

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: December 30, 2012

B. Khasnabish
ZTE USA, Inc.
J. Chu
S. Ma
Y. Meng
ZTE
N. So
Tata Communications
P. Unbehagen
Avaya
M. Morrow
Cisco Systems [Switzerland] GmbH
M. Hasan
Cisco Systems
Y. Demchenko
University of Amsterdam
June 28, 2012

Cloud Reference Framework
draft-khasnabish-cloud-reference-framework-03.txt

Abstract

This document presents a cloud reference framework. In general, a cloud-based system utilizes virtualized computing/communications/storage resources and applications. In the emerging cloud-based systems, 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) and other research and developments in the cloud technology area. Both intra-cloud and inter-cloud reference frameworks are presented and the requirements of each layer 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

Internet-Draft

Cloud Reference Framework

June 2012

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 December 30, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](http://trustee.ietf.org/bcp78) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1.	Introduction	4
2.	Terminology	7
3.	Reference Cloud Services Model	8
3.1.	HORIZONTAL/CSM LAYERS	9
3.1.1.	Application/Service Layer	9
3.1.2.	Resources Control Layer	10
3.1.3.	Resources Abstraction and Virtualization Layer	11
3.1.4.	Physical Resources Layer	12
3.2.	VERTICAL LAYERS	13
3.2.1.	Cloud Management Layer -> Cloud Management Plane	13
4.	Inter-Cloud Framework	20
4.1.	Inter-Cloud Requirements	20
4.2.	Intercloud Control and Management Plane (ICCMP)	22
4.3.	Intercloud Federation Framework (ICFF)	23
4.4.	Intercloud Operation Framework (ICOF)	24
5.	Use Cases	26
5.1.	Virtual Network Management	26
5.2.	Telecom Network Virtualization	26
5.3.	Virtual Data Center	28
5.4.	Security Framework for VDCS	29
6.	Conclusion	31
7.	Security Considerations	32
8.	Acknowledgement	33
9.	IANA Considerations	34
10.	Normative references	35
	Authors' Addresses	38

1. Introduction

Clouds are emerging as a common way of provisioning virtualised 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 virtualised 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) and defines the Intercloud framework to address interoperability and integration issues in provisioning multi-domain 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 (ICF/ICAF) addresses a number of issues in ensuring interoperability of cloud infrastructures built using different cloud software stacks/platform 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 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 (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, b) define the interfaces between the functional elements, and c) propose further standardisation.

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

We develop a general cloud reference framework. This reference framework describes basic functions in different layers to support the requirements of virtualized applications and services. 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

- o Five horizontal layers

- * Data/Content Layer(DCL)
- * Application/Service Layer(ASL)
- * Resource Control Layer(RCL)
- * Resource Abstract and Virtualization Layer(RAVL)
- * Physical Resource Layer(PRL)
- o One stacked vertical layer to support
 - * Configuration management, registry, logging and auditing, security management, and service level agreement (SLA) management

The Cloud Services Model includes another important components the security services (infrastructure) which task is to ensure normal operation of 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 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.

[2.](#) Terminology

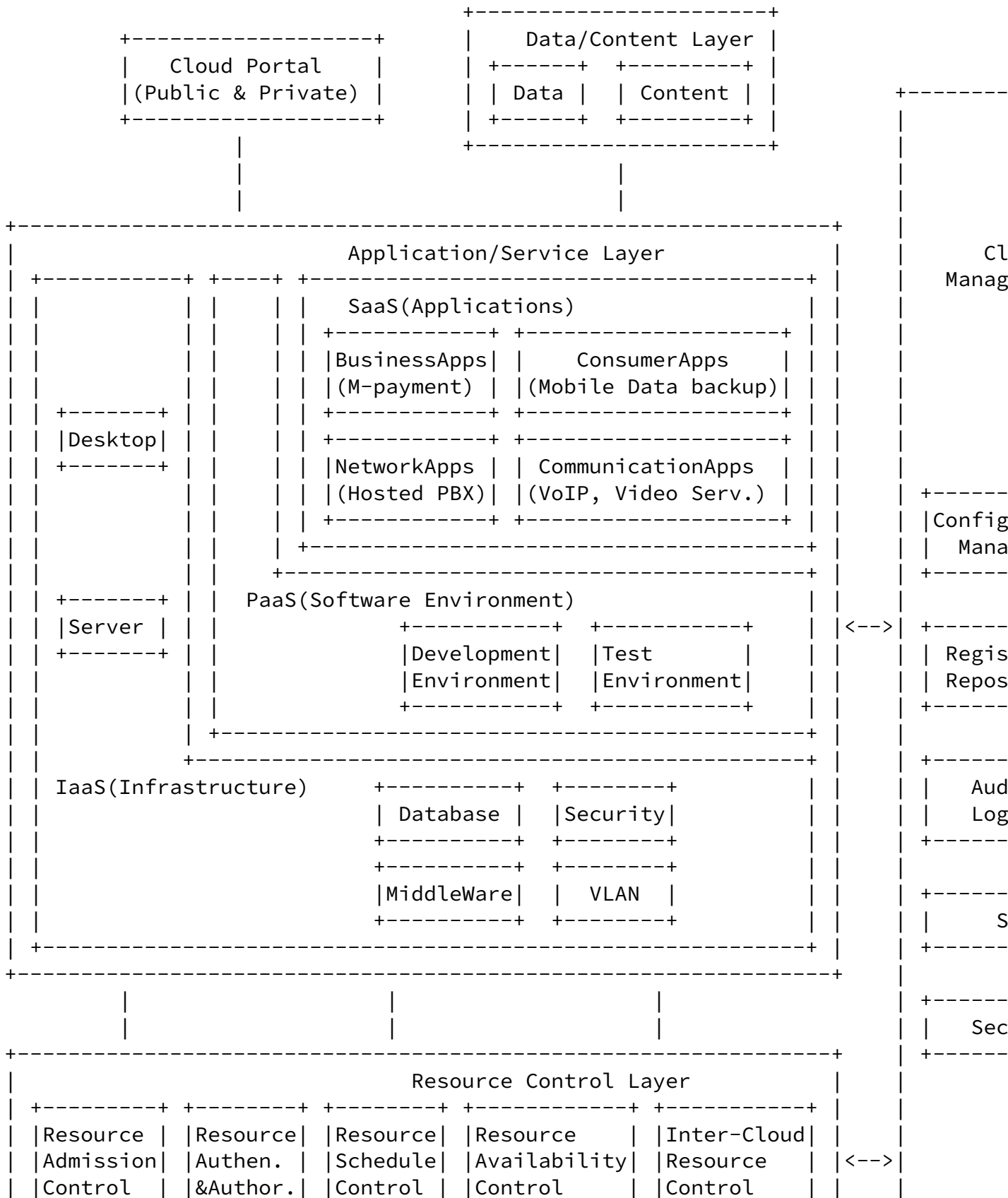
Clouds Discussion Archive:

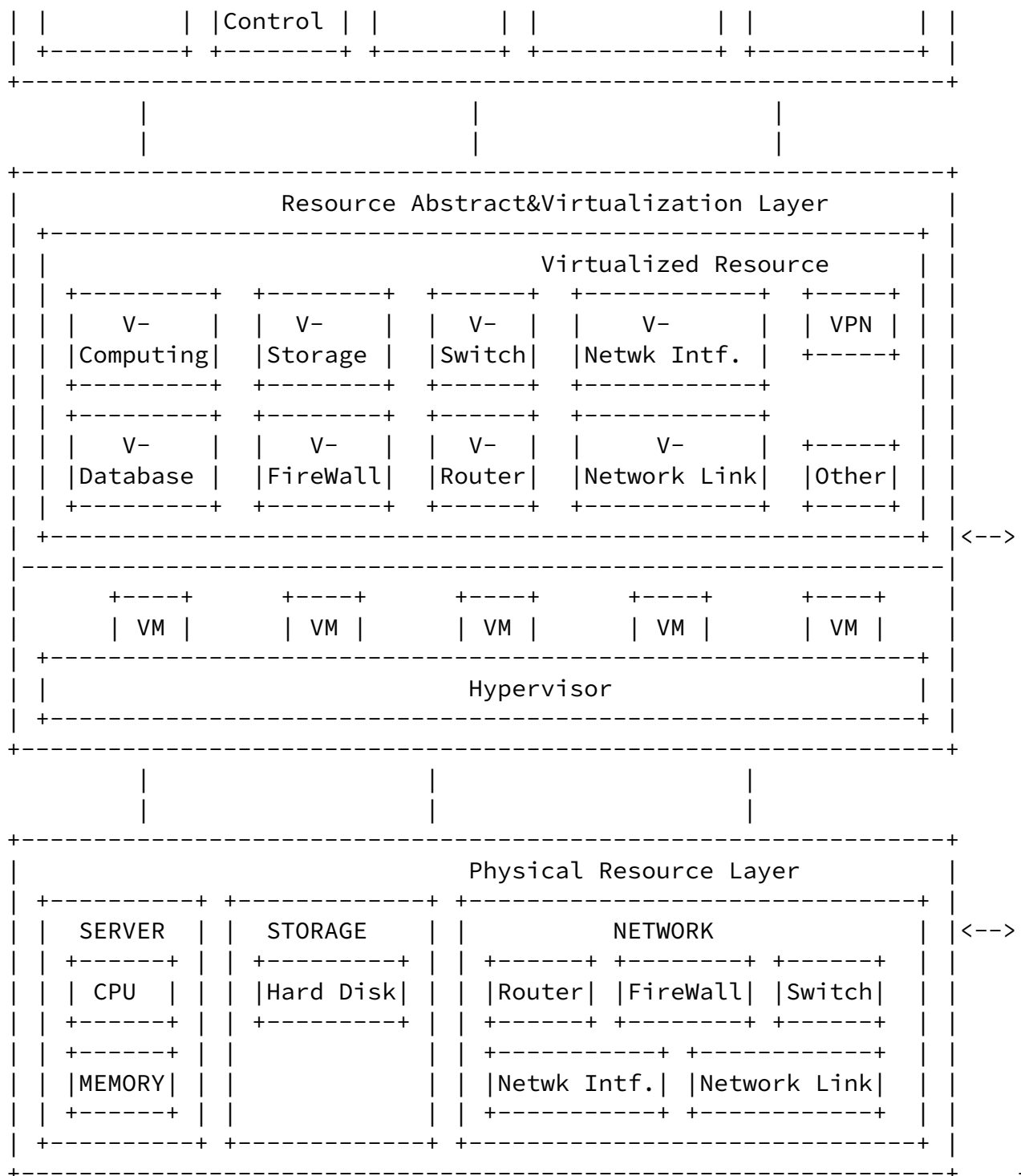
<http://www.ietf.org/mail-archive/web/clouds/current/maillist.html>

IETF Wiki Website for slides from Clouds bar BoFs:

<http://trac.tools.ietf.org/area/app/trac/wiki/Clouds>

[3.](#) Reference Cloud Services Model





[3.1.](#) HORIZONTAL/CSM LAYERS

[3.1.1.](#) Application/Service Layer

Application/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 services

models IaaS, PaaS & SaaS. Some cloud services are illustrated as an example of applications like:

- o Server, desktop, database and VLAN for IaaS,
- o Development environment and test environment for PaaS,
- o Business, consumer, network and communication applications for SaaS.

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

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

[3.1.2.](#) Resources Control Layer

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:

- o 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;
- o 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 equipments to achieve higher hardware utilization. Virtual resources can be migrated between physical equipments if necessary, and also can be allocated according to user's priority grade.

- o 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.

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

[3.1.3.](#) 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 be 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 virtualised 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 equipments, and have the features:

- o Have all features as physical resources, resource users can't distinguish the difference between them;
- o Can be allocated and released on demand;

- o Support heterogeneous physical equipments, and supply a consistency view of resources to users;
- o 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:

- o Through the interface of physical equipment to manage physical resource, mapping the virtual resources to physical resource;

- o Supply the interface to upper layer to manage and access virtual resources;
- o Hide the details of physical equipments, mask the difference between physical equipments.

[3.1.3.1](#). 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

- o Virtual Switch
- o Virtual Router
- o Virtual Firewall
- o Virtual Network Interface
- o Virtual Network Link
- o VPN

[3.1.4.](#) Physical Resources Layer

Physical Resources Layer include

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

[3.2.](#) VERTICAL LAYERS

[3.2.1.](#) Cloud Management Layer -> Cloud Management Plane

Cloud Management Layer (CML) provides monitoring and administration of the cloud network platform to keep the whole cloud operating normally.

Key features of the Virtual System Management Layer include:

- o Automatically deploying the cloud system based on the configuration data and policy
- o Real-time monitoring and alerting of cloud status, resource usage and performance of cloud
- o Reporting and charting of historical events and performance metrics

- o Flexible IT management and operational status displays
- o Authenticating/Authorizing the published cloud service registry
- o Auditing the cloud environment to check whether its running smoothly
- o Controlling the SLA implemented in the cloud system
- o Maintenance concerned with performing repairs, upgrades and new nodes join into the Cloud
- o Providing Security mechanism for the Cloud

Basically CML includes four Functions:

- o Cloud Configuration Management
- o Cloud Service Registry and Audit Management
- o Cloud SLA Management
- o 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:

- o Provide efficient and reliable means to provision large amounts of configuration data. Current versions of provision configuration data are CLI, SNMP and NETCONF.
- o 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.

- o Provide means to send feedback information to the management system. Feedback information include configuration data confirmation, network status and monitoring information, specific events, etc.
- o 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.
- o Provide facilities to help in tracing back configuration changes
- o 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.
- o Leverage knowledge of the existing SNMP management infrastructure, such as the knowledge of and experience with MIBs and SMI.
- o Basically, the CM includes CM database, CM policy, system change management and version management.
- o 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:

- o Authentication & Authorization. Once a service is published by the service provider to the Cloud system, it should be authenticated to check the authority of the provider and the support capability of the Cloud. If the check is passed, the

service is authorized and put into the repository, and the services and related metadata are classified into groups.

- o Publication & 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.
- o Service Access Control. The service repository enables dynamic and efficient access to services information by enabling selection of services based on service metadata.
- o 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.
- o Impact analysis. By maintaining relationships, Cloud Service Registry/Repository has extensive support for analyzing the impact of service introduction, deletion or alteration.
- o 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.
- o 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.
- o Governance profile. To help you get started easily and quickly, Cloud Service Registry/Repository provides a welldefined service model that includes templates, associated life cycles, governance policies, a classification system, roles and perspectives.

[3.2.1.3](#). Cloud Audit Management

Cloud Audit Management (CAM) 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 CAM are as follows:

- o A well-defined objective and scope tied to quality compliance and risk management processes
- o 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.
- o 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 (CSM)

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.

parties. The strategy of CSM includes the negotiation of the contract and the monitoring of its realization in real-time. Thus, CSM encompasses the SLA contract definition (basic schema within QoS parameters), the SLA negotiation, the SLA monitoring, and the SLA enforcement.

SM also need 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 CSM 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.
- o 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.
- o 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.
- o 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.
- o 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.

- o 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.

Related Language: WSLA, ITIL

[3.2.1.5](#). Cloud Service Security Management

Cloud Service Security (CSS) provides a set of security services and mechanisms (e.g. IP address filtering, firewall, message integrity & confidentiality, private key encryption, dynamic session key encryption, user authentication and Service certification) to protect Cloud Services and their operating environment from not authorised use, policy/operation violation and intrusion..

Requirements on CSS are as follows

- o Licensing. It is likely that your service is made up of many different components, most of which have some type of licensing agreement associated with them. You will need to review each of those agreements to determine if, or how, those licenses will be affected by deployment in a cloud. If your service uses a component that is licensed by CPU and you deploy it in a cloud environment designed to launch new instances and request more resources as load increases, for example, you could easily exceed your CPU license limit. You will need to understand how your licenses affect your ability to scale.
- o Processing requirements and memory locks. If dynamic scalability is your main reason for looking to the cloud, then your application should be designed to take advantage of a parallel architecture. If the application is designed with multi-threaded

code that allows processing to be split into small chunks, it's well-suited for use within the cloud. An application that is designed around single monolithic thread processing, on the other hand, will find it difficult to take advantage of the cloud's distributed nature.

- o Communication protocol. The cloud is based on the Internet Protocol (IP), so for a 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.
- o 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.

[4.](#) Inter-Cloud Framework

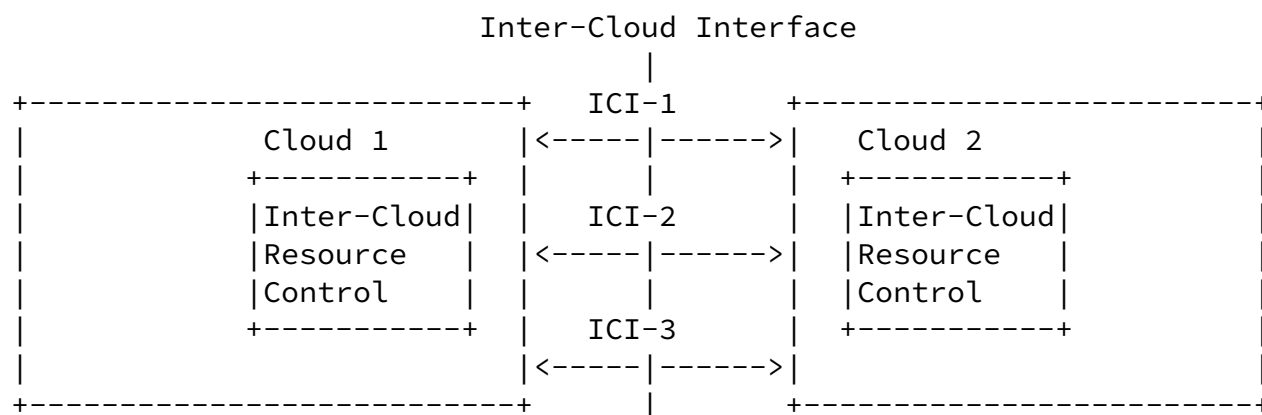
The inter-cloud interoperability and integration is motivated by a number of uses to provide multi-provider cloud services and infrastructures, multi-platform cloud services integration and traditional/legacy infrastructure services migration to clouds, and IT infrastructure services recovery or migration/move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

A Cloud Service Provider (CSP) can offer services using one or more data 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 interconnction 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).



4.1. Inter-Cloud Requirements

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

- o 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).
- o 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).

- o Provide a framework for heterogeneous inter-cloud federation
- o Facilitate interoperable and measurable intra-provider infrastructures
- o Explicit/Guaranteed intra- and inter-Cloud network infrastructure provisioning (as NaaS service model)
- o 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:

- o Provide a mechanism for resource search and discovery, to determine which serving cloud might have certain resources available (including a match making mechanism).
- o Provide a mechanism to authenticate participating entities belonging to different cloud domains.
- o Provide a mechanism for requesting, controlling, and releasing resources between two clouds.
- o Provide a secure transport channel between the interconnecting entities.
- o Provide end-to-end isolation to support multitenancy.
- o Provide a mechanism for monitoring, assuring, and troubleshooting across the interconnection.
- o 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.

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 [CNDI, I-D], XMPP [XMPP, RFC] and the Generalized Multi-Protocol Label Switching (GMPLS) [[GMPLS](#), RFC].

Main functional components include

- o Cloud Resource Manager

- o Network Infrastructure Manager

Possible ICCMP Interfaces include

- o Signaling
- o Control
- o Monitoring
- o Management
- o Location
- o Message routing

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 leverage existing platforms for federated network access and federated identity management widely used for multi-domain and multi-provider infrastructure integration [22, 23].

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.

Main functional components include

- o Trust and service broker
- o Identity provider
- o Service Registry

Internet-Draft

Cloud Reference Framework

June 2012

- o Service discovery
- o Trust manager/router
- o Attribute/namespace resolver
- o Intercloud gateway and/or attribute/namespace translator

Possible ICFF Interfaces

- o Naming, Addressing and Translation (if/as needed)
- o Publishing
- o Discovery
- o Attributes management
- o Trust/key management

[4.4.](#) Intercloud Operation Framework (ICOF)

ICOF includes functionalities to support multi-provider infrastructure operation including business workflow, SLA management, accounting, and operational security. 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.

ICOF 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 ICOF 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].

Main functional components include

- o Service Broker

- o Service Registry
- o Cloud Service Provider, Cloud Operator, Cloud (physical) Resource provider, Cloud Carrier

Khasnabish, et al. Expires December 30, 2012 [Page 24]

Internet-Draft Cloud Reference Framework June 2012

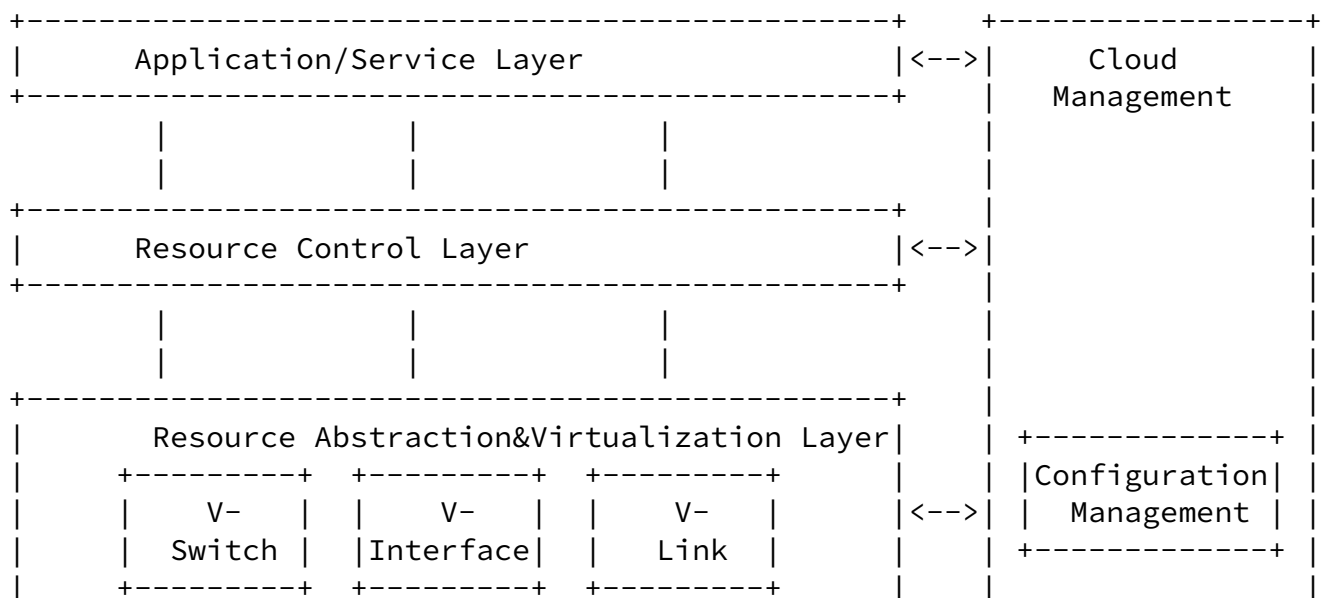
Possible ICOF Interfaces

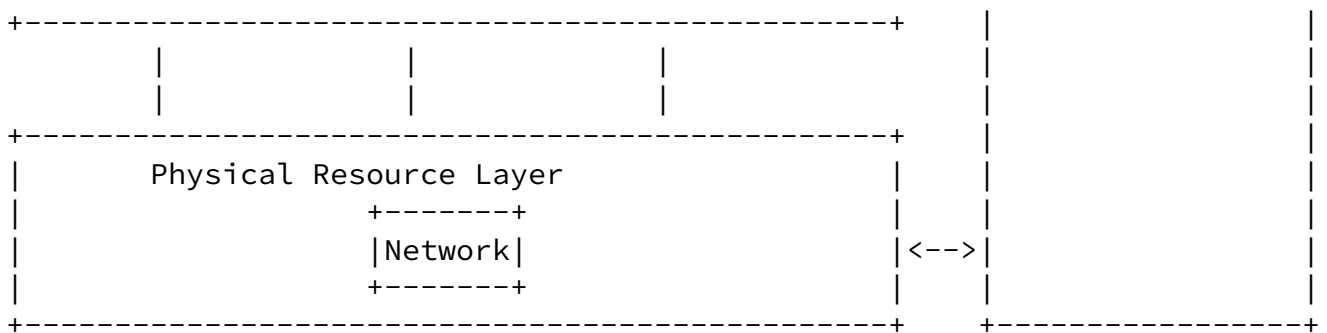
- o Provisioning, Deployment, Decommissioning/Termination
- o SLA management and negotiation
- o Services Lifecycle management
- o Services deployment

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&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

Khasnabish, et al.

Expires December 30, 2012

[Page 26]

Internet-Draft

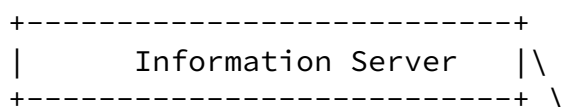
Cloud Reference Framework

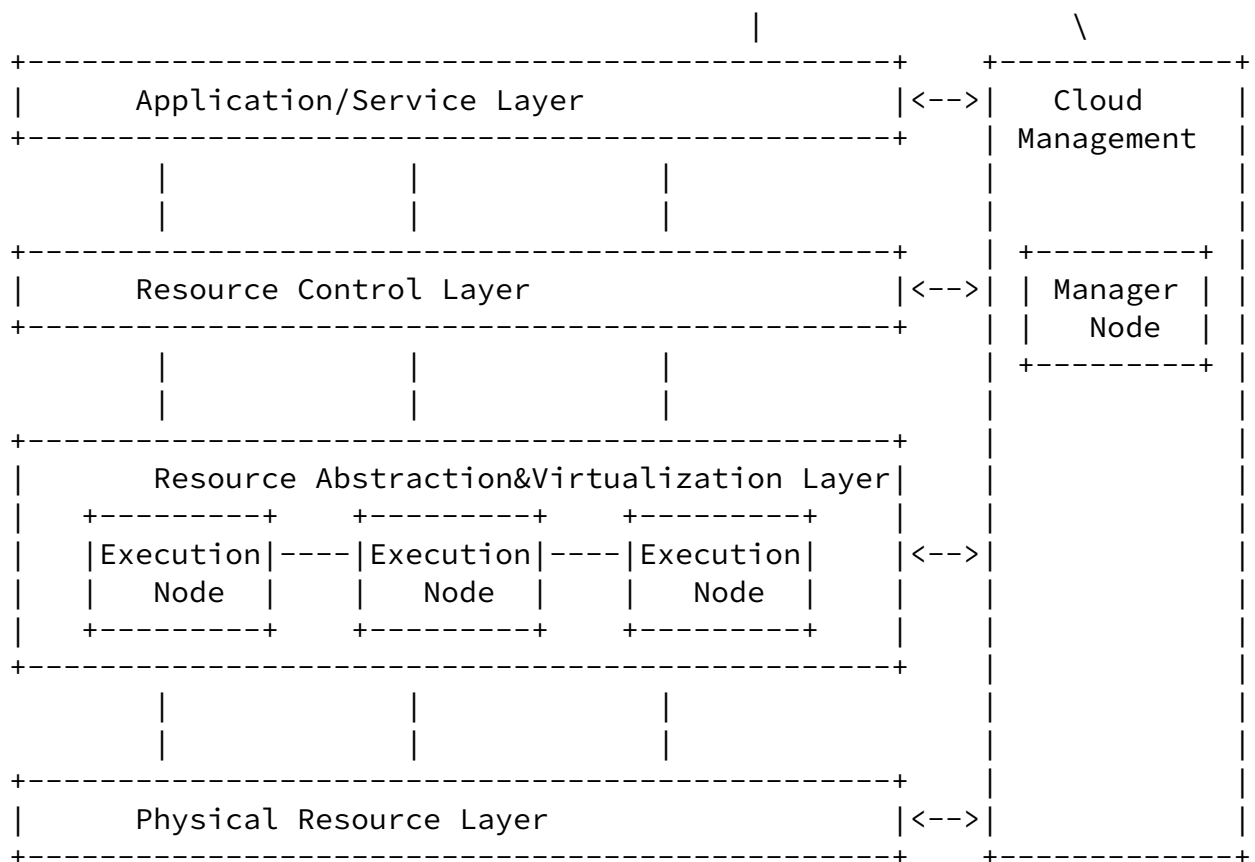
June 2012

- o scale telecom services on demand
- o improve reliability and availability
- o 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.

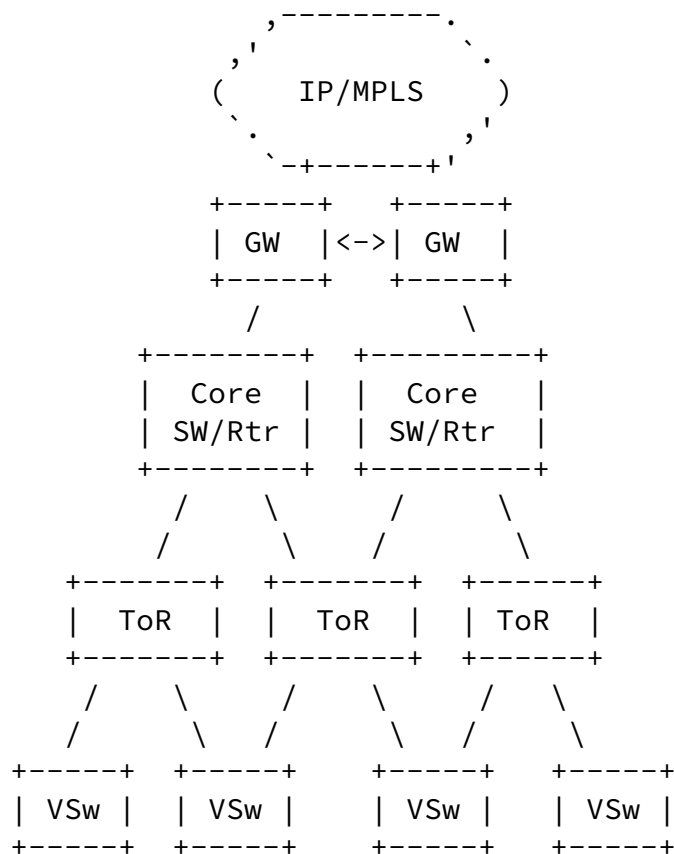
Execution Node is a physical or virtual machines on which target telecomm functions (software) are running. For example, in IMS, CSCF and HSS are candidates of functions.

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](#),



The following network components are present in a DC:

- o 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.

- o 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.

- o 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.
- o 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. 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.

- o Applications & Services: The most widely used protocol that is in use today for application & 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.
- o Infrastructure Operations & 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 & 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-00.txt](#)

[6.](#) Conclusion

We presented a high-level cloud reference framework. 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 ICOF.

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](#)].

[9.](#) IANA Considerations

This document has no actions for IANA.

[10](#). Normative references

[CDN, I-D]

IETF, "Leung, K. and Lee, Y. (2011). Content Distribution Network Interconnection (CDNI) Requirements", March 2012.

[Cloud SD0]

Khasnabish, B., "[draft-khasnabish-cloud-sdo-survey-02](#)", June 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.

[ITU-T FGCC]

FGCC, "cloud-o-0046-funct_ref_arch", 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-02](#)",
June 2012.

Khasnabish, et al. Expires December 30, 2012 [Page 35]

Internet-Draft Cloud Reference Framework June 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.
- [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 Framework", 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 1, Draft Version 0.4. SNE Techn. Report SNE-UVA-2012-03-02, 19 June 2012. [Online] <http://staff.science.uva.nl/~demch/worksinprogress/sne2012-techreport-12-05-intercloud-architecture-draft04.pdf>", 19 June 2012.
- [VDCS Security]
Karavettil, S.,
"[draft-karavettil-vdcs-security-framework-00.txt](#)",
June 2012.
- [VNet Model]

Authors' Addresses

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

Phone: +1-781-752-8003
Email: vumip1@gmail.com, bumip.khasnabish@zteusa.com

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

Meng Yu
ZTE
No.50 Ruanjian Dadao Road, Yuhuatai District
Nanjing
China

Phone: +86-25-8801-4631
Email: meng.yu@zte.com.cn

Internet-Draft

Cloud Reference Framework

June 2012

Ning So
Tata Communications
2613 Fairbourne Cir.
Plano, TX 75082
USA

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

Paul Unbehagen
Avaya
USA

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

Monique Morrow
Cisco Systems [Switzerland] 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

University of Amsterdam
Science Park 904
Amsterdam, 1098 XH
The Netherlands

Phone:

Email: y.demchenko@uva.nl