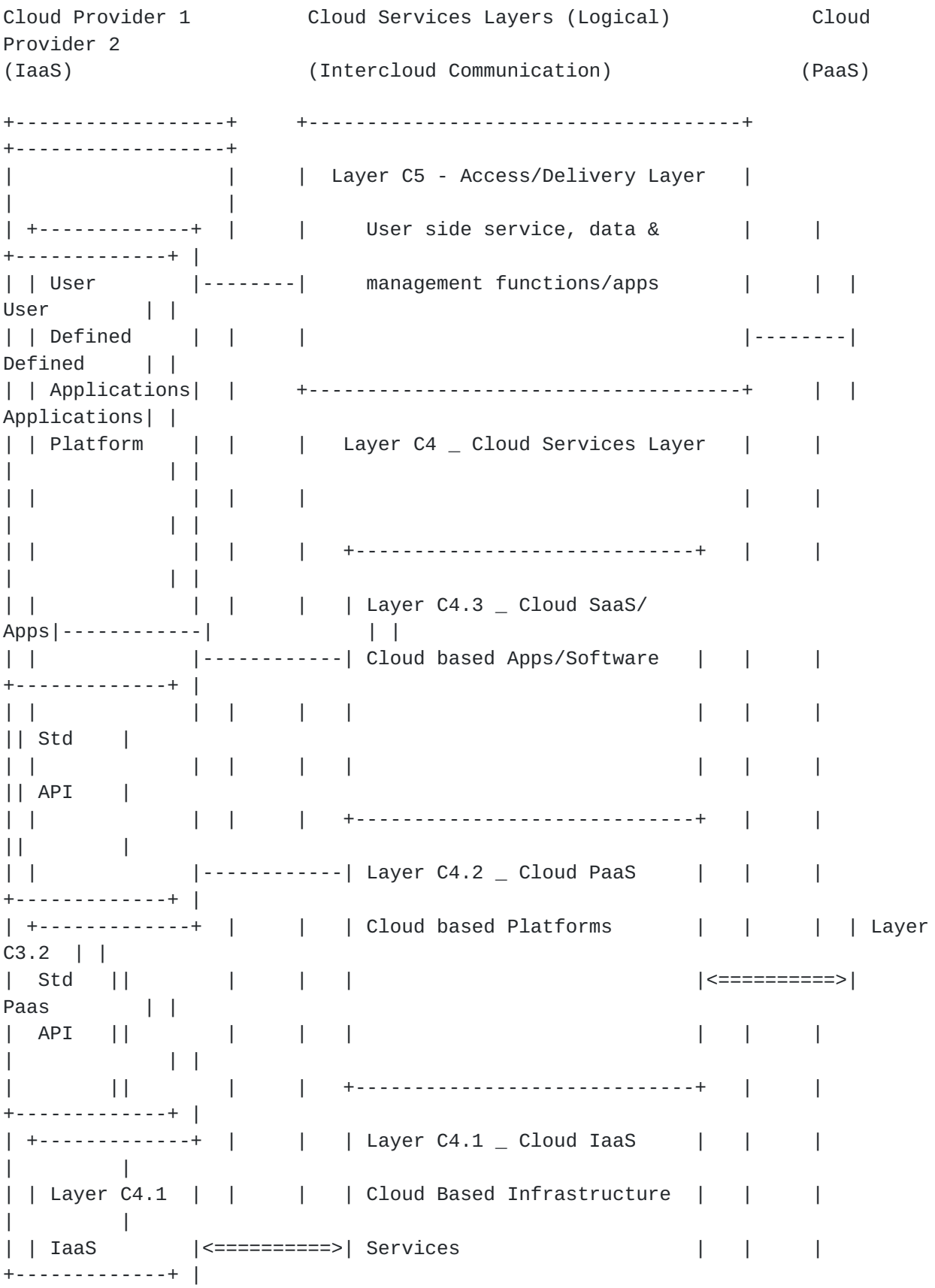
The following sections provides in details descriptions of the proposed ICF components definition and suggestions about required interfaces and supporting protocols.

4.2. Intercloud Control and Management Plane (ICCMP)

The ICCMP defines functionality and functional components for Intercloud applications/infrastructure control and management, including inter-applications signaling, synchronization and session management, configuration, monitoring, runtime infrastructure optimization. ICCMP should support also more complex operations such as VM migration, resources scaling, and jobs/objects/data routing

The ICCMP definition/development attempts to leverage the general Internet technologies such as provided by CDN [CDNI, I-D], XMPP [XMPP, RFC] and the Generalized Multi-Protocol Label Switching (GMPLS) [GMPLS, RFC].

Figure 4.2 illustrates an example where two different cloud/segments domains IaaS and PaaS need to interact (communicate) to allow applications from one domain to control underlying virtualized resources and infrastructure in another domain. Upper layer (north band) interfaces facing customer applications are typically standardised and can use e.g. Open Cloud Computing Interface (OCCI) [OCCI] as a standard interface or Amazon Web Services (AWS) as an industry standard-de-facto interface, while lower layer interfaces controlling internal provider virtualized and physical resources may be non-standard or proprietary.


Cloud Provider 1 (IaaS)
Cloud Services Layers (Logical) (Intercloud Communication)
Cloud Provider 2 (PaaS)
Layer C5 - Access/Delivery Layer
User side service, data & management functions/apps
User Defined Applications
Layer C4 _ Cloud Services Layer
Layer C4.3 _ Cloud SaaS/ Cloud based Apps/Software
Std API
Layer C4.2 _ Cloud PaaS
Cloud based Platforms
Std API
Layer C4.1 _ Cloud IaaS
Cloud Based Infrastructure
Layer C4.1 IaaS
Services
Layer C3.2 Paas

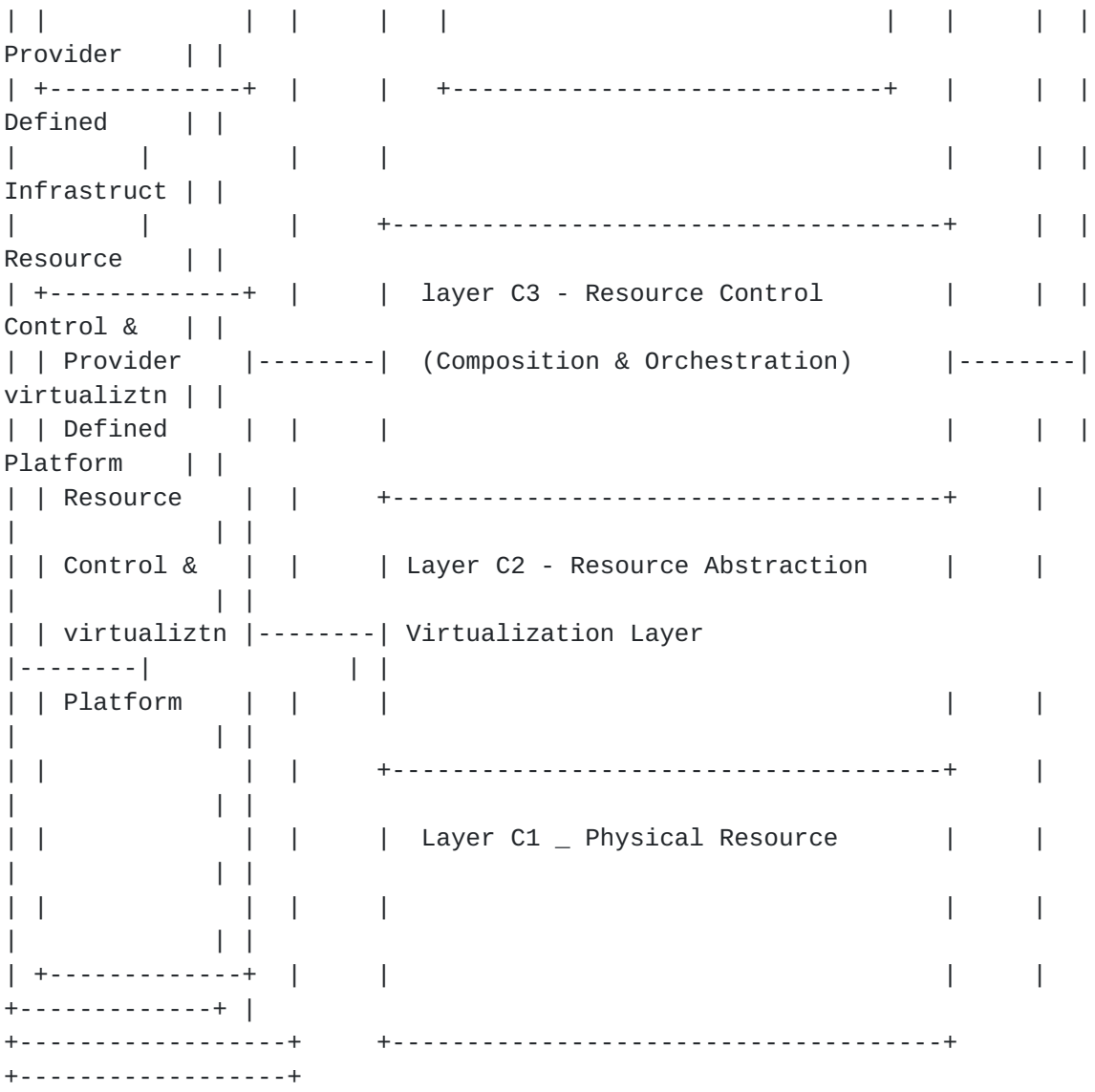


Figure 4.2. Inter-Cloud Control and Management Plane (ICCMP)

Interfaces Logical model

The role of ICCMP is to provide logical and functional interface between different cloud service layers running in different cloud domains. This provides another motivation for the standardisation of such interlayer interfaces; otherwise they can be implemented as part of user applications.

ICCMP supports Intercloud signalling, monitoring, dynamic configuration and synchronisation of the distributed heterogeneous clouds.

Main functional components include

- Cloud Resource Manager
- Network Infrastructure Manager
- Virtual Infrastructure composition and orchestration
- Services and infrastructure lifecycle management (that can be also a part of the composition and orchestration layer).

The ICCMP Interfaces should support the following functionalities:

- Inter-/cross-layer control and signalling
- Message routing
- Monitoring
- Location service
- Topology aware infrastructure management
- Configuration and protocols management.

4.3. Intercloud Federation Framework (ICFF)

ICFF is defined to allow independent clouds and related infrastructure components federation of independently managed cloud based infrastructure components belonging to different cloud providers and/or administrative domains; this should support federation at the level of services, business applications, semantics, and namespaces, assuming necessary gateway or federation services, and also supporting federated security infrastructure including federated identity and trust management;

The ICFF is built upon and extends current cloud federation concept [CloudFed] and leverages existing platforms for federated network access and federated identity management widely used for multi-domain and multi-provider infrastructure integration [Bujja, 2010], [ICFF, 2013]. The federation allows for end-users to access cloud services from multiple domains without need to obtain a separate identity, while services remain under control of their original operator or home provider.

One of the main components of the federated Intercloud architecture is the Intercloud gateway that provides translation and forwarding of the requests, protocols, data formats between cloud domains that may use different semantics, protocols, trust relations.

The main goal of ICFF is to allow heterogeneous clouds integration at service and business level.

When considering Intercloud federation scenarios we can define two general types of federation:

1) user-side federation that federates cloud services and applications provided by CSPs (single or multiple) and federates user identities/accounts to allow federation based Single Sing On (SSO) to cloud services provisioned on-demand;

2) provider-side federation of cloud resources that is typically created between cooperating CSP to outsource some cloud resources to specialized cloud resource providers, extend used resources pool in cased of excessive demand, or offer to used resources to other providers.

In both cases the main task of the federation infrastructure is to support federated access and control and federated resources or identity management. Although the federation infrastructure can be built using existing platforms for federated network access and federated identity management widely used for multi-domain and multi-provider infrastructure integration, the cloud scenario requires dynamic on-demand identity provisioning and dynamic security associations establishment what is not standard procedure for existing federation technologies that in most cases rely on the off-line and apriori established trust relations.

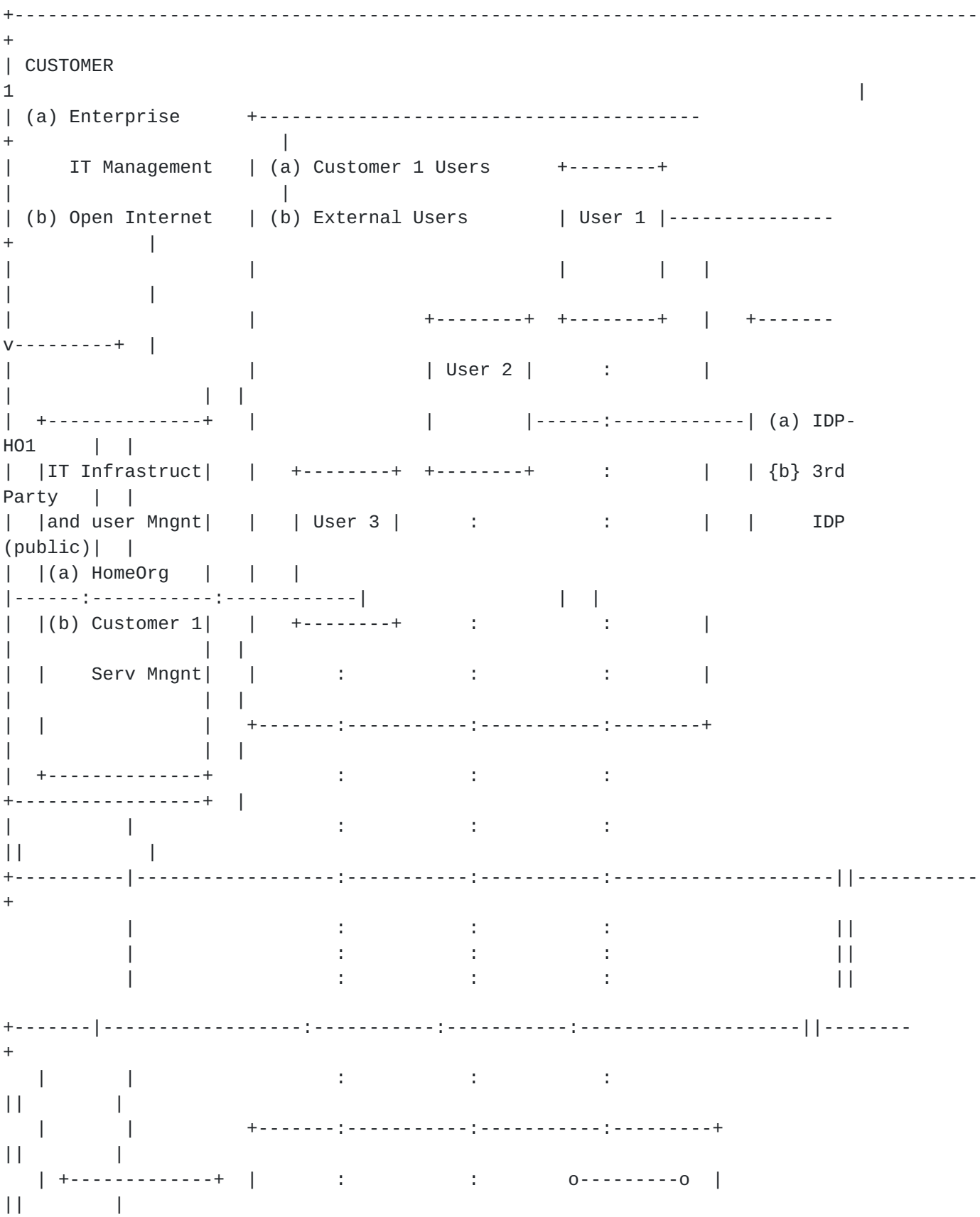
Figure 4.3 illustrates the main actors and relations in the user-side federation that covers the following basic scenarios:

a) Enterprise as a Customer 1 creates a virtualized service or infrastructure on the CSP A premises that will be used by the customer's employees acting as cloud based service users.

User accounts and/or identities to access cloud based services can be created as (i) unique cloud based identities that will be used by the employees directly or (ii) federated with (mapped to) their home identities.

In this case, the enterprise Identity Provider, often referred to as Home Organisation (HO) IDP needs to be federated with the cloud based IDP that in practice can be either (i) completely virtualized IDP-Xa for the on-demand provisioned service Xa, or (ii) CSP's IDP can be used as a gateway for translating/mapping identities between HO and services Xa.

b) Customer 1 creates services that will run from the cloud and serve external customers and users (like in case of cloud based e-commerce site). In this case, the external users should have an opportunity to use the third party IDP services such as from the global Identity Services Microsoft, Gmail, Facebook, etc.


CUSTOMER 1
(a) Enterprise
IT Management
(b) Open Internet
(a) Customer 1 Users
(b) External Users
User 1
User 2
User 3
(a) IDP-HO1
{b} 3rd Party IDP (public)
IT Infrastruct and user Mngnt
(a) HomeOrg
(b) Customer 1
Serv Mngnt

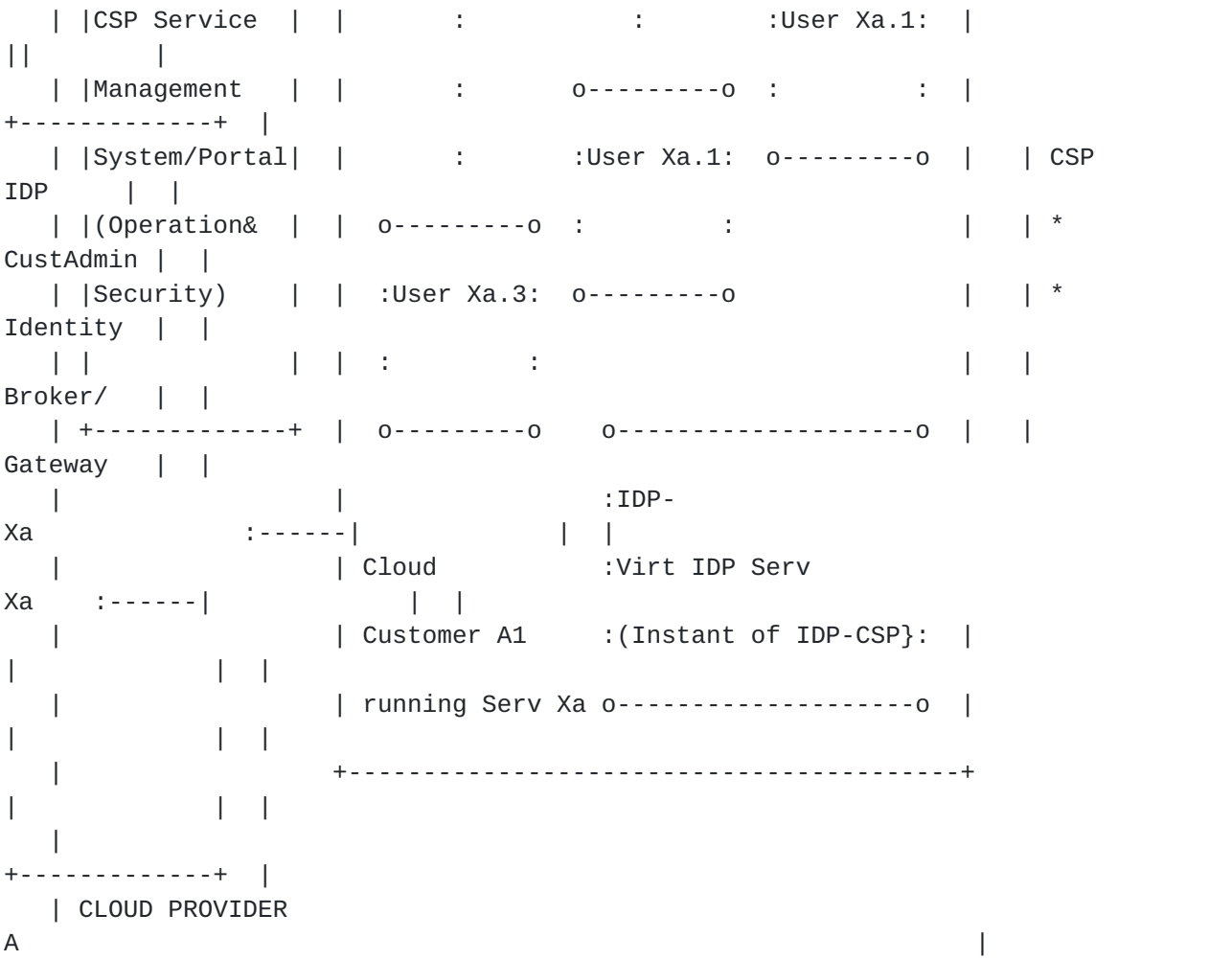


Figure 4.3. Basic federation relations when provisioning cloud based services or infrastructure

The Intercloud Federation Framework is responsible for coordinating allocation and management of the resources and users in a unified way. Figure 4.4 illustrates the main components of the federated

Intercloud Architecture, specifically underlying the Intercloud gateway function (GW) that provides translation of the requests, protocols and data formats between cloud domains. The federated Intercloud infrastructure requires a number of functionalities, protocols and interfaces to support its operation. The following common services constitute the federated Intercloud infrastructure:

- Service and Trust Brokers
- Service Registry
- Service Discovery
- Federated Identity Provider (FedIDP), including attributes management service
- Service and/or inter-domain gateway (GW) that provides translation of the requests, protocols and data formats between cloud domains

Each Federated Cloud infrastructure instance typically contains Cloud Service Broker and trust Broker or manager that support correspondingly dynamic services federation and dynamic trust establishment. Each Cloud Provider domain also includes Identity Provider IDP and Authentication, Authorisation, Accounting (AAA) services, both of them supporting federated identity and federation policy.

Recent research and developments in Intercloud architecture have defined a new component of the federated Intercloud network infrastructure the Open Cloud eXchange (OCX) [OCX, 2015]. The OCX has been proposed to bridge the gap between the two major components of the general cloud services provisioning and delivery infrastructure: (1) the Cloud Service Provider (CSP) infrastructure which either has a global footprint, or is intended to serve global customer community, including those customers who target to deliver services to the global/worldwide community; and (2) cloud services delivery infrastructure which in many cases requires dedicated local infrastructure and quality of services that cannot be delivered by the public Internet infrastructure. The OCX will remain neutral to actual cloud services provisioning and limit its services to Layer 0 through Layer 2 to remain transparent to current cloud services model.

The ICFF interfaces should support the following functionalities:

- Names and attributes resolution, translation and management (if/as needed)

- Publishing and subscription
- Discovery
- Trust/key management
- Service, infrastructure and federation itself lifecycle management.

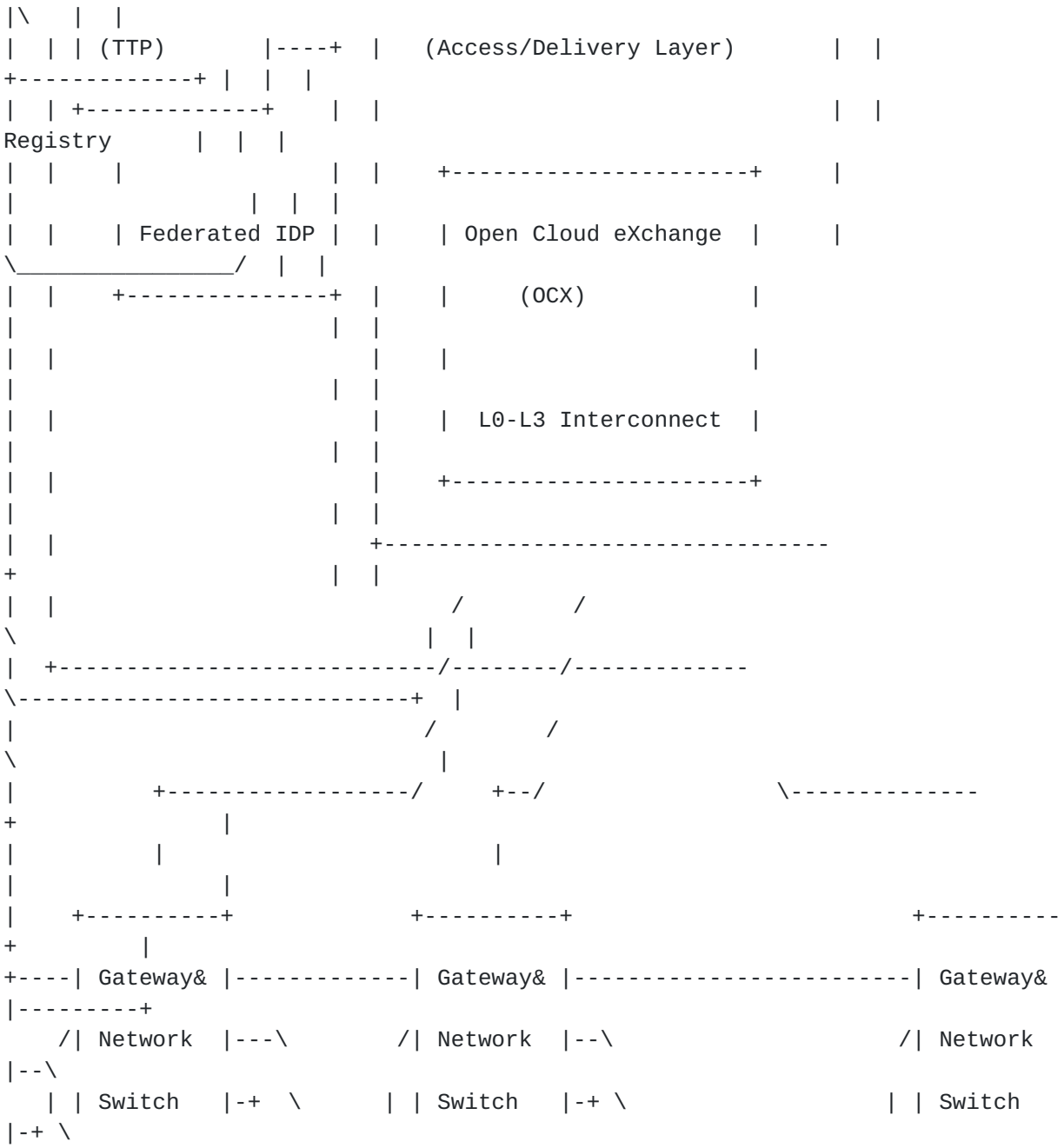

(TTP)
(Access/Delivery Layer)
Registry
Federated IDP
Open Cloud eXchange
(OCX)
L0-L3 Interconnect
Gateway&
Gateway&
Gateway&
Network
Switch
Network
Switch
Network
Switch

Figure 4.4. Intercloud Federation Infrastructure: Main components

The following federation related issues must be addressed in the further ICFF definition:

- Federation, delegation and trust management
- Single Sign On (SSO) and session credentials management
- Attributes management in federations, attributes validation , mapping and translation
- Federation governance, including federation lifecycle management.

4.4. Intercloud Operation and Management Framework (ICOMF)

ICOMF includes functionalities to support multi-provider infrastructure operation and managment including business workflow, SLA management, accounting, and operational security. ICOMF defines the basic roles, actors and their relations in sense of resources operation, management and ownership. ICOMF requires support from and

interacts with both ICCMP, ICFF and ICSF.

The ICOMF definition will include analysis and adoption of the TeleManagement Forum (TMF) documents related to eTOM and Operational Support Systems [TMF], Service Delivery Framework (SDF) [TMF SDF], and SLA Management [TMF SLAM].

ICOMF defines the main roles and actors based on the RORA model: Resource, Ownership, Role, Action. This should provide a basis for business processes definition, SLA management and access control policy definition and also Broker and Federation operation.

The following actor are defined as involved into business, ownership and operational relations:

- Intercloud Service Provider
- Intercloud Broker
- Intercloud Carrier
- Intercloud Service Operator
- Intercloud Resource Provider

Main functional components include

- Service Broker
- Service Registry
- SLA Repository
- Service Monitoring System

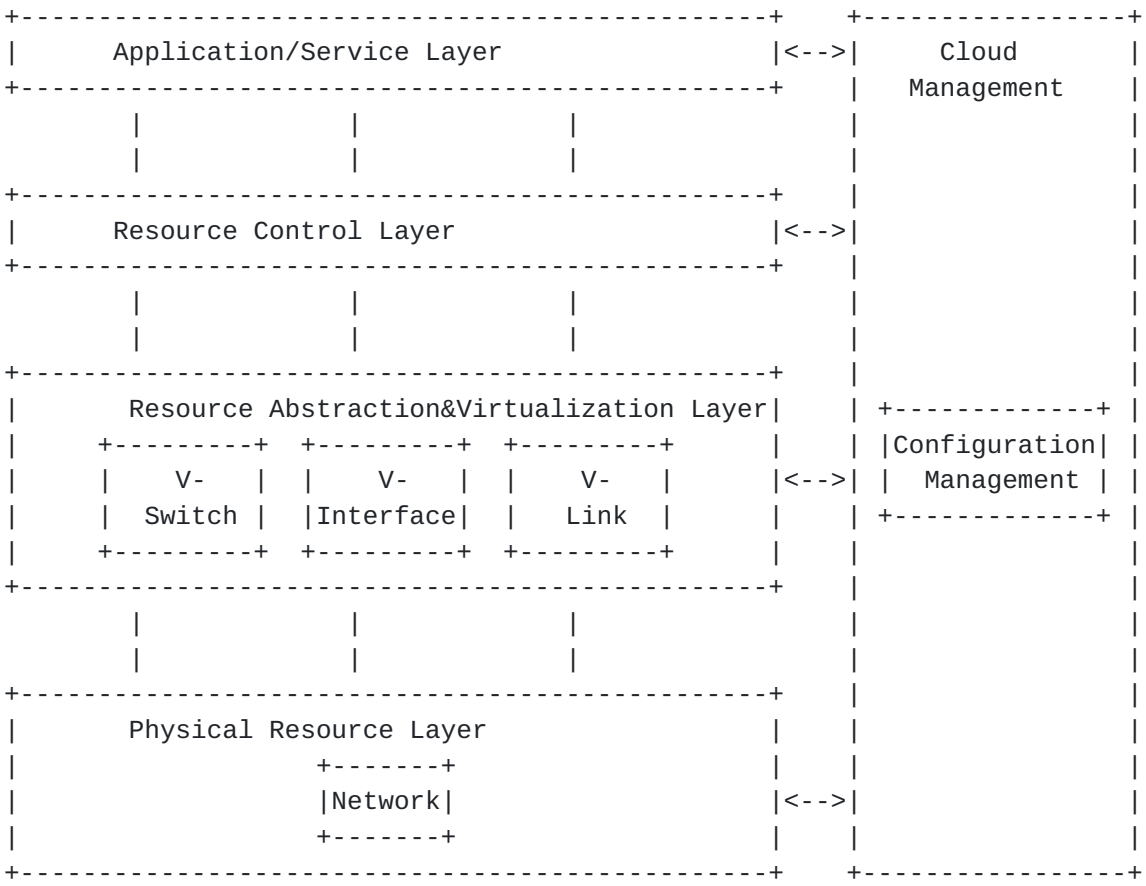
The ICOMF Interfaces should support the following functionalities

- Provisioning, Deployment, Decommissioning/Termination
- SLA management and negotiation
- Services Lifecycle management
- Services deployment
- Monitoring information exchange

5. Use Cases

5.1. Virtual Network Management

Configuration Management in VSML is responsible for creating and managing virtual network through the interface between the Configuration Manager and the Resources Abstraction and Virtualization Layer or Physical Resource Layer. This section is based on the information available in the following draft: draft-Okita-Clouds-VNM-model-for-PaaS-00, Okita-Clouds-VNM-model-for-PaaS-Sept10.pdf



5.2. Telecom Network Virtualization

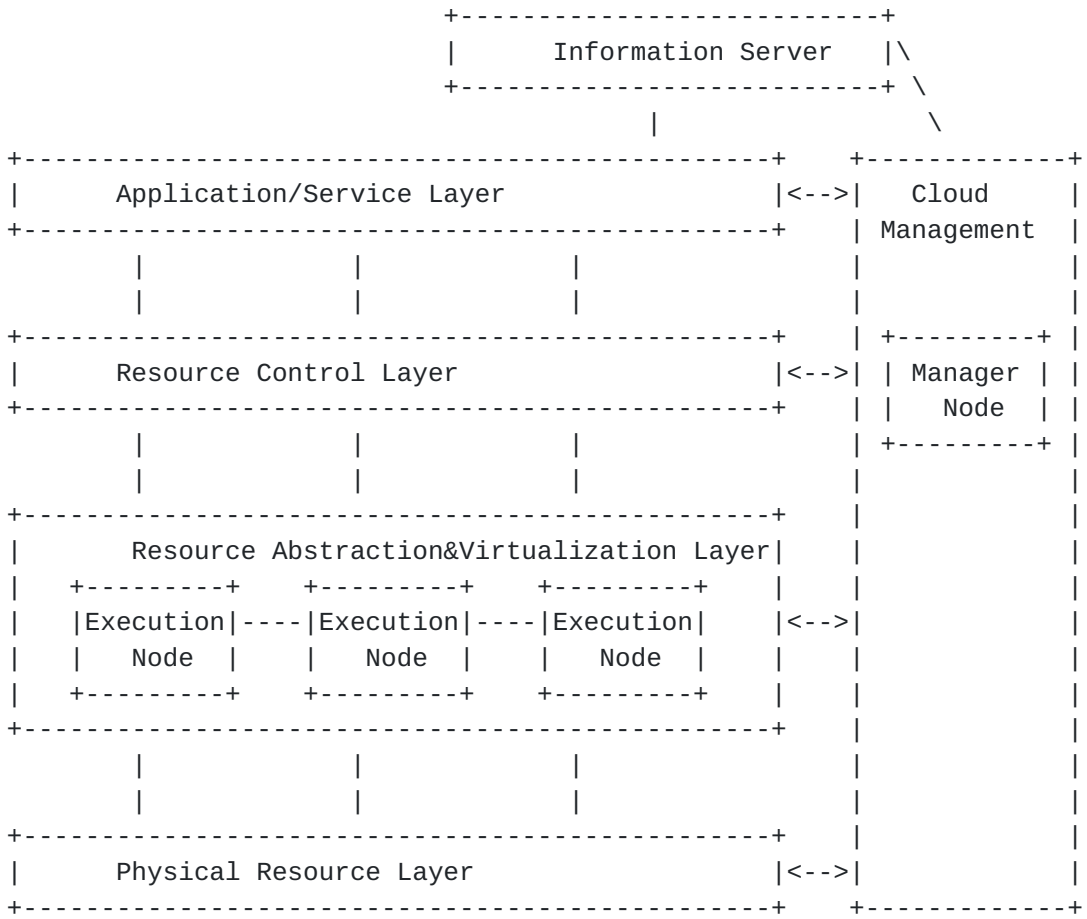
Telecom Network virtualization is the technology that enables the creation of logically isolated network partitions over shared physical network infrastructures so that multiple virtual Telecom networks can simultaneously coexist over the shared infrastructures.

The objectives of Telecom network virtualization is to

- scale Telecom services on demand
- improve reliability and availability
- efficiently use infrastructure

In order to facilitate the deployment of Telecom network virtualization, Manager Node provides control procedures such as creating Functional (Service) Entity operating on Execution Node, monitoring the status of Functional (Service) Entity and Execution Node, measuring the performance, retrieving deployment data from Information Server, and so on.

This section is based on the information available in the following draft: draft-Yokota-Clouds-Telecom-Net-Virtualization-00, Yokota-Clouds-Telecom-Net-Virtualization-Sept10.pdf



Manager Node manages the Execution Node and communicates with Information Server to get configuration data.

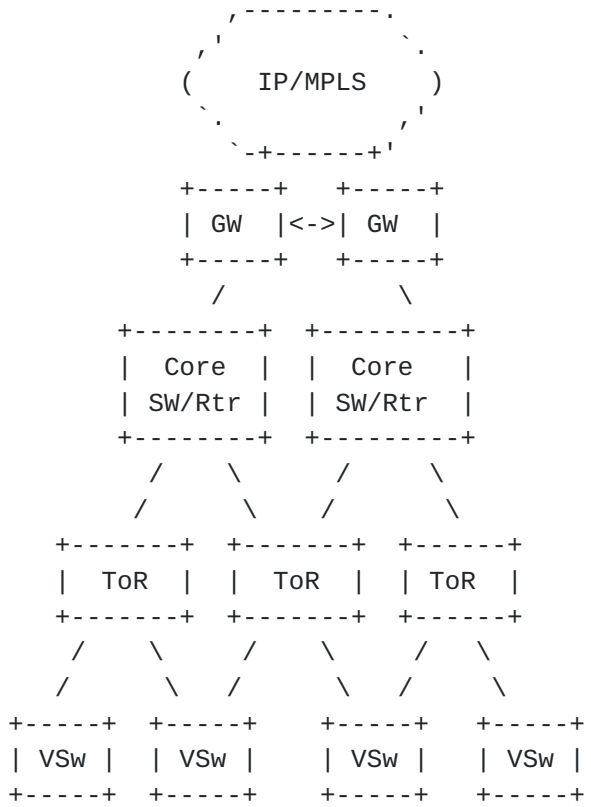
Execution Node is a physical or virtual machines on which target Telecom functions (software) are running. For example, in IMS, CSCF and HSS are candidates of functions.

Information Server (optional) is used for discovery and assignment of Execution Node for a session (e.g., P-CSCF at a UE's registration).

5.3. Virtual Data Center

Virtual Data Center (VDC) can be constructed base on the virtualized resources in cloud environment.

This section is based on the information available in the following draft: draft-bitar-datacenter-vpn-applicability-01.txt, draft-armd-datacenter-reference-arch-01.txt.



The following network components are present in a DC:

- VSw or virtual switch - software based Ethernet switch running inside the server blades. The individual VMs appear to a VSw as IP hosts connected via logical interfaces. The VSw may evolve to

support IP routing functionality.

- ToR or Top of Rack - software-based or hardware-based Ethernet switch aggregating all Ethernet links from the server blades in a rack representing the entry point in the physical DC network for the hosts. ToRs may also perform routing functionality.

- Core SW (switch) - high capacity core node aggregating multiple ToRs. This is usually a cost effective Ethernet switch. Core switches can also support routing capabilities.

- DC GW - gateway to the outside world providing DC Interconnect and connectivity to Internet and VPN customers. In the current DC network model, this may be a Router with Virtual Routing capabilities and/or an IPVPN/L2VPN PE.

5.4. GEANT Open Cloud eXchange (gOCX)

The Open Cloud eXchange (OCX) has been proposed by the GEANT project as a new conceptual and functional component of the general inter-cloud service delivery infrastructure with the intent to bridge the gap between the cloud provider's infrastructure and National Research Network Infrastructure (NREN) and/or campus infrastructure, in particular, to solve the "last-mile" problem in delivering cloud services to customer locations and individuals or end-users [OCX1, 2013], [OCX2, 2015].

5.4.1. gOCX Concept

The proposed OCX concept is based on and extends the Internet eXchange Points (IXP) and GLIF Optical Lightpath Exchange (GOLE) service models with additional functionalities to allow ad hoc dynamic Intercloud federation establishment and non- restricted peering between cloud providers, customers, and also local infrastructure providers, in case cloud services delivery requires involvement of such entities.

Additionally to providing physical location for (network) interconnecting of all involved actors, the OCX declares two basic principles that simplify and facilitate services delivery:

- No value-added third party services (i.e. service composition, integration or operation). In this way, OCX will not be involved in the business dealings related to the actual cloud services provisioning and delivery;

- Trusted Third Party (TTP) services for ad-hoc/dynamic federations establishment: OCX may provide the directory service, trusted

repository of provider certificates operating under supervision of the community (representatives), which can act as a policy authority for security and operational practices.

The proposed OCX role as a TTP will facilitate creation of dynamic federations and establishment of dynamic trust relation between CSPs and customers.

Referring to the generic Cloud Services Model defined in section 3 of current document, the OCX functionality can be related to the Access and Service Delivery Layer (ASDL) layer where the main goal is to deliver cloud based services to organizational customers and end users. Structurally ASDL includes all infrastructure components between the CSP, the final consumer and other entities involved into cloud services delivery and operation. However, to allow easy integration into existing cloud infrastructures and remain transparent to current service models, the OCX limits its services to Layer 0 through Layer 2 transport (or bearer) networks. OCX can be similarly defined as a place for inter-connection and peering between CSPs and customers. Thus, it may also benefit from being collocated with the service provider, NREN exchange points or regional data centers servicing the regional/national research community.

5.4.2. gOCX Architecture

Architecturally and functionally, the OCX includes the following services and functional components (see Figure 4.4):

- Physical Point of Presence (PoP) or OCX Access Points (OCXP) for providers and customers

- L0-L2 network interconnection facility (optionally also connectivity with dedicated optical links). The associated service should allow customer related topology information exchange (such as related to virtual private clouds) between providers and customers in a secure and consistent way (this is of extreme importance since topology information in most cases is considered as commercial or restricted information)

- Trusted Third Party (TTP) services for support of dynamic peering, business/service and trust relations establishment between OCX members; the specific services may include:

  * Trusted Certificates repository and associated Trusted Introducer service to allow dynamic trust associations and/or federations establishment

* Additionally Trust Broker service can be provided and supported by either or both Trusted Introducer and privacy/data security policy Registry or clearinghouse.

5.5. Security Framework for VDCS

Virtualized Data Center Services (VDCS) Security Framework is a reference framework to build secure and interoperable services on top of a virtualized infrastructure. A security framework and the associated requirements for Protocols, Profiles, Network Interfaces, Operations and Management, and Application Interfaces(APIs) need to be proposed in an environment where virtualized resources are shared among a variety of public and private subscribers/clients seamlessly.

The various applications and interworking protocols developed by the IETF MAY need to be extended or profiled to support the security requirements of virtualized services and infrastructure environment.

- Applications and Services: The most widely used protocol that is in use today for application and services development areas like HTTP have been considered for the applications in the virtualized environment. The protocol may have to be profiled or extended with significant changes to be ready to handle the security requirements in a virtualized environment.

- Infrastructure Operations and Management: The various security parameters related to operations and management of virtualized network resources in multiple administrative domains may need to be defined. The results of monitoring may need to be exchanged periodically to support the private and public virtualized domains and infrastructure in order to maintain the expected end-to-end security.

The above protocol extension and operations and management requirements can be implemented in current cloud reference framework (CRF) based on the security functionality provided by cloud management layer, resource authentication and authorization mechanism, and services/users admission control.

This section is based on the information available in the following draft: draft-karavettil-vdcs-security-framework-05.txt

6. Conclusion

This document presents a high-level cloud reference framework that includes both multi-layer Cloud Services Model (CSM) and InterCloud Architecture Framework (ICAF). A few examples on utilization of the reference framework are also discussed.

7. Security Considerations

Contents in this section will be added based on discussion and contributions.

8. Acknowledgement

We thank T. Sridhar (thsridhar@gmail.com), Simon Leinen (simon.leinen@switch.ch) for comments on an earlier version of this document.

The Intercloud Framework definition is an outcome of the ongoing research and developments in the FP7 EU funded project, "Generalised Architecture for Dynamic Infrastructure Services" (GEYSERS, FP7-ICT-248657, http://www.geysers.eu/) which provides implementation of the main components of ICCMP and ICOMF.

The presented work is also supported by the research on Cloud architecture research at the System and Network Engineering group of the University of Amsterdam [UVA2011, UVA2012, ICAF2012].

9. IANA Considerations

This document has no actions for IANA.

10. Normative references

[Buyya, 2010]
Buyya, R., "Buyya, R., R.Ranjan, R.Calheiros, InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. Proc. 10th Intern Conf. on Algorithms and Architectures for Parallel Processing (ICA3PP 2010, Busan, South Korea, May 21-23, 2010), LNCS, Springer, Germany, 2010.", May 2010.

[CDN, I-D]
IETF, "Leung, K. and Lee, Y. (2011). Content Distribution Network Interconnection (CDNI) Requirements", March 2012.

[Cloud SDO]
Khasnabish, B., "draft-khasnabish-cloud-sdo-survey-04", December 2012.

[Cloud ServiceMobility]
Yokota, H., "draft-yokota-cloud-service-mobility-01", March 2011.

[CloudFed]
Blog post by Krishnan Subramanian, "Defining Federated Cloud Ecosystems", October 6 2011.

[DSP0004] DMTF, "Common Information Model (CIM) Infrastructure", May 2009.

[DSP1041] DMTF, "Resource Allocation Profile", June 2009.

[DSP1042] DMTF, "System Virtualization Profile", April 2010.

[DSP1057] DMTF, "Virtual System Profile", October 2009.

[DSP1059] DMTF, "Generic Device Resource Virtualization Profile", July 2009.

[FedNetwork]
GEANT, "Federated Network Architectures. GEANT3 Project.", March 2012.

[GMPLS] IETF, "RFC 3945. Generalized Multi-Protocol Label Switching (GMPLS) Architecture.", October 2004.

[ICFF, 2013]
Makkes, M., "Defining Intercloud Federation Framework for Multi-provider Cloud Services Integration, The Fourth

International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2013), May 27 - June 1, 2013,Valencia, Spain.", June 2013.

[ITU-T FGCC]
FGCC, "FG Cloud Technical Report (Part 1 to 7). [onlie] ht tp://www.itu.int/en/ITU-T/focusgroups/cloud/Documents/ FG-coud-technical-report.zip", April 2011.

[ITU-T Y.2011]
ITU SG13, "Y.2011_General principles and general reference model for NGN", October 2004.

[Industry WorkItem]
Khasnabish, B.,
"draft-khasnabish-cloud-industry-workitems-survey-04",
December 2012.

[NIST CCRA]
NIST, "NIST SP 500-292, Cloud Computing Reference Architecture, v1.0", October 2011.

[NIST Cloud]
NIST, "NIST SP 800-145, A NIST definition of cloud computing", October 2011.

[OASIS IDCloud]
OASIS IDCloud TC, "OASIS Identity in the Cloud", May 2012.

[OCX1, 2013]
Demchenko, Y., "Open Cloud eXchange (OCX): Architecture and Functional Components. Proc. "The 3rd workshop on Network Infrastructure Services as part of Cloud Computing (NetCloud 2013)", in conjunction with The 5th IEEE International Conference and Workshops on Cloud Computing Technology and Science (CloudCom2013), 2-5 December 2013, Bristol, UK.", December 2013.", December 2013.

[OCX2, 2015]
Demchenko, Y., "Open Cloud eXchange (OCX): A Pivot for Intercloud Services Federation in Multi-provider Cloud Market Environment. Proc. IEEE 4th International Workshop on Cloud Computing Interclouds, Multiclouds, Federations, and Interoperability (Intercloud 2015), at IEEE International Conference on Cloud Engineering (IC2E), March 12, 2015, Tempe, USA.", March 2015.

[RFC2119] IETF, "Key words for use in RFCs to Indicate Requirement

Levels", March 1997.

[RFC4741] IETF, "NETCONF Configuration Protocol", December 2006.

[TMF] TMF, "TM Forum Frameworx", March 2012.

[TMF SLAM]
TMF, "TMF SLA Management", November 2011.

[TMF-SDF] TMF, "TR139, Service Delivery Framework (SDF) Overview, Release 2.0.", October 2010.

[UML] OMG, "Unified Modeling Language", September 2002.

[UVA2011] University of Amsterdam, "Generic Architecture for Cloud Infrastructure as a Service (IaaS) Provisioning Model, Release 1. SNE Techn. Report SNE-UVA-2011-03, 15 April 2011. [Online] http://staff.science.uva.nl/~demch/worksinprogress/ sne2011-techreport-2011-03-clouds-iaas-architecture-release1.pdf", 15 April 2011.

[UVA2012] University of Amsterdam, "Intercloud Architecture for Interoperability and Integration, Release 2, Draft Version 0.7. SNE Techn. Report SNE-UVA-2012-03-02, 1 July 2013. [Online] http://staff.science.uva.nl/~demch/worksinprogress/ sne2012-techreport-12-05-intercloud-architecture-draft07.pdf", 1 July 2013.

[VDCS Security]
Karavettil, S.,
"draft-karavettil-vdcs-security-framework-05.txt",
December 2012.

[VNet Model]
Okita, H., "draft-okita-ops-vnetmodel-07", July 2013.

Authors' Addresses

Bhumip Khasnabish
ZTE (TX) Inc.
55 Madison Avenue, Suite 160
Morristown, NJ 07960
USA

Phone: +1-781-752-8003
Email: vumip1@gmail.com, bhumip.khasnabish@ztetx.com
URI: http://tinyurl.com/bhumip/

Chu JunSheng
ZTE
No.50 Ruanjian Dadao Road, Yuhuatai District
Nanjing
China

Phone: +86-25-8801-4630
Email: chu.junsheng@zte.com.cn

Ma SuAn
ZTE
No.68 Zijinghua Rd,Yuhuatai District
Nanjing
China

Phone: +86-25-5287-8189
Email: ma.suan@zte.com.cn

Ning So
Vinci Systems
2613 Fairbourne Cir.
Plano, TX 75082
USA

Phone: +1-972-955-0914
Email: ning.so@vinci-systems.com

Paul Unbehagen
Avaya
USA

Phone: +1-919-606-8845
Email: paul@unbehagen.net

Monique Morrow
Cisco Sys. GmbH
Richistrasse 7
CH-8304 Wallisellen
Switzerland

Phone:
Email: mmorrow@cisco.com

Masum Hasan
Cisco Systems
3675 Cisco Way
San Jose, California 95134
USA

Phone:
Email: masum@cisco.com

Yuri Demchenko
Univ. of Amsterdam
Science Park 904
Amsterdam, 1098 XH
The Netherlands

Phone:
Email: y.demchenko@uva.nl

Meng Yu
.
Nanjing
China

Phone:
Email: zjumengyu@hotmail.com