InterCloud Architecture Framework (ICAF) for Interoperability and Integration

Yuri Demchenko
SNE Group, University of Amsterdam

ISOD-RG Meeting, OGF35
18 June 2012, Delft, Netherlands

Outline

- General use cases for Intercloud Architecture
- Related standardisation initiatives
  - NIST Cloud Computing Reference Architecture (CCRA) and extension for network aware cloud resources provisioning
  - IEEE Intercloud Working Group
  - ITU-T Cloud Interest Group final report
  - OGF ISOD-RG infrastructure services definition
  - IETF Internet-Draft on Cloud Architecture Framework
- Intercloud Architectural Framework (ICA/ICAF) components
  - Multi-layer/Layered Cloud Services Model (CSM)
  - Intercloud Control and Management Plane (ICCMP)
  - Intercloud Federation Framework (ICFF)
  - Intercloud Operations Framework (ICAF)
- Abstract Model for Cloud IaaS Provisioning Model
- Possible standardisation contribution plan

SNE Cloud Research Directions

(1) Generic Cloud IaaS Architecture, Release 1, 15 April 2011
Published as http://staff.science.uva.nl/~demch/worksinprogress/sne2011-techreport-2011-03-clouds-iaas-architecture-release1.pdf

- Being developed in the framework of the GEYSERS project
- Virtual Infrastructure Composition and Management (VICM) layer
- Infrastructure Services Modeling Framework (ISMF)
- Composable Services Architecture (CSA)
- Service Delivery Framework (SDF)

(2) InterCloud Architecture

- Including InerCloud OS and InterCloud BGP-like protocol
- Network infrastructure provisioning as part of Cloud infrastructure provisioning
- Intercloud Architecture for Interoperability and Integration, Release 1, Draft Version 0.3. SNE Technical Report 2012-03-02, 11 May 2012 http://staff.science.uva.nl/~demch/worksinprogress/sne2012-techreport-12-05-intercloud-architecture-draft03.pdf

(3) Security Infrastructure for Clouds (dynamically provisioned)

- Dynamic Access Control Infrastructure (DACI)

- Following and contributing to cloud related standardisation by NIST, IEEE, IETF

General use cases for Intercloud Architecture

- Clouds are evolving as a common way of provisioning infrastructure services on-demand
  - In this way, clouds add a new type of services in addition and on the top of currently existing network based and distributed services
- Intercloud Architecture Framework (ICAF) provides a framework to support provisioning of cloud based project oriented infrastructures on-demand and distributed virtualised applications mobility
  - Hybrid Cloud/Grid e-Science collaborative environment
  - Enterprise/campus cloud infrastructure evolution and migration/mobility
  - Infrastructure disaster recovery (Vodafone NL Datacenter Incident)
  - Educational Lab deployment in clouds
- More use cases to be defined

InterCloud: Related standardisation activities

- OGF ISOD-RG
  - BCP on existing on-demand network and cloud infrastructure resources provisioning systems (including GEYSERS)
- NIST Cloud definition (NIST SP 800-145), and Cloud Computing Reference Architecture (CCRA), v1.0 (NIST SP 500-292)
- IEEE - WGs on InterCloud issues and Cloud Profiles
  - IEEE ICWG/2302 WG - Intercloud WG (ICWG) Working Group http://standards.ieee.org/develop/wg/ICWG-2302_WG.html
- ITU-T Focus Group on Cloud: Technical Report (Part 1 to 7) http://www.itu.int/en/ITU-T/focusgroups/cloud/Documents/FG-coud-technical-report.zip
- IETF Internet Drafts
  - Cloud Reference Framework. Internet Draft, by B. Khasnabish, J. Chu, S. Ma, Y. Meng, N. So, P. Unbehagen, M. Morrow, M. Hasan. http://tools.ietf.org/html/draft-khasnabish-cloud-reference-framework-02.txt
  - Cloud Service Broker, Internet Draft by Shao Weixiang, Hu Jie, Bhumip Khasnabish. http://tools.ietf.org/html/draft-shao-opsawg-cloud-service-broker-03.txt

Work on I-Draft "Cloud Reference Framework" (Version 0.2)

http://tools.ietf.org/html/draft-khasnabish-cloud-reference-framework-02.txt

B. Khasnabish
(ZTE USA)
J. Chu
S. Ma
Y. Meng
(ZTE)
N. So
(Verizon)
P. Unbehagen
Avaya
M. Morrow
(Cisco Systems Switzerland)
M. Hasan
(Cisco Systems)

Contributed
To be contributed
Under consideration

UvA's contribution is sponsored by the GEYSERS project

Intercloud Architecture - Requirements

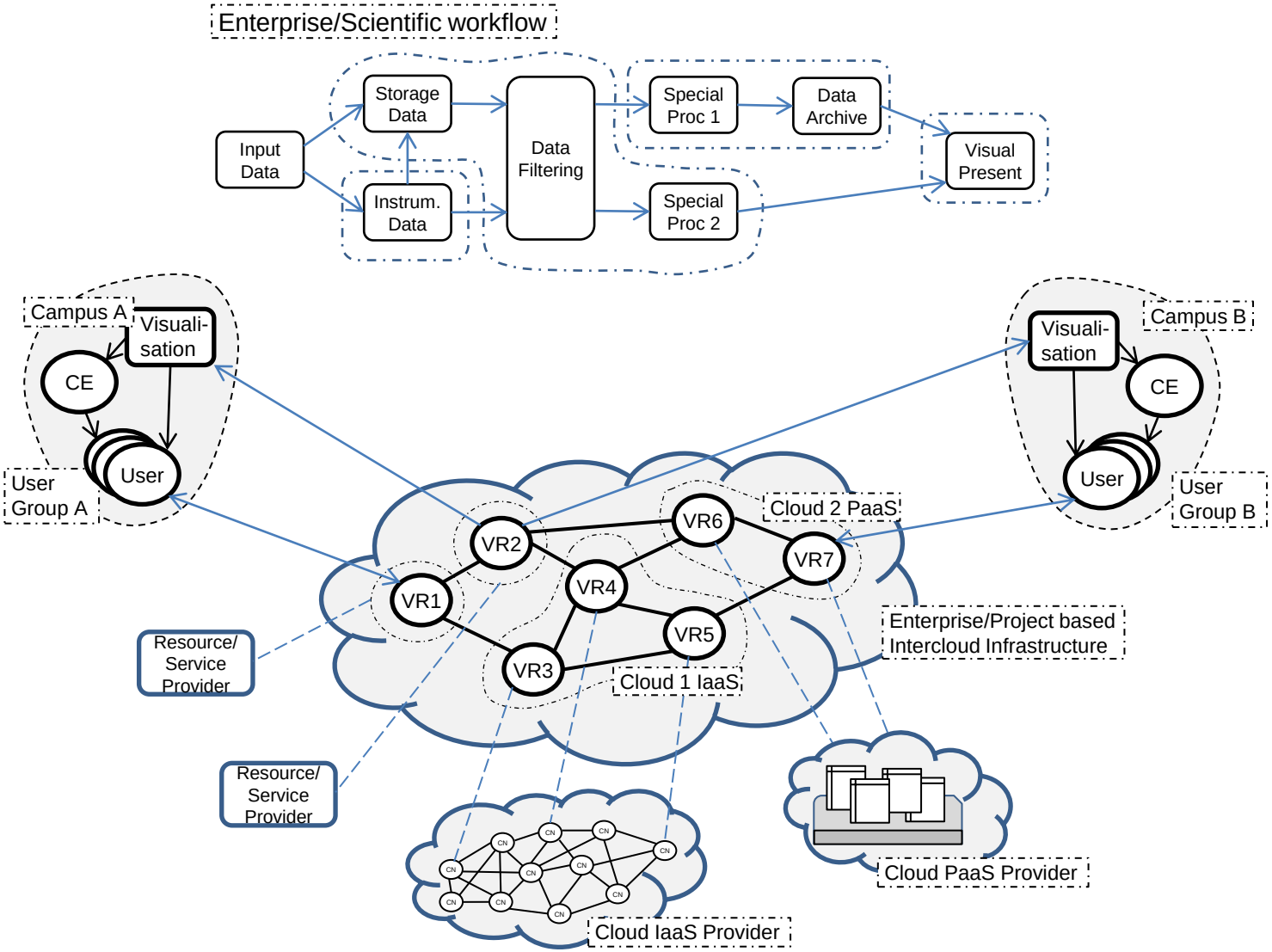
Intercloud Architecture (ICA) should address interoperability and integration of different Cloud service platforms and multi-cloud integration, including with legacy campus/enterprise infrastructure

- Provide a framework for heterogeneous inter-cloud federation
- Be compatible and provide multi-layer integration of existing Cloud service models – IaaS, PaaS, SaaS and Apps clouds
- Common Intercloud Control Plane and signalling for better cloud services and network integration
- 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
- Presumably following the same architecture patterns as Internet and Grid/OGSA
  - Provide functionalities for creating VO based infrastructures

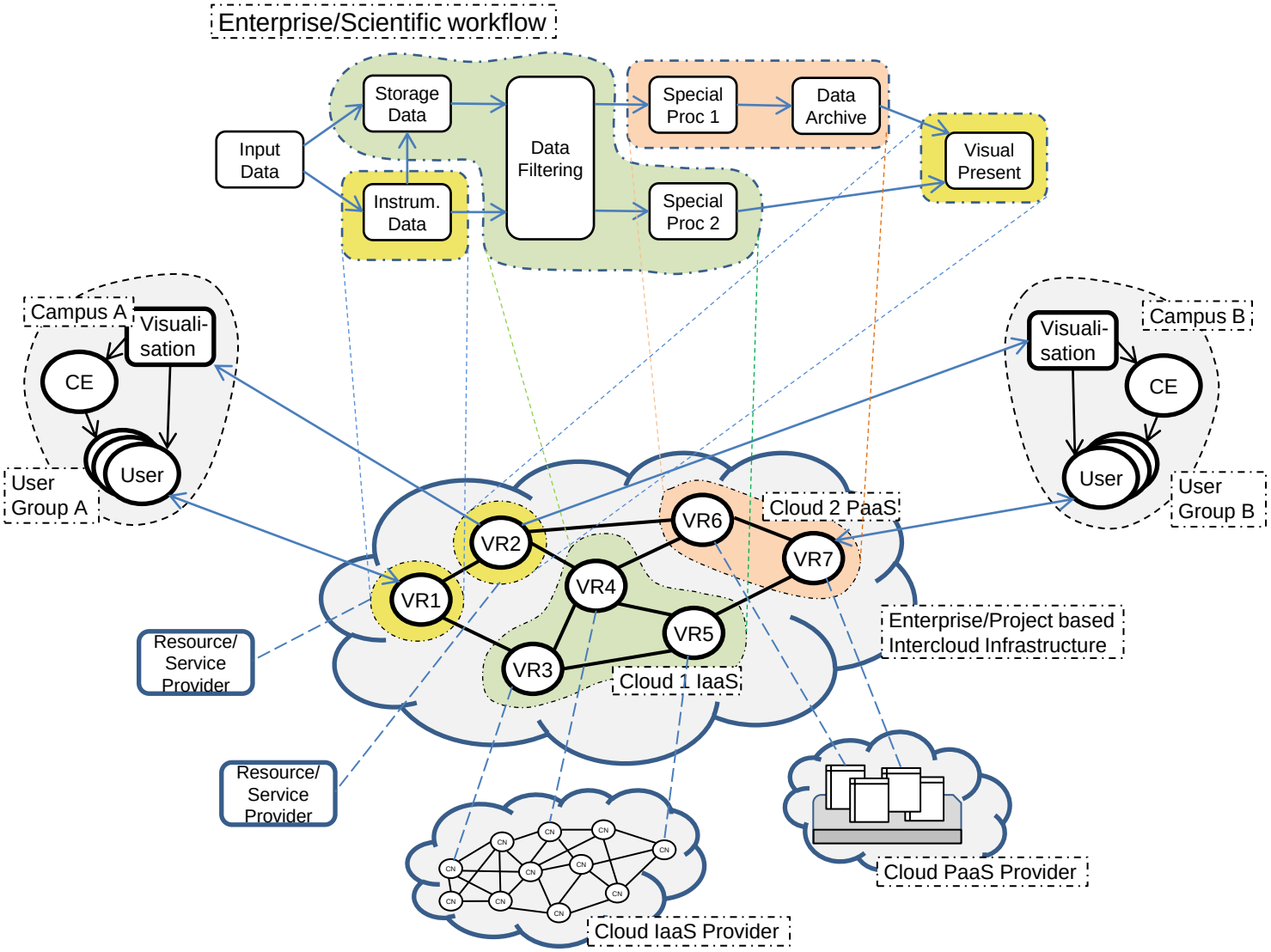
InterCloud Architecture components (Proposed)

- Multi-layer Cloud Services Model (CSM)
  - Combines IaaS, PaaS, SaaS into multi-layer model with inter-layer interfaces
  - Including interfaces definition between cloud service layers and virtualisation platform
- InterCloud Control and Management Plane (ICCMP)
  - Allows signaling, monitoring, dynamic configuration and synchronisation of the distributed heterogeneous clouds
  - Including management interface from applications to network infrastructure and virtualisation platform
- InterCloud Federation Framework (ICFF)
  - Defines set of protocols and mechanisms to ensure heterogeneous clouds integration at service and business level
  - Addresses Identity Federation, federated network access, etc.
- InterCloud Operations Framework (ICOF)
  - RORA model: Resource, Ownership, Role, Action
    - RORA model provides basis for business processes definition, SLA and access control
  - Broker and federation operation

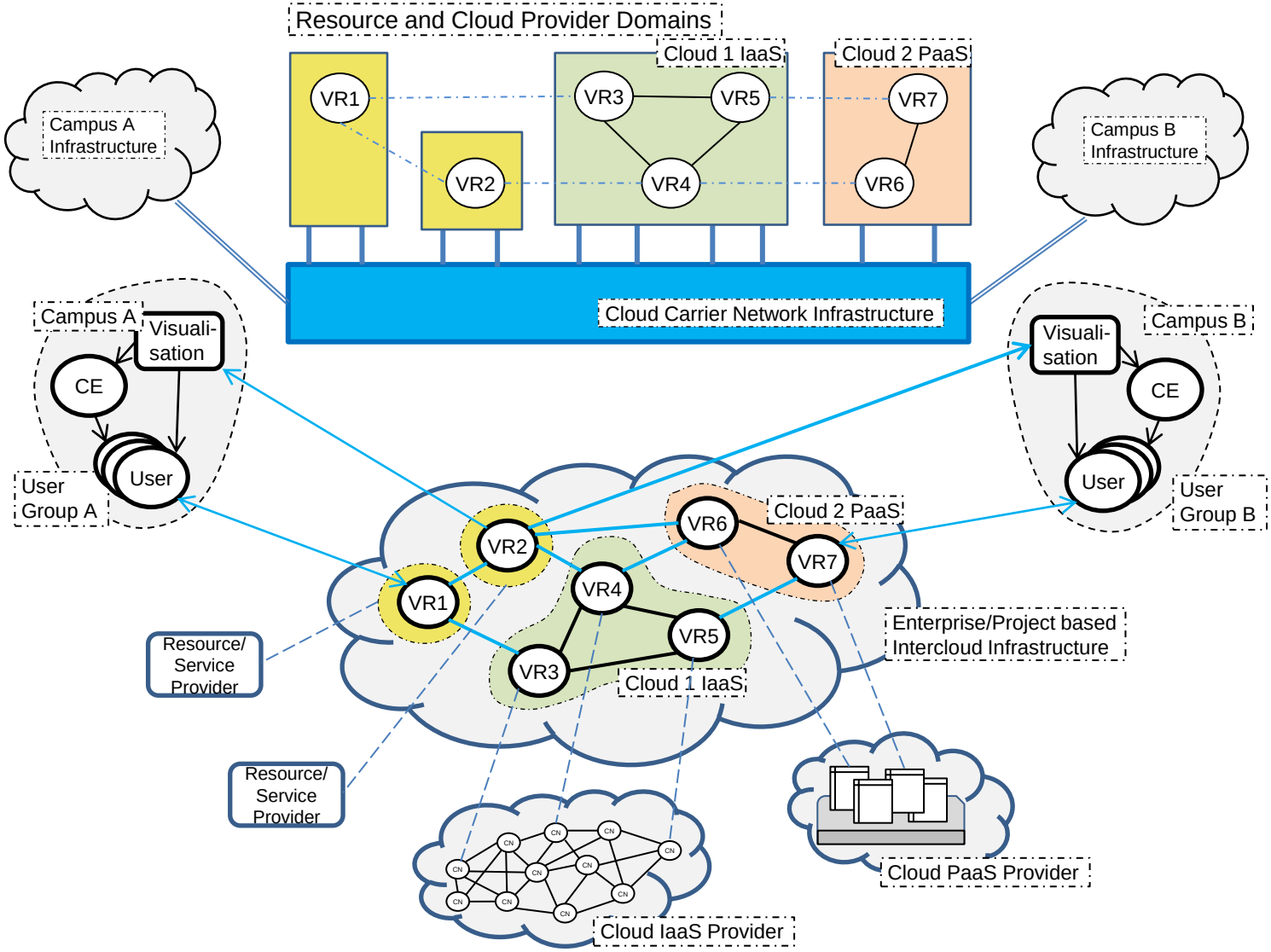
General use case for infrastructure provisioning: Workflow => Logical (Cloud) Infrastructure



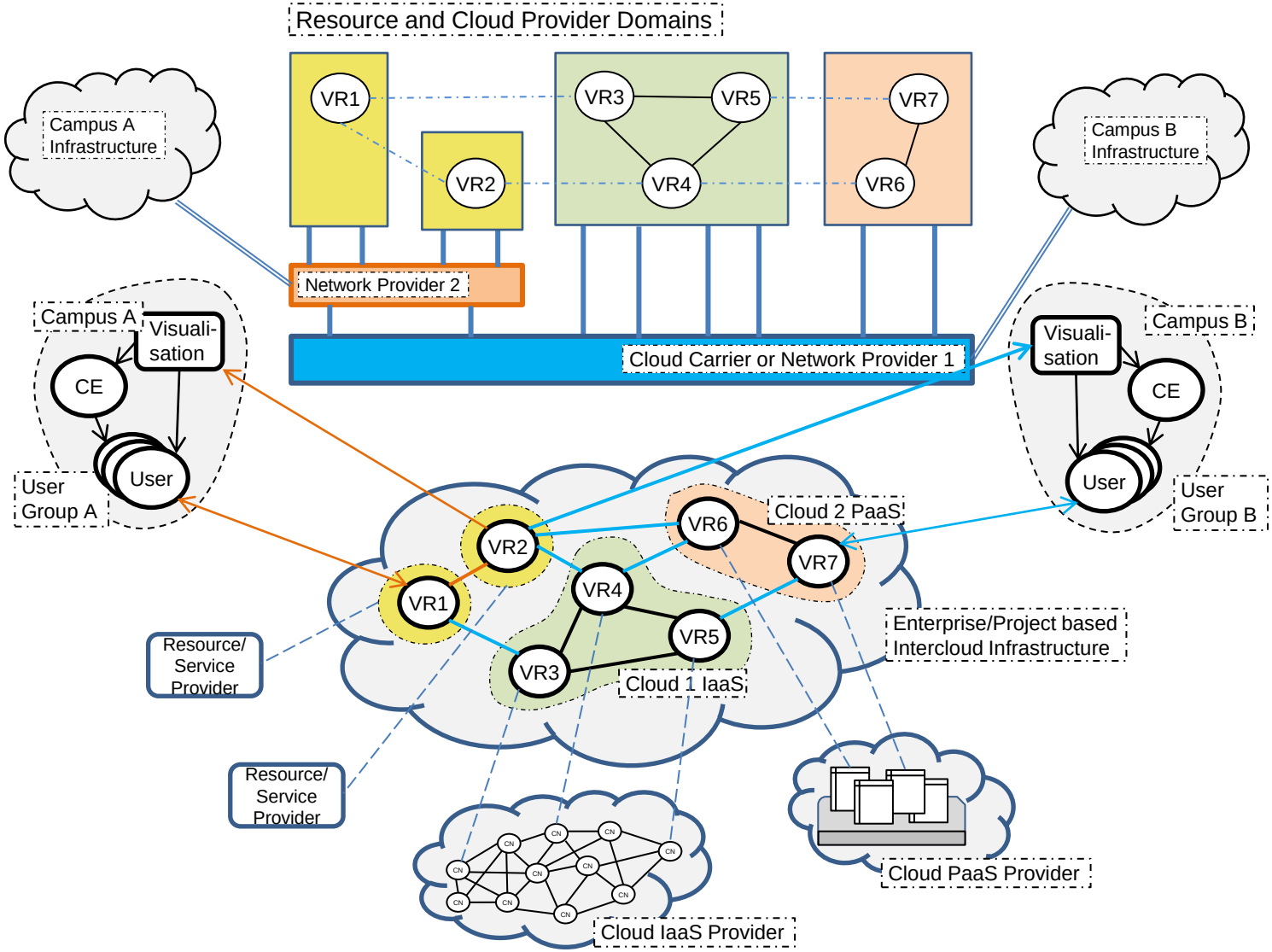
General use case for infrastructure provisioning: Workflow => Logical (Cloud) Infrastructure



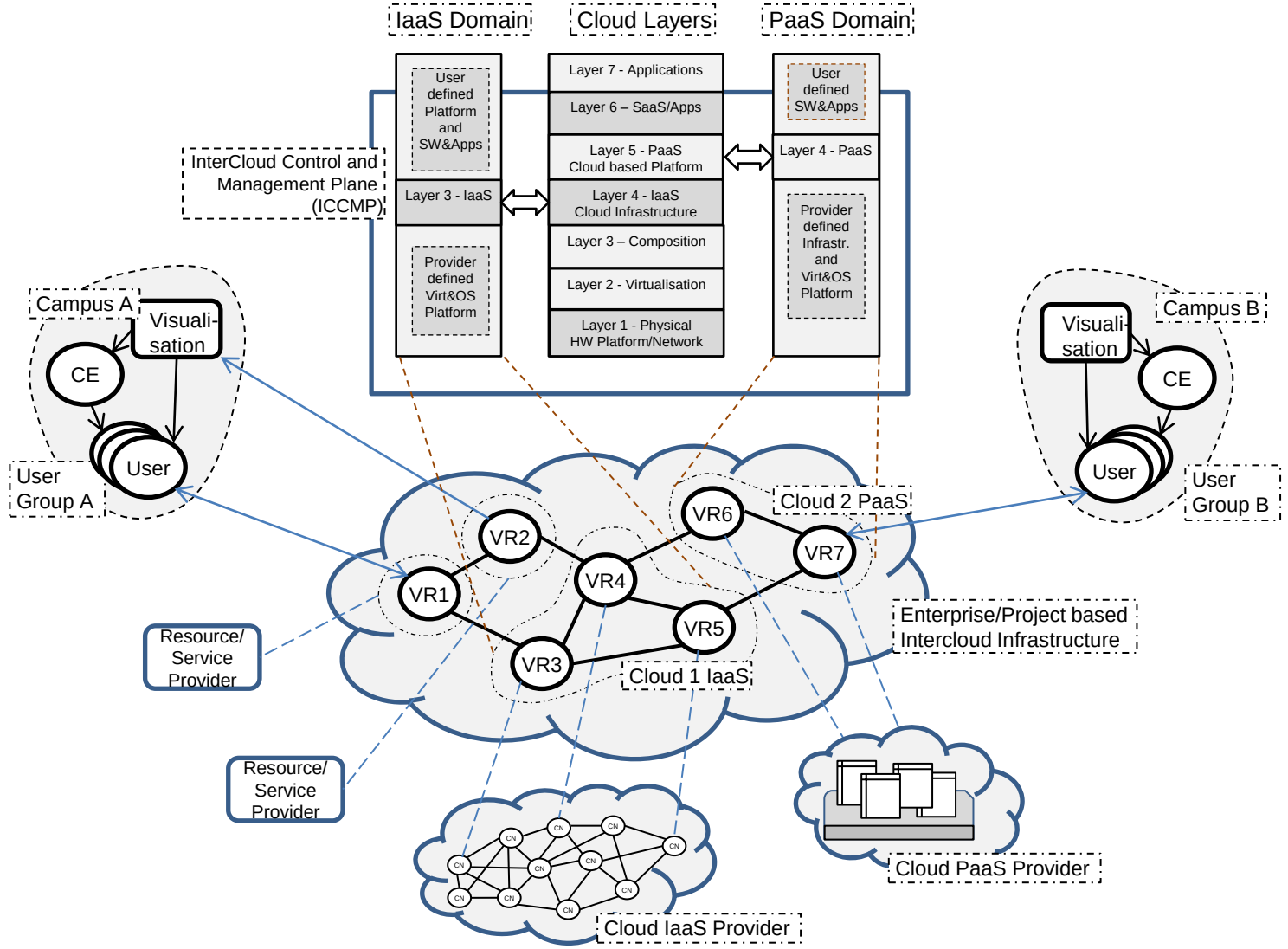
General use case for infrastructure provisioning: Logical Infrastructure => Network Infrastructure (1)



General use case for infrastructure provisioning: Logical Infrastructure => Network Infrastructure (2)



Multi-cloud Integration and Interoperability



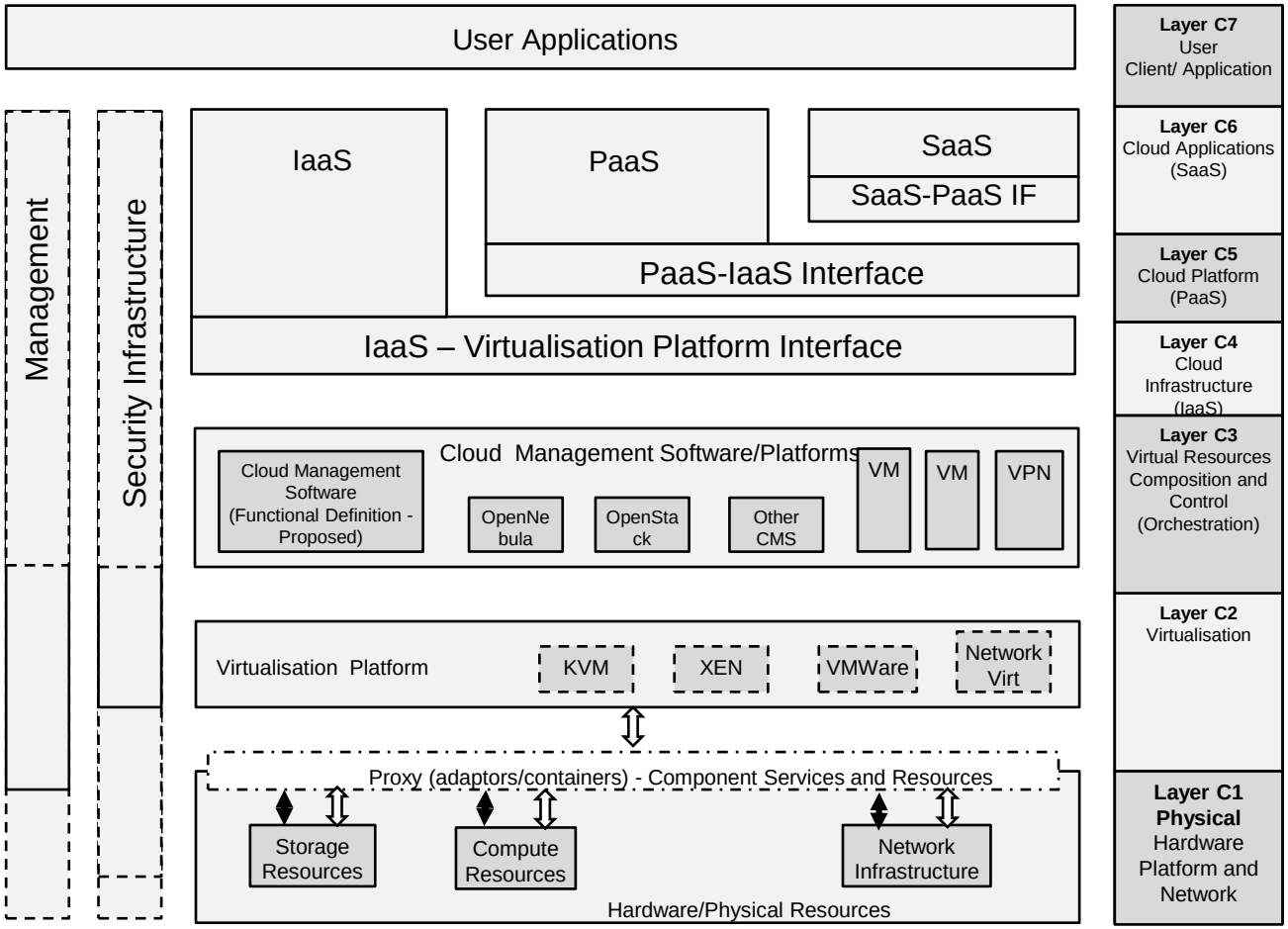
InterCloud Architecture components

- Multi-layer Cloud Services Model (CSM)
  - Combines IaaS, PaaS, SaaS into multi-layer model with inter-layer interfaces
  - Including interfaces definition between cloud service layers and virtualisation platform
- InterCloud Control and Management Plane (ICCMP)
  - Allows signaling, monitoring, dynamic configuration and synchronisation of the distributed heterogeneous clouds
  - Including management interface from applications to network infrastructure and virtualisation platform
- InterCloud Federation Framework (ICFF)
  - Defines set of protocols and mechanisms to ensure heterogeneous clouds integration at service and business level
  - Addresses Identity Federation, federated network access, etc.
- InterCloud Operations Framework (ICOF)
  - RORA model: Resource, Ownership, Role, Action
    - RORA model provides basis for business processes definition, SLA and access control
  - Broker and federation operation

Multi-layer Cloud Services Model (CSM)

- Combines IaaS, PaaS, SaaS into multi-layer model with inter-layer interfaces
- Including interfaces definition between cloud service layers and virtualisation platform

Multilayer Cloud Services Model (CSM)



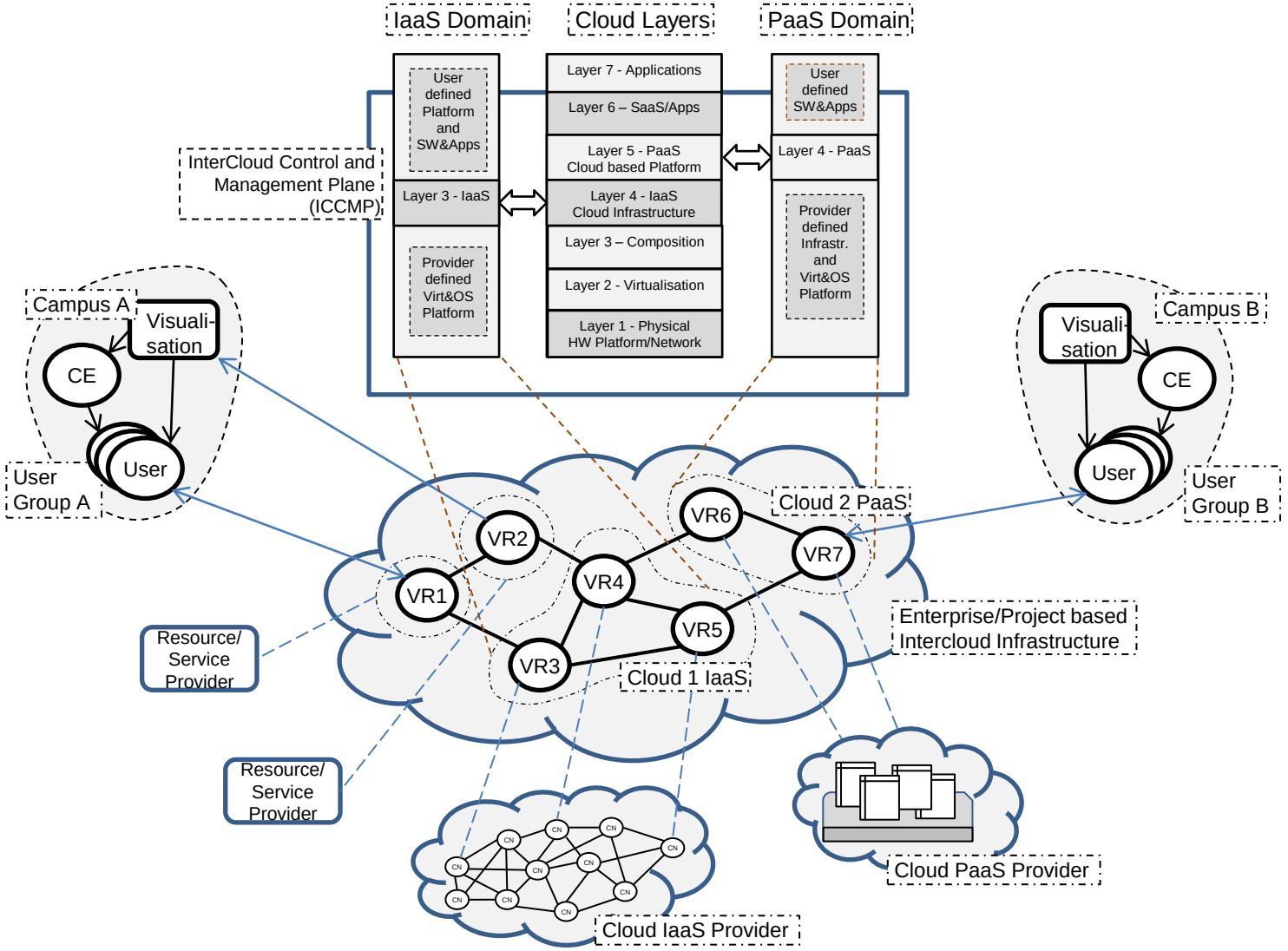
CSM layers

(C7) User Client/Application
(C6) Cloud Application (SaaS)
(C5) Cloud Platform (PaaS)
(C4) Cloud Infrastructure (IaaS)
(C3) Virtual Resources Composition and Orchestration
(C2) Virtualisation Layer
(C1) Hardware platform and dedicated network infrastructure

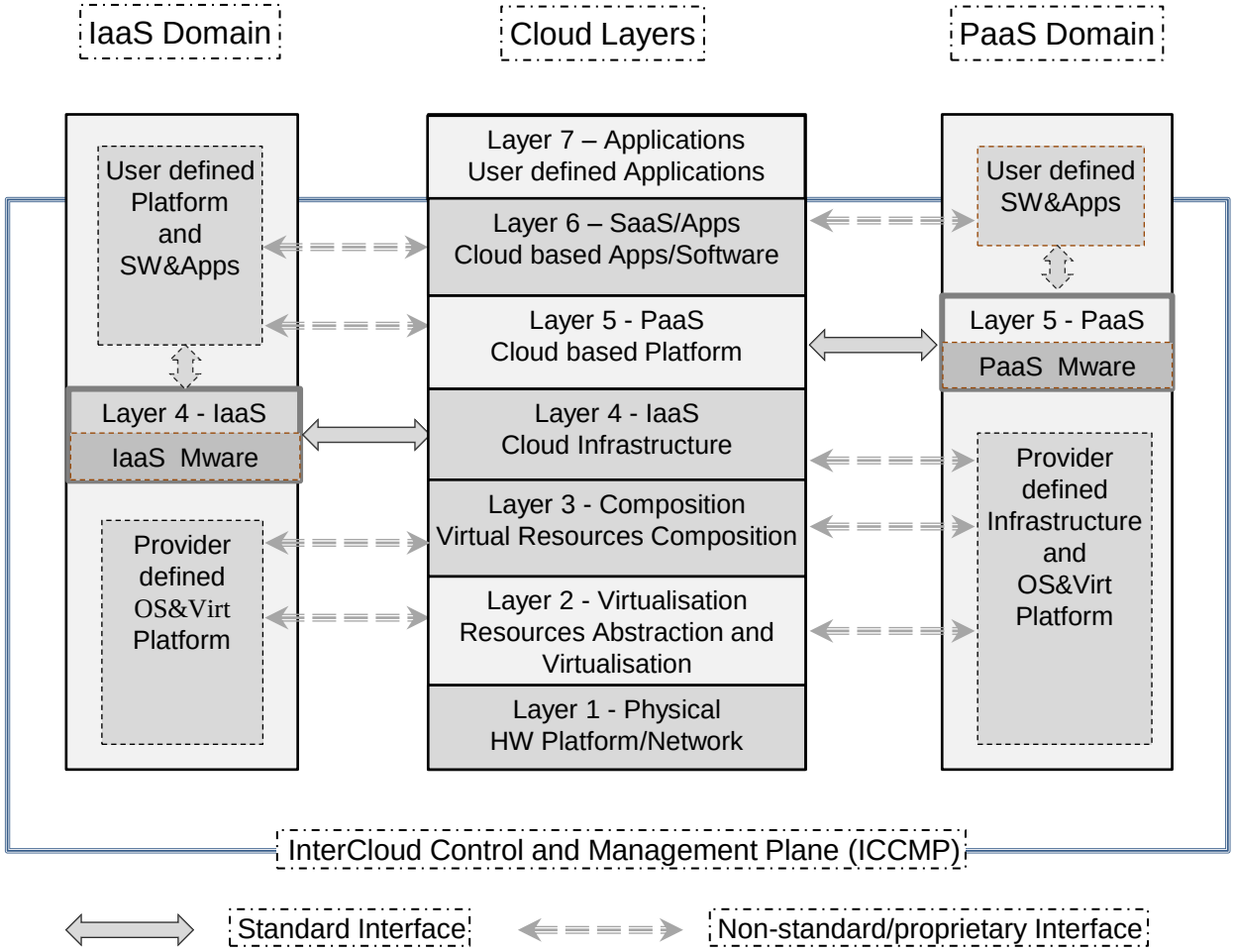
InterCloud Control and Management Plane (ICCMP)

- Supports signaling, monitoring, dynamic configuration and synchronisation of the distributed heterogeneous clouds
- Includes management interface from upper layers and applications to network infrastructure and virtualisation platform

Intercloud Control and Management (1)



Intercloud Control and Management (2)



InterCloud Control and Management Plane (ICCMP)

- Allows signaling, monitoring, dynamic configuration and synchronisation of the distributed heterogeneous clouds
- Including management interface from applications to network infrastructure and virtualisation platform
- Main functional components include
  - Cloud Resource Manager
  - Network Infrastructure Manager
  - *To be added*
- Possible ICCMP Interfaces include
  - Control
  - Signaling
  - Message routing
  - Management
  - Monitoring
  - Location

InterCloud Federation Framework (ICFF)

- Defines set of protocols and mechanisms to ensure heterogeneous clouds integration at service and business level
- Addresses Identity Federation, federated network access, etc.
- Main functional components include
  - Intercloud gateway and/or attribute/namespace translator
  - Service Registry
  - Service discovery
  - Identity provider
  - Attribute/namespace resolver
  - (Service broker)
  - (Trust broker)
  - Trust manager/router
- Possible ICFF Interfaces
  - Naming, Addressing and Translation (if/as needed)
  - Publishing
  - Discovery
  - Attributes management
  - Trust/key management

InterCloud Operations Framework (ICOF)

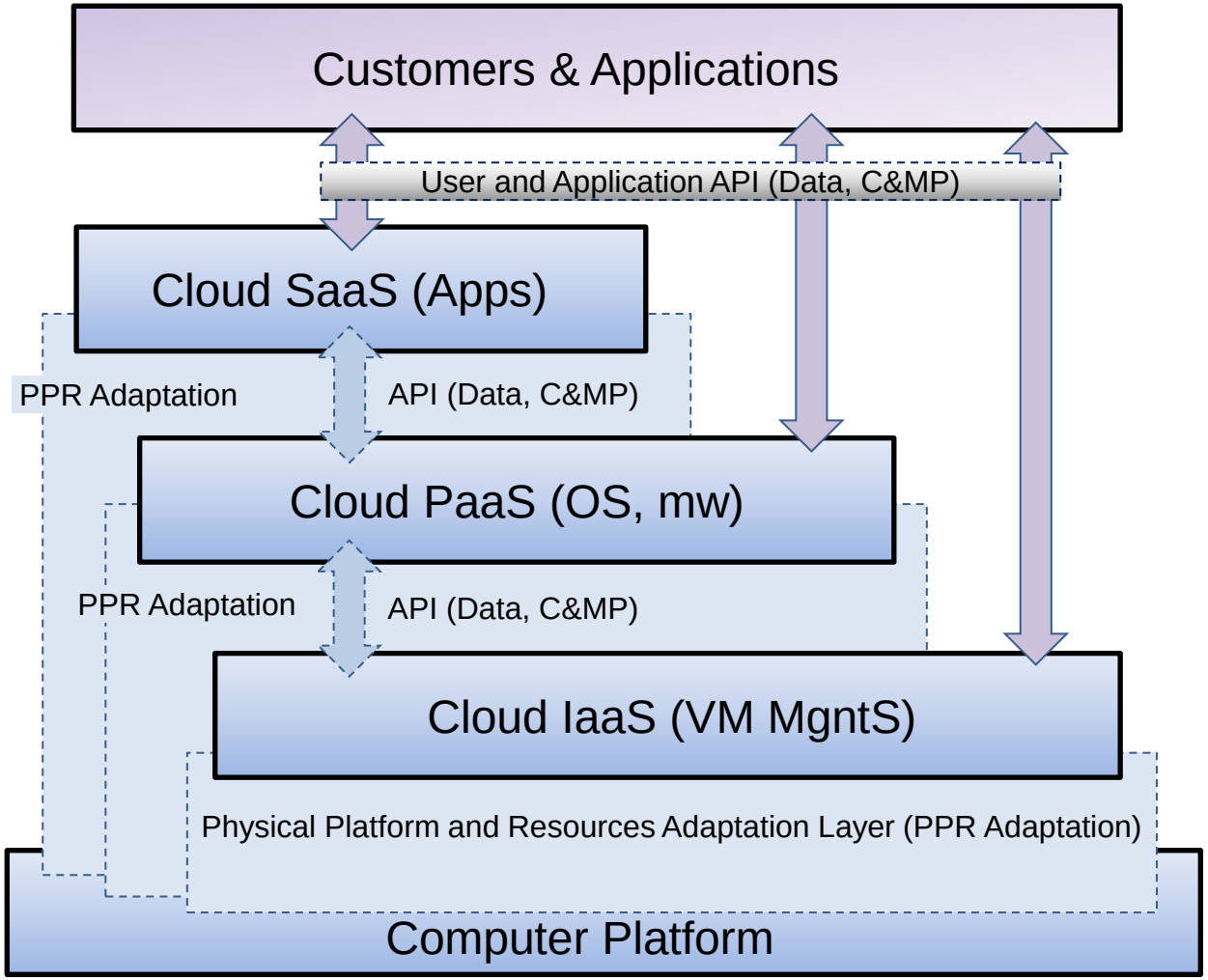
- Defines the main roles and actors
  - RORA model: Resource, Ownership, Role, Action
    - Provides basis for business processes definition, SLA management and access control policy definition
- Broker and Federation operation
- Main functional components include
  - Service Broker
  - Service Registry
  - Cloud Service Provider, Cloud Operator, Cloud (physical) Resource provider, Cloud Carrier
- Possible ICOF Interfaces
  - Provisioning, Deployment, Decommissioning/Termination
  - SLA management and negotiation
  - Services Lifecycle management
  - Services deployment

Main Actors in Cloud/InterCloud Architecture

- Cloud Service Provider
- Cloud Customer
- Cloud User
- Cloud Carrier (Cloud network provider)
- Intercloud (Cloud Service) Operator
- Cloud Broker
  - ITU-T analogy: Last resort carrier, i.e. local provider
- Cloud Auditor
- Cloud Resource Provider
- Physical Resource Provider
  - Can also be a “fixed” resources provider interfaced by Cloud Provider

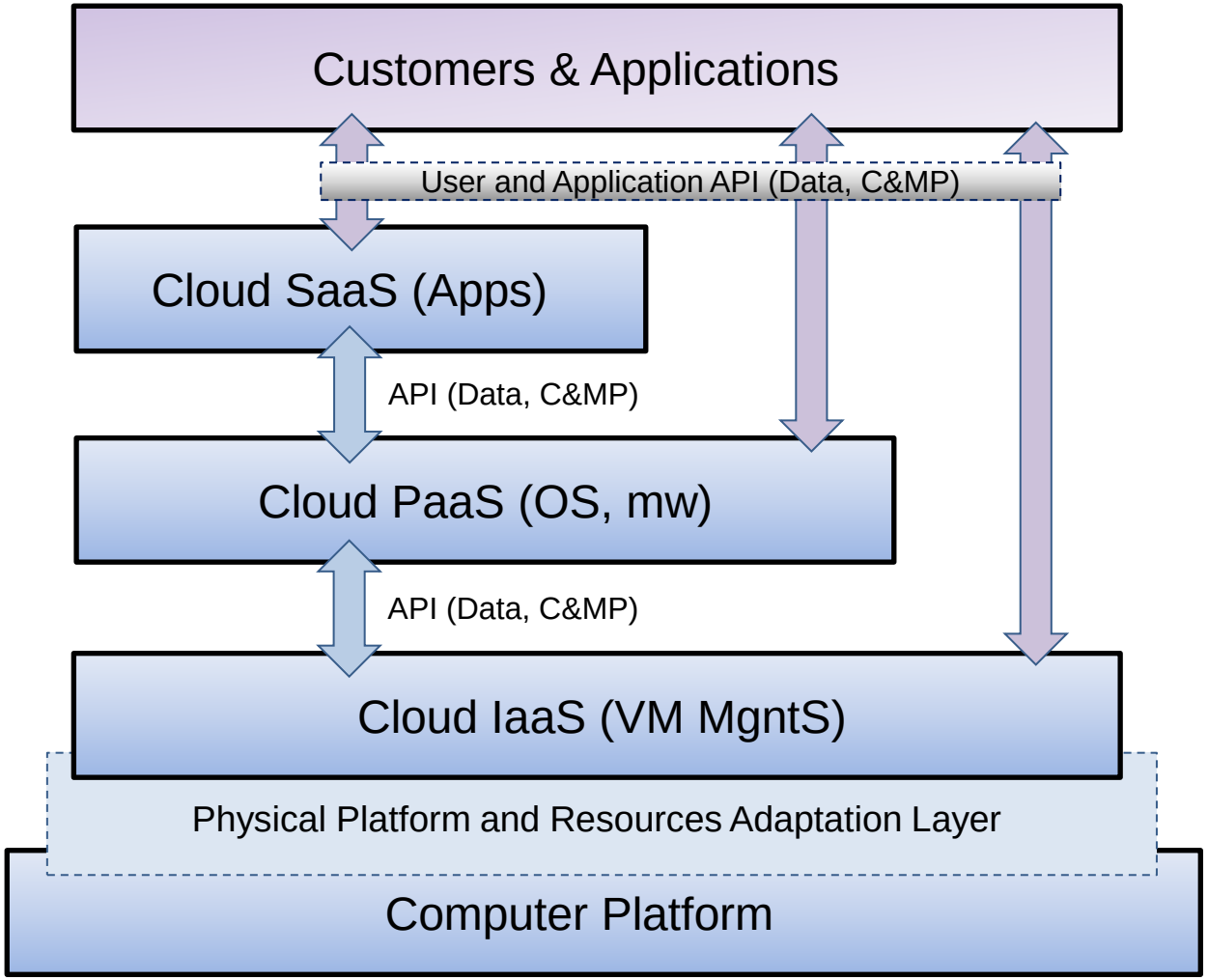
Ownership/Management model need to be applied to these actors using extended RORA model

Current relation between Cloud services models



- Cloud service models IaaS, PaaS, SaaS use proprietary Physical Platform and Resources Adaptation Layer
  - Limited control over network services provisioning and QoS
- Public User and application interfaces
  - Data and Control&Management functions

Proposed Interlayer Cloud Services Integration



- Standardisation API's between different Cloud service models
  - Interacting as Cloud infrastructure layers
- Cloud/ICA inter-layer API
  - For application data communication
  - For Control and Management
    - Services lifecycle management
  - Security context management
  - May be run at provider or customer side
- Explicit network infrastructure provisioning as NaaS
- ***OGF OCCI can be a basis for all layer related API's***

Defining CSM Inter-layer API's

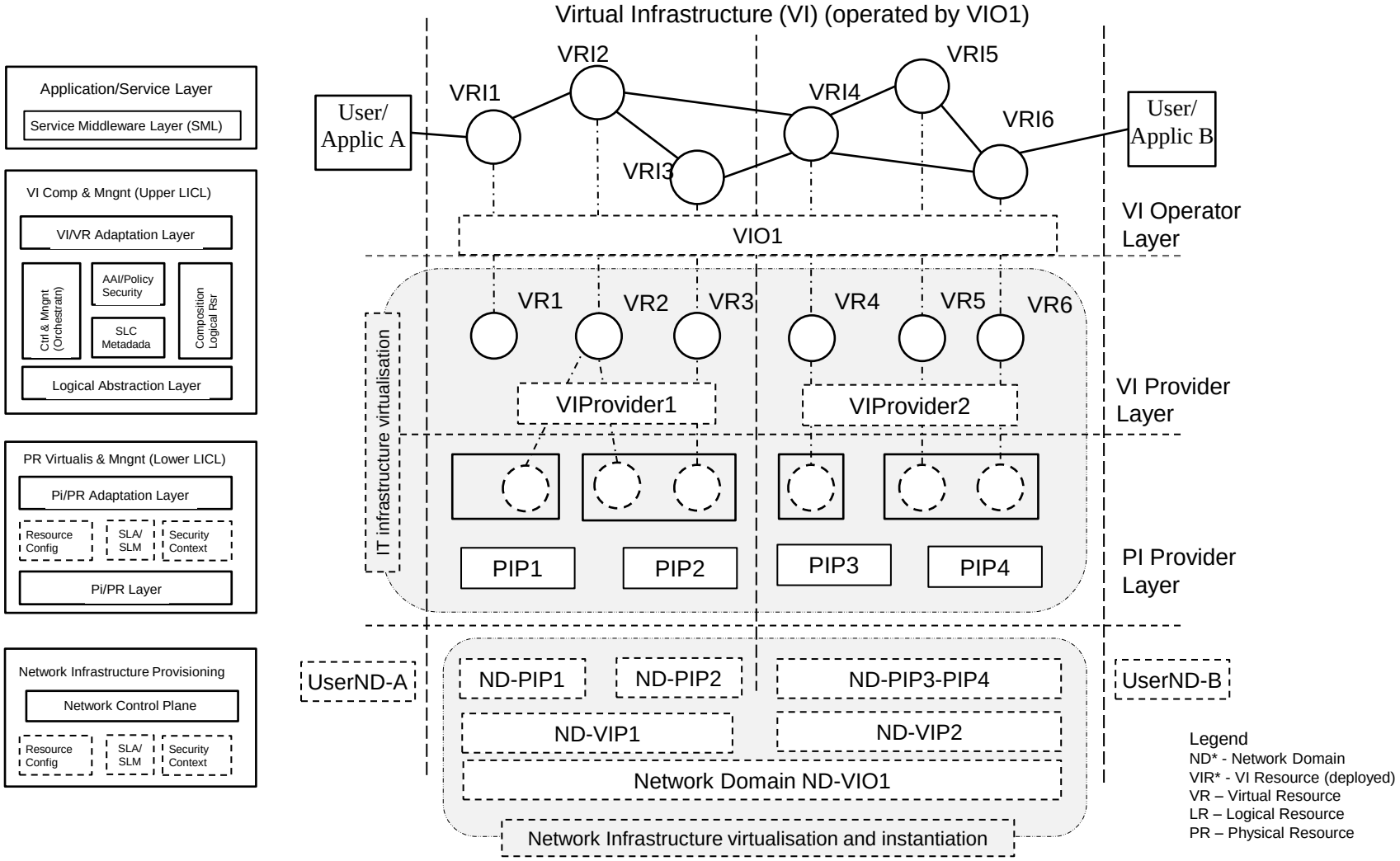
- Intercloud Architecture (ICA) should address interoperability of different cloud service platforms and multi-cloud integration, including with legacy campus infrastructure
- Define Intercloud protocols and API's stack
  - VI-API – IaaS API
  - P-API – PaaS API
  - SA-API – Software (and applications) API
  - *OCCI can be a base for defining most of APIs*
- Depending on service model, some API's may be run by providers and some by customers/users

Architectural Framework for Cloud IaaS

- Abstracted from the GEYSERS LICL (Logical Infrastructure Composition Layer)
- Includes Composable Services Architecture (CSA) being developed in GEANT3 JRA3
- Incorporates NDL, NML, ISDL research at SNE/UvA
- Includes the following main components
  - Infrastructure Services Modeling Framework (ISMF)
  - Composable Services Architecture (CSA)
  - Service Delivery Framework (SDF)
- Additional components (orthogonal)
  - Cloud Security Infrastructure
  - Control and Management Plane

Published as SNE Technical Report (2011)
http://staff.science.uva.nl/~demch/worksinprogress/sne2011-techreport-2011-03-clouds-iaas-architecture-release1.pdf

Abstract IaaS Provisioning Model



Proposed Architectural Framework for Cloud IaaS

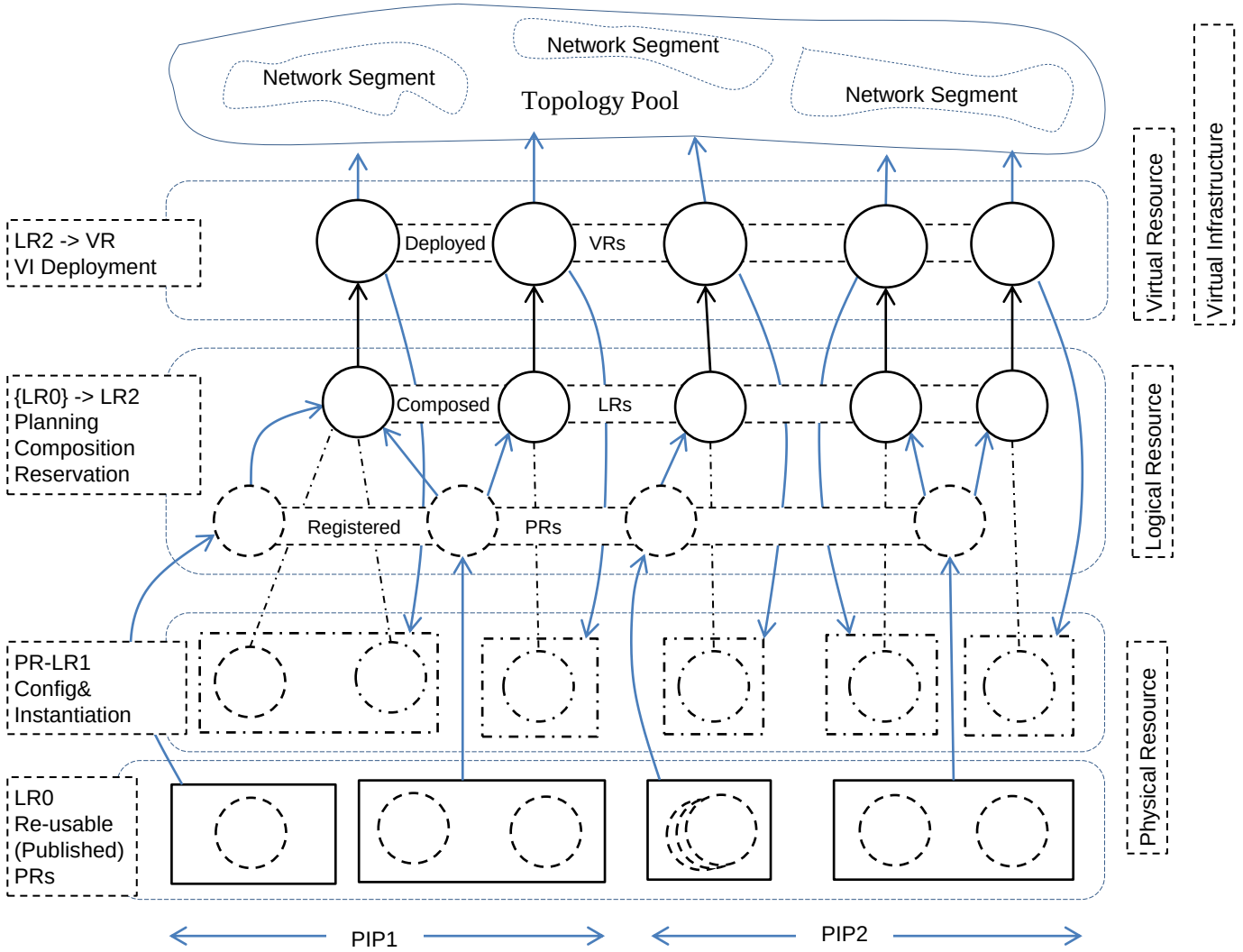
The proposed framework should support on-demand infrastructure services provisioning and operation

- **Composable Services Architecture (CSA)** that intends to provide a conceptual and methodological framework for developing dynamically configurable virtualised infrastructure services
- **Service Delivery Framework (SDF)** that provides a basis for defining the whole composable services life cycle management and supporting infrastructure services
- **Infrastructure Services Modeling Framework (ISMF)** that provides a basis for the infrastructure resources virtualisation and management, including description, discovery, modeling, composition and monitoring
- (Additionally) ***Service Control and Management Plane/Framework*** may be defined as combination of management functionality in all 3 components
- (Additionally) ***Security services/infrastructure*** have a dual role:
  - Virtual Security Infrastructure - provisioned as a part of virtualised infrastructure
  - Support normal/secure operation of the whole provisioning framework

Virtual Infrastructure Composition and Management (VICM) Layer Operation

- Main actors involved into provisioning process
  - Physical Infrastructure Provider (PIP)
  - Virtual Infrastructure Provider (VIP)
  - Virtual Infrastructure Operator (VIO)
- Virtual Infrastructure Composition and Management (VICM) layer includes
  - VICM middleware - defined as CSA
  - Logical Abstraction Layer and the VI/VR Adaptation Layer facing correspondingly lower PIP and upper Application layer.
- The infrastructure provisioning process is defined by the Service Delivery Framework (SDF)
- VICM redefines Logical Infrastructure Composition Layer (LICL) proposed by GEYSERS project
  - Basic functionality is implemented as GEMBus/ESB/CSA

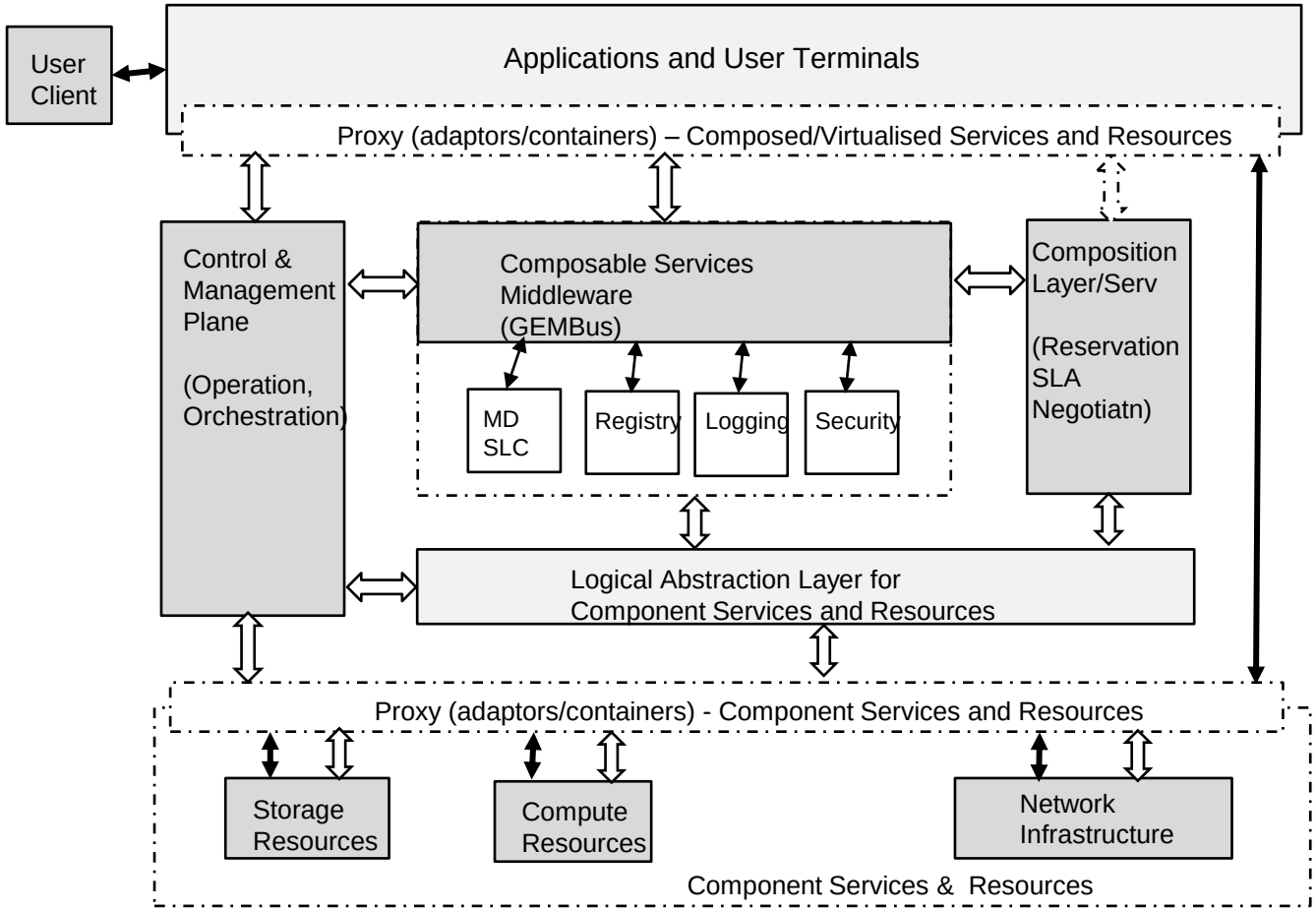
ISMF – Virtual Resource Lifecycle



ISMF - Relation between PR-LR-VR-VI

- Virtual Resource lifecycle – defines relations between different resource presentations along the provisioning process
- Physical Resource information is published by PIP to the Registry service serving VICM and VIP
  - Logical Resource representing PR includes also properties that define possible (topological) operations on the PR, such as e.g. partitioning or aggregation.
- Published LR information presented in the commonly adopted form (using common data or semantic model) is then used by VICM/VIP composition service to create requested infrastructure as combination of (instantiated) Virtual Resources and interconnecting them with the available network infrastructure
- Network infrastructure can be composed of a few network segments (from the network topology pool) run by different network providers.
- Composed LRs are deployed as VRI/VI to VIP/VIO and as virtualised/instantiated PR-LR to PIP
- Resource/service description format considered
  - NDL/NML (Network Description Language / Network Markup Language at OGF)
  - Compatibility with VXDL infrastructure service request format by INRIA

Composable Services Architecture (CSA)



Composable Services lifecycle/provisioning stages
(1) Request
(2) Composition/ Reservation
(3) Deployment
(4) Operation
(5) Decommissioning

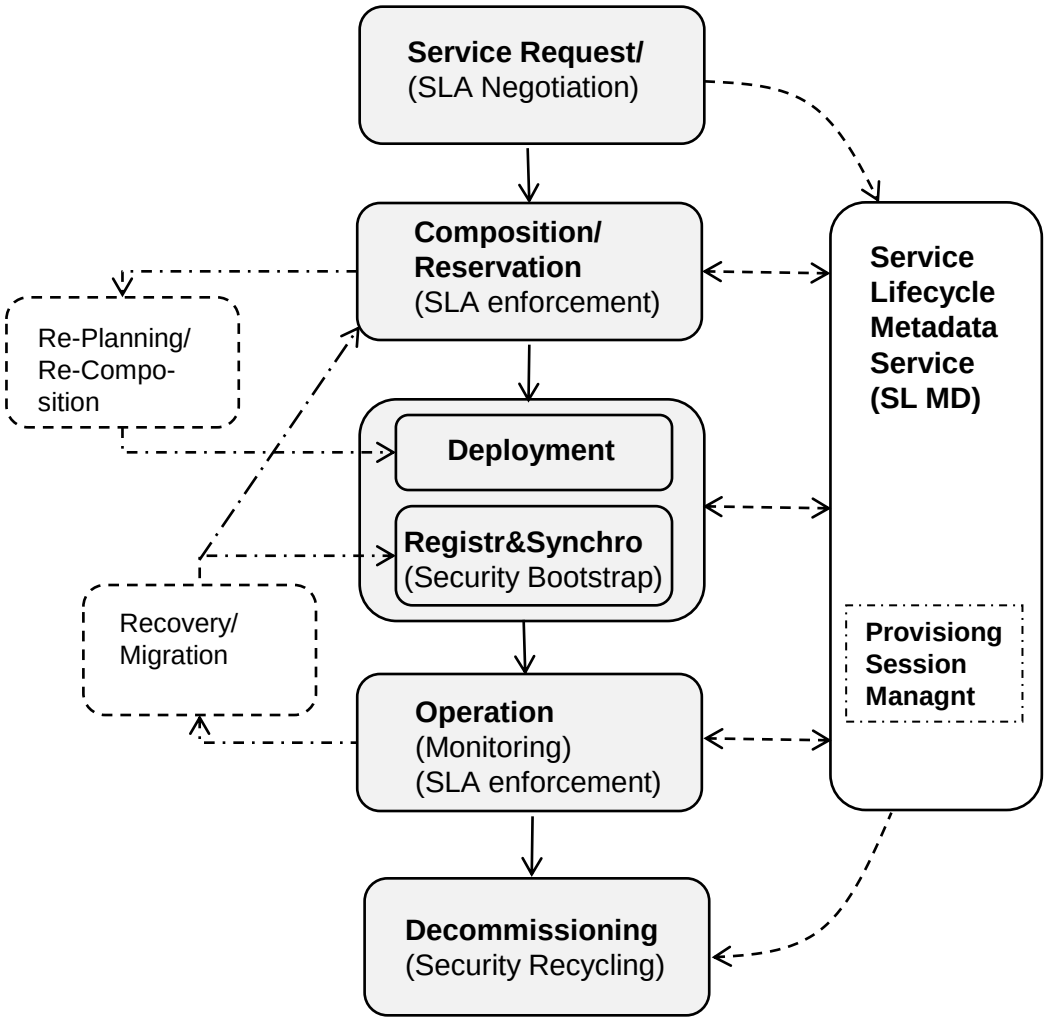
Defined as middleware for on-demand provisioned Composable Services

Proposed in the GEANT3 JRA3 Composable Services project and being implemented as

Control/ Mngnt Links

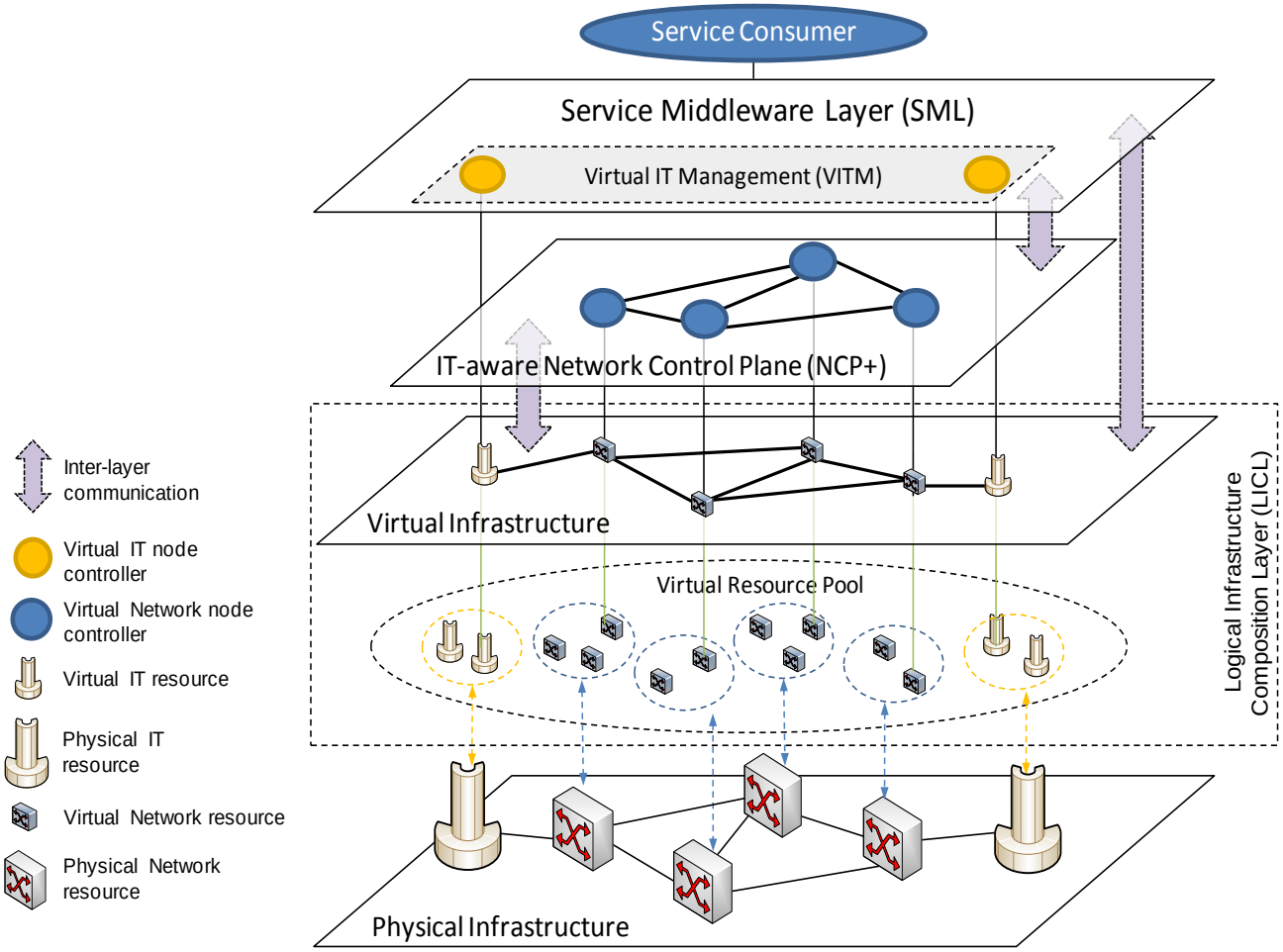
Data Links

Composable Services Lifecycle/Provisioning Workflow



- Main stages/phases
  - **Service Request** (including SLA negotiation)
  - **Composition/Reservation** (aka design)
  - **Deployment**, including Reqistration/Synchronisation
  - **Operation** (including Monitoring and SLA enforcement)
  - **Decommissioning** (including Dynamic Security Associations destroying/recycling)
- Additional stages
  - **Re-Planning**/Re-Composition should address incremental infrastructure changes
  - **Recovery/Migration** can use SL-MD to initiate resources re-synchronisation but may require re-composition
- The whole workflow is supported by the Service Lifecycle Metadata Service (SL MD)
- Provisioning session provides a framework for services context and security context management

GEYSERS Layered Architecture – CSM and ICCMP



- Developed and implemented in the GEYSERS project http://www.geysers.eu/

Additional Information

- NIST Cloud definition and standardisation activity
- Useful links on Cloud standardisation and practice

Questions to answer regarding ICA

- Network provisioning in connection to IT resources provisioning – what's first
- Cloud Broker vas Cloud Operator
  - Broker role similar to telephone network
- Firewall and its role?
  - Difference between host based and VM based
- Particular: Link to ALBL-FR architecture of Composition and Orchestration functional framework

Use case 2: Educational Lab (mobility)

- Educational lab is created for a specific course in one university
  - A course is computing intensive and has periodicity of one semester
    - The required infrastructure is expensive and is deployed on Cloud (generally multiple)
  - First installation requires significant efforts that need to preserved
- Between periodic course runs the Lab will be dormant or should be suspended and resumed for the next term
  - Used/required Cloud resources may change/evolve
- The Lab may need to be moved to another university with different campus network installation and available Cloud providers
  - Requires Cloud services standardisation and interoperability

InterCloud: Related standardisation activities

- IEEE - WGs on InterCloud issues and Cloud Profiles
  - IEEE ICWG/2302 WG - Intercloud WG (ICWG) Working Group http://standards.ieee.org/develop/wg/ICWG-2302_WG.html
  - CPWG/2301 WG - Cloud Profiles WG (CPWG) Working Group http://standards.ieee.org/develop/wg/CPWG-2301_WG.html
- DMTF OVF (http://www.dmtf.org/standards/ovf)
  - Supported by VMware OVF Tool 2.0
- VMware vApp
  - http://labs.vmware.com/flings/vapprun

vApp by VMware

- vApp container for distributed multi-VM solution
  - Decouples application from the deployment platform
  - Built on top of OVF2.0
  - Implemented as a vApprun package
    http://labs.vmware.com/flings/vapprun
- Concept of a vService dependency is used to decouple a vApp from infrastructure services and to support mobility between cloud providers

vApp: a standards-based container for cloud providers, by R.Schmidt, S.Grarup
http://portal.acm.org/citation.cfm?id=1899943

OpenStack

- Intends to address all Cloud services models http://www.openstack.org/
  - Highly modular architecture
  - IaaS, PaaS, SaaS
  - Network provisioning as pluggable module
- Open for cooperation
  - Good contacts with OpenNebula team

NIST Publications on Cloud Computing

- [NIST CC] NIST SP 800-145, “A NIST definition of cloud computing”, [online] Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- [NIST CCRA] NIST SP 500-292, Cloud Computing Reference Architecture, v1.0. [Online] http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf
- [NIST Synopsis] DRAFT NIST SP 800-146, Cloud Computing Synopsis and Recommendations. [online] Available: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf
- Draft SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing. [online] Available: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
- [NIST CC Roadmap] DRAFT NIST SP 800-293, US Government Cloud Computing Technology Roadmap, Volume I, Release 1.0. [online] http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf
- NIST SP500-291 NIST Cloud Computing Standards Roadmap. [online] Available: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Jul5A.pdf

NIST Cloud definition – Draft SP 800-145 (1)

- NIST Definition of Cloud – missing network provisioning, just “limited control over network”

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., ***networks***, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

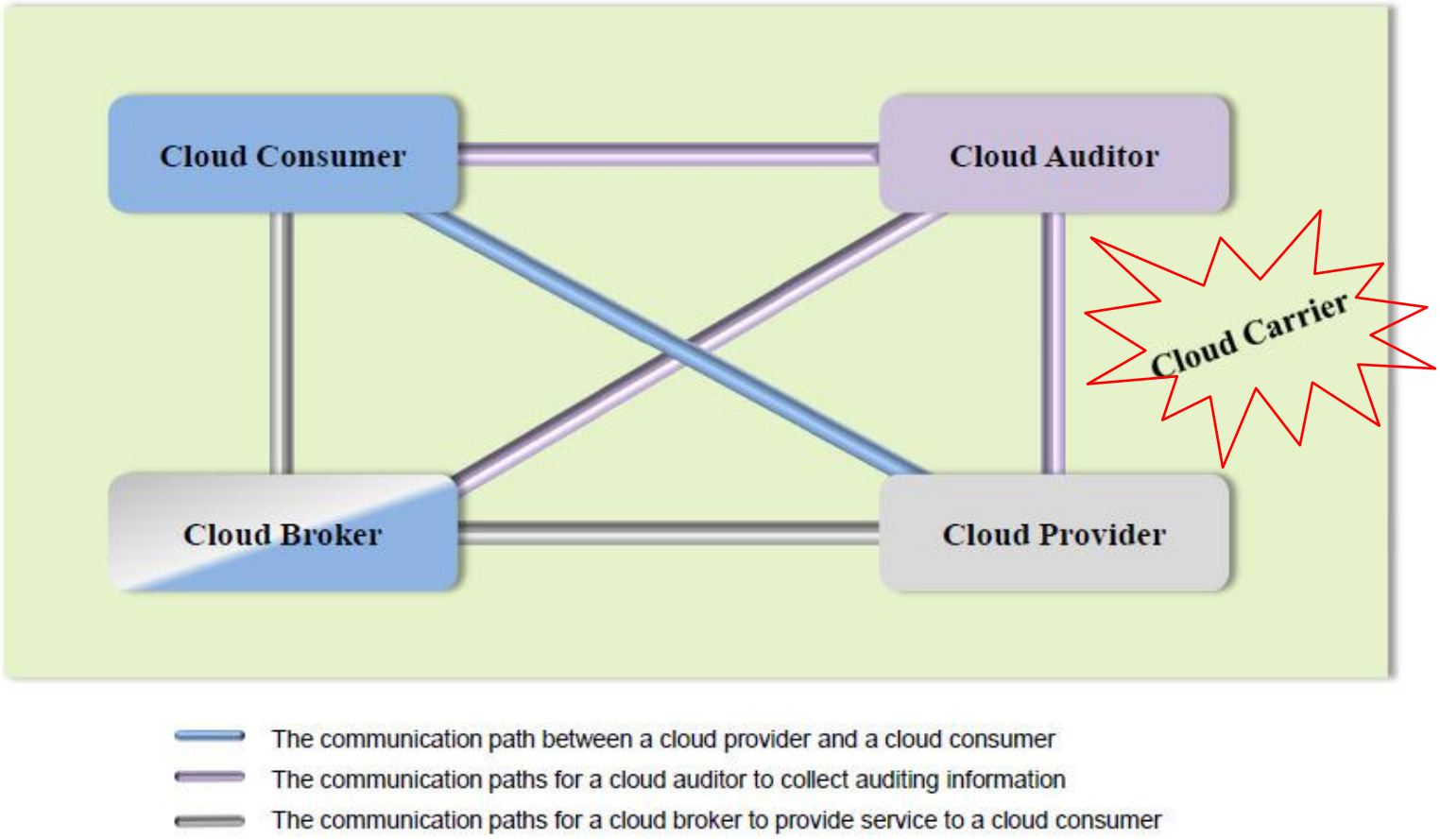
Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, ***networks***, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer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

NIST Cloud definition – Draft SP 800-145 (2)

Draft SP 800-145 A NIST Definition of Cloud Computing (published)
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

- Five essential clouds characteristics
  - On-demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured Service
- 3 service/provisioning models
  - Software as a Service (SaaS)
  - *Platform as a Service (PaaS)*
  - Infrastructure as a Service (IaaS)
- 4 deployment models
  - Public cloud
  - Private cloud
  - Community cloud
  - Hybrid cloud

NIST Cloud Computing Reference Architecture (CCRA) 2.0 - Main Roles (1)



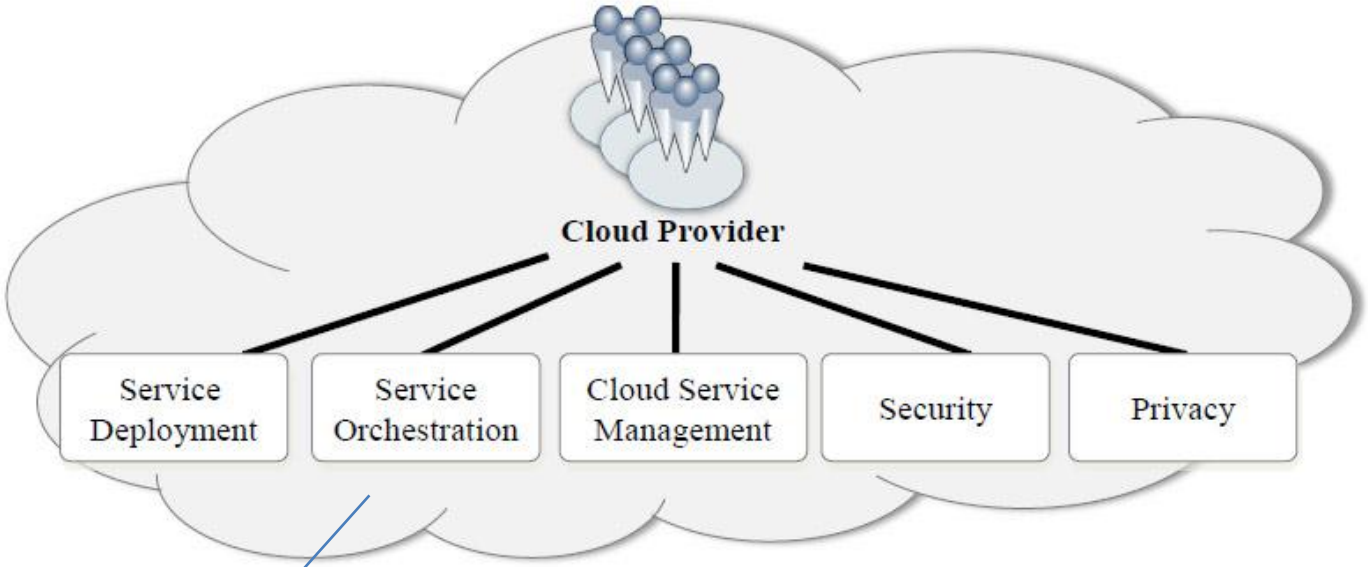
- Cloud Carrier as a role to accommodate telco's interests

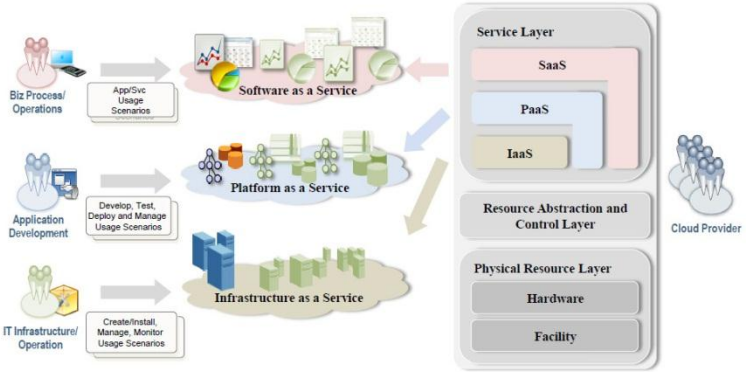
NIST Cloud Computing Reference Architecture (CCRA) 2.0 - Provider Functions (2)

Add:

Service Delivery (Framework)

- Request&SLA
- Reservation/ Composition
- Deployment
- Operation
- Decommissioning

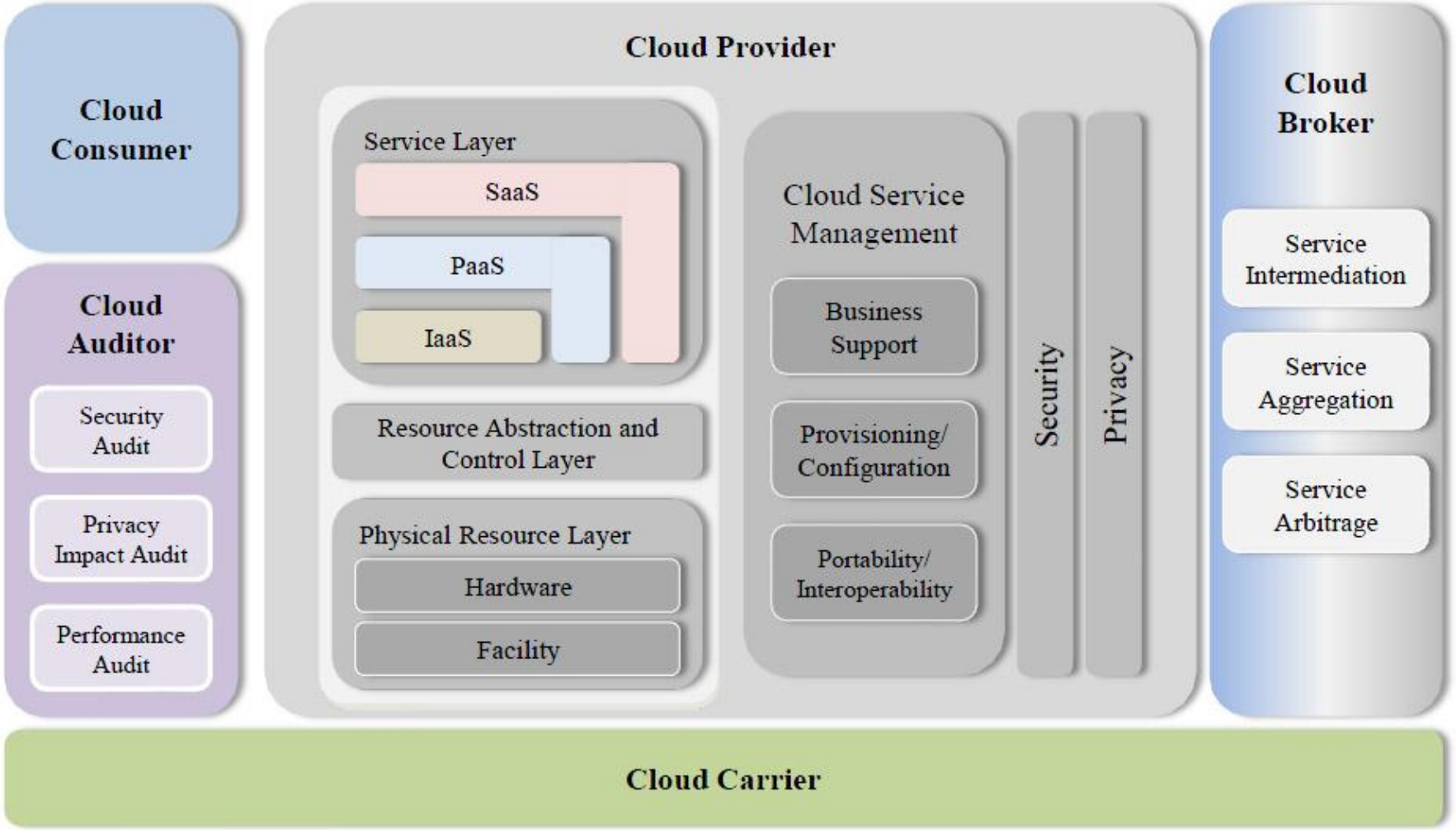




Provider functions

- Defined ambiguously
- Need clear separation between Delivery process, Operation and Control&Mngnt functions
- Service Orchestration is a Control function

NIST Cloud Computing Reference Architecture (CCRA) 2.0 – Consolidated View (3)



Dedicated Network Provisioning in Clouds

- This issue is not addressed in details in any of currently proposed CC architectures
- It can not be consistent infrastructure QoS without (dedicated) network provisioning
  - Specifically for Optical networks
- Telco, network providers and telecom equipment vendors are working in this direction
  - GEYSERS project is an example of network+IT infrastructure virtualisation
-

Extending NIST Cloud IaaS definition to support NaaS
(in the context of Network Infrastructure provisioning)

The suggested extensions to the Cloud IaaS model to meet requirements of the critical enterprise services:

- Define layered cloud services model that should be suitable for defining main inter-layer and inter-service (functional) interfaces
- Add topology aware infrastructure view
- Define resources and services virtualisation as one of generic cloud features (TBD)
- Include improved network services definition capable of provisioning required QoS and allowing control from user run applications
- At the business/operational level, the CCRA should be extended to address the following features:
  - Improved definition of the Cloud Carrier role, operational model and interaction with other key actors
  - Extended set of basic roles to reflect typical for telecom operators/providers business relations:
    - Cloud/infrastructure Operator, Customer, and User (in place of the currently used consumer role)
- Other cloud service models PaaS and SaaS should also allow management of QoS and other network related parameters