Cloud Networking: An Infrastructure Service Architecture for the Wide Area

Paul Murray, Azimeh Sefidcon, Rebecca Steinert, Volker Fusenig, Jorge Carapinha

HP Laboratories
HPL-2012-111R1

Keyword(s):

cloud computing; cloud networking; network virtualisation; infrastructure as a service; virtual infrastructure management; virtual infrastructure security

Abstract:

We present an architecture for cloud networking, the provision of virtual infrastructure in a multi-administrative domain scenario, where data centre and network operators interact through defined interfaces to provide seamless virtual infrastructure. To support this scenario we introduce the flash network slice, dynamic elastic network connections that compose to form integrated cross-domain networks. Flash network slices support decomposition of virtual infrastructure into partitions that can be managed independently but seamlessly interconnected across administrative boundaries. The approach supports limited information disclosure about implementation details on behalf of the providers, scalability, heterogeneity, and a migration path from currently deployed infrastructure technologies to future network implementations. The resulting infrastructure services are suited to on-demand deployment of emerging cloud services such as content distribution, social networks and cloud-based IT applications.

External Posting Date: July 21, 2012 [Fulltext] Approved for External Publication
Internal Posting Date: July 21, 2012 [Fulltext]
Published in Future Network & Mobile Summit 2012: 21st Annual Conference Proceedings

Future Network and MobileSummit 2012 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2012
ISBN: 978-1-905824-30-4

Cloud Networking: An Infrastructure Service Architecture for the Wide Area

Paul Murray[1], Azimeh Sefidcon[2], Rebecca Steinert[3]
Volker Fusenig[4], Jorge Carapinha[5]
[1]*HP Labs, Bristol, UK, Email: pmurray@hp.com*
[2]*Ericsson AB, Kista, Sweden, Email: azimeh.sefidcon@ericsson.com*
[3]*SICS, Kista, Sweden, Email: rebste@sics.se*
[4]*Fraunhofer AISEC, Garching, Germany, Email: volker.fusenig@aisec.fraunhofer.de*
[5]*PT Inovação, Aveiro, Portugal Email: jorgec@ptinovacao.pt*

Abstract:
We present an architecture for cloud networking, the provision of virtual infrastructure in a multi-administrative domain scenario, where data centre and network operators interact through defined interfaces to provide seamless virtual infrastructure. To support this scenario we introduce the flash network slice, dynamic elastic network connections that compose to form integrated cross-domain networks. Flash network slices support decomposition of virtual infrastructure into partitions that can be managed independently but seamlessly interconnected across administrative boundaries. The approach supports limited information disclosure about implementation details on behalf of the providers, scalability, heterogeneity, and a migration path from currently deployed infrastructure technologies to future network implementations. The resulting infrastructure services are suited to on-demand deployment of emerging cloud services such as content distribution, social networks and cloud-based IT applications.

Keywords: cloud computing, cloud networking, network virtualisation, infrastructure as a service, virtual infrastructure management, virtual infrastructure security

1. Introduction

Current cloud computing infrastructure services provide on-demand compute and storage facilities for dynamic end-user services. These are typically hosted in large, centralised data centres, operated by a single provider, with only rudimentary support for virtual networking beyond the data centre.

Network operators will introduce processing and storage resources throughout their networks, potentially at every router and edge device, and dynamic virtual networks, providing an ideal environment to deploy network based services such as content distribution, video conferencing and on-line gaming. As a result, we envisage an evolution to cross-provider infrastructure delivery for global scale cloud services.

In the following, we describe an architecture developed in SAIL [1] (detailed in [2]) that supports seamless virtual infrastructures deployed on-demand across multiple providers, including data centre and network operators. It addresses issues related to inter-provider service provision, such as management delegation and cross-domain connection set up in the presence of limited information disclosure between parties.

1.1 The Cloud Networking Concepts

The term *cloud networking* is introduced in a multi-administrative domain scenario, where network and data centre domains exist and must interact through defined interfaces to provide a service to cloud customers. A cloud networking service is adaptive,

scalable, reliable and autonomous, and operates seamlessly to the user. These properties require a cloud networking architecture that allows for: efficient means of specifying a service through high-level objectives or goals; rapid deployment and management of cloud services across data centres and operator networks; and, autonomous optimisation and management of underlying resources to provide and maintain requested QoS.

The cloud networking architecture builds upon two main concepts: integration of virtual networks across data centre and network operator infrastructures; and deployment of compute and storage resources across network operator equipment. These federated infrastructures are exploited through a composable model of virtual networks called a *flash network slice* (FNS). A FNS models a network as a single entity that forwards messages between resources connected to it. Multiple FNS can be linked across administrative boundaries to form a federated network that can also be modelled as a single abstract FNS. Communication properties can be defined between resources linked to an FNS and used to determine their placement in underlying infrastructure.

1.2 Challenges and Design Goals

The cloud networking architecture provides functionality for efficient management of computational, storage and network resources, and is designed to address the following challenges: *Multi-domain operation:* Cross-provider provision raises inter-domain networking problems due to limited information disclosure between providers. *Heterogeneity:* The architecture should facilitate management of legacy networks and utilise legacy management capabilities where needed, while allowing for deployment and migration to future network technologies. *Scalability:* The number of peer providers and the total number of users should not affect the performance of any particular provider. *Dynamic provisioning and reconfiguration:* Provision should be fully automatic, based on high level goals, and at time scales comparable to existing cloud infrastructures. *Robustness and security:* The infrastructure service must be resilient to failures and degradations and provide means for controlling security properties for virtual resources. Providers must be able to apply their own filtering policies to service requests.

The cloud networking architecture is described in Section 2 with management and security covered in Section 3 and 4 respectively. Section 5 describes use cases for the architecture. Related work is described in Section 6 and we conclude in Section 7.

2. Cloud Network Architecture

We assume an environment with multiple infrastructure service providers including network operators. The providers may chose to collaborate to some extent in order to implement virtual infrastructures that span their domains. They implement virtual resources and can connect their resources at their boundaries to give the impression of a single virtual infrastructure. The user is presented with a single service control interface and propagation of the user's infrastructure and its control is managed collaboratively by the providers. This arrangement is depicted in Figure 1.

2.1 Roles and Interfaces

We define three main classes of interface and three primary roles shown in Figure 1. The interfaces are *infrastructure service*, *resource administration*, and the *distributed control plane* (DCP). The roles are *infrastructure service user*, *infrastructure service provider*, and *resource administrator*.

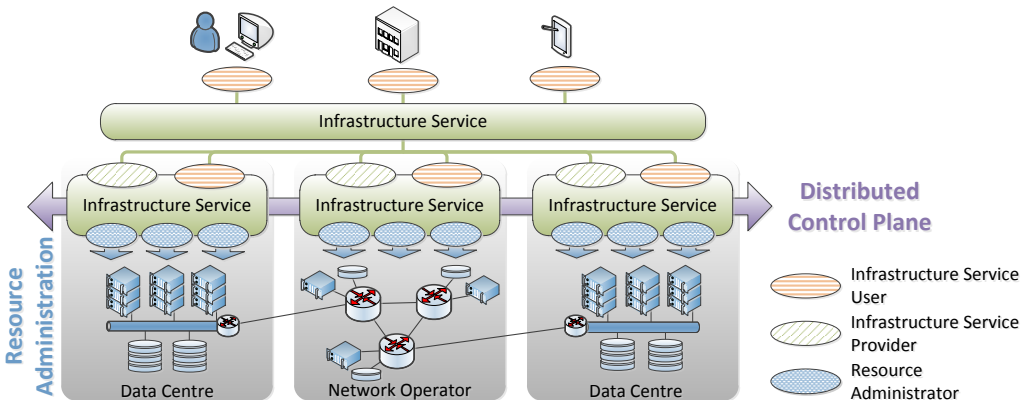


Figure 1: High level view of cloud networking architecture

The infrastructure service user and provider interact with each other through the infrastructure service interface. The resource administrator has authority over underlying virtual or physical equipment (the administrative domain) and uses the resource administration interfaces to create virtual infrastructure. A single actor may adopt all these roles to receive service requests, implement infrastructure resources and issue requests to another provider. The DCP is a collection of protocols and interfaces used to implement coordinating actions across administrative domains.

2.2 Delegation and Cross-Coordination

A user's request for infrastructure through the infrastructure service interface is an act of *delegation*: the user specifies the infrastructure and transfers responsibility for determining how to implement it to the provider. One option available to a service provider is to delegate part or all of the requested infrastructure to other providers. In doing so it does not admonish itself of responsibility to the original user, instead it builds a management hierarchy with delegation of control going down, and reporting going up.

The delegation process leads eventually to virtual infrastructure that is implemented across one or multiple domains. Some aspects of management control require coordination across domains, such as creating cross domain links, or monitoring information for distributed decision making. For this reason peer domains may interact through the DCP to perform distributed control.

In general, the pay-per-use model similar to what is used in Cloud Computing is assumed. The architecture does not yet include specific billing and accounting mechanisms adapted to cloud network concepts, but is designed to allow for solutions in cross-domain billing and accounting. Development of such mechanisms will therefore be targeted in future refinement of the architecture.

2.3 Information Model

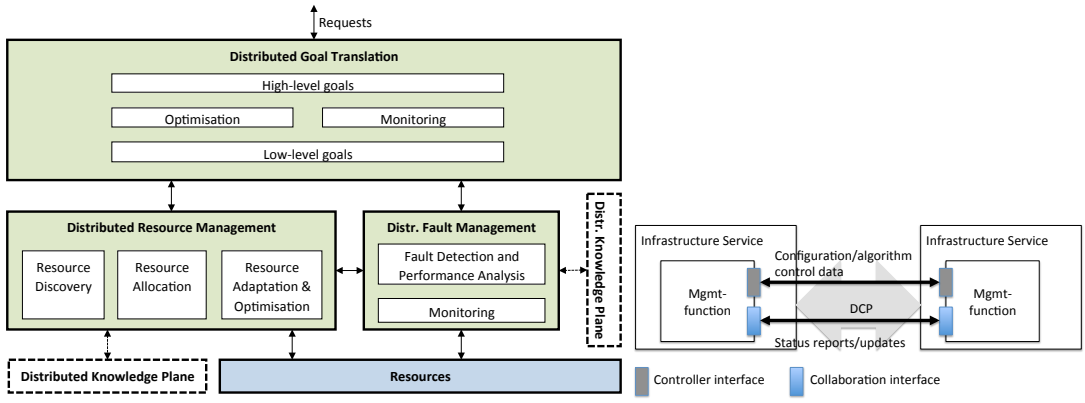
The interfaces use a declarative information model to describe compute, storage, and network resources, that is fundamental to interoperability and is required to support *heterogeneity*, *limited information disclosure*, *delegation*, and *scalability*. The model includes *external references*; references to information held outside the model.

A decomposition process can exploit FNS by transforming a model using a single network into one with multiple FNS linked using external references, thus creating partitions that can be delegated to other providers in isolation. Linking Multiple FNSs across domains creates a network capabiliity that spans providers.

Decomposition (along with abstraction) and the external references support information hiding. A model can be specified in an abstract form, be decomposed, and then the partitions can be specialised independently. Where a model contains an external reference an external mechanism is used to access the related information. So the original abstraction, the decomposition, and the specialised parts can be managed by different authorities without exposing their local transformations.

3. Management Functionality

The cloud network management consists of three high-level management functions (MF): *goal translation* (GT), transforming business, technical and security goals into resource configuration objectives; *fault management* (FM), providing status updates of monitored resources, measurements and models, as well as detecting faults, anomalies, and changes in performance; and *resource management* (RM), responsible for provisioning, allocation, reconfiguration, optimisation of resources and performance (Figure 2(a)). The MFs operate within infrastructure service providers and contribute in managing the administrative domain. Through the DCP and MF interfaces, the management functions exchange information for decentralised, adaptive and efficient management in both single-domains and cross-domains (Figure 2(b)). MFs can be instantiated in any virtual instance or level of an infrastructure service provider, addressing management in both single- and cross-domain cases.



(a) Management functions and blocks. (b) Interfaces and information exchanges.

Figure 2: Conceptual overview of the management architecture.

The Distributed Knowledge Plane (DKP) represents distributed information retrieval and information maintenance of distributed resources, and allows for information transparency over the heterogeneous equipment on which the management functions operate (Figure 2(a)). The DKP enables abstraction over potential heterogeneities caused by technical (e.g. varying network virtualisation technologies), administrative (e.g. operator limits knowledge it is willing to share with other domains), or legal limitations (e.g. country-specific encryption limitations). The DKP can relate to databases or functions for retrieving information about resources (e.g., for RM), or relate to the

common form in which heterogeneous information should be presented (e.g. for FM collecting information from similar systems or legacy networks).

4. Security Functionality

The flexible and distributed nature of cloud networking demands new security solutions. On one side a common identity management framework is needed to uniquely identify infrastructure service users, infrastructure service providers, infrastructures, and virtual resources. Based on this identity management framework authentication and fine granular access control can be defined. On the other hand, as virtual resources can be placed and moved anywhere in the cloud networking infrastructure, mechanisms are needed that allow an infrastructure service user to define security properties that need to be fulfilled for its virtual resources.

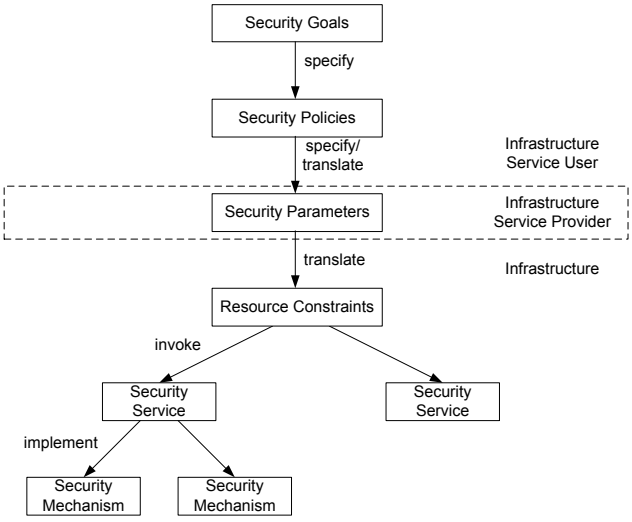


Figure 3: Security goal translation

The security functionality is integrated in the management components (see Figure 2(a)) and can be used to define and enforce infrastructure service user's security policies (see Figure 3). While requesting virtual resources an infrastructure service user defines a security policy that needs to be fulfilled for these resources. By performing a resource discovery which is part of the distributed resource management component the infrastructure service provider has an overview of available infrastructure and its security mechanisms. When receiving a request an infrastructure service provider checks the available infrastructure and selects one that has the demanded security functionality. Afterwards, the distributed goal translation component of the infrastructure service provider translates the security policy of the infrastructure service user to resource constraints. The resource allocation of the service provider's distributed resource management component includes these resource constraints in the request for virtual resources.

When an infrastructure service provider plans to move a virtual resource to another infrastructure it again needs to check if the target infrastructure offers the demanded security mechanisms. The resource constraints are invoked on the target infrastructure when moving the virtual resource.

5. Use Cases

The FNS concept can be materialised in multiple scenarios and use cases. In the framework of the SAIL project, two broad scenarios have been considered: dynamic enterprise and elastic video distribution. In this section, the first scenario is used to illustrate the typical service provisioning workflow.

The dynamic enterprise scenario targets the enterprise sector such as media production and refers to the provisioning of IT solutions based on the cloud network ecosystem. In media production use case: a TV channel playing the user role uses cloud networking to extend production facilities and IT services to a sub-contractor (video animation company), based in a remote geographical location. The computing resources should be physically located near the sub-contractor premises to fulfil SLAs at minimum cost and optimise resource efficiency. The cloud networking architecture supports this use case by providing the means to dynamically establish secure networking connectivity between the remote cloud site, the animation company and the channel production systems. The TV channel would be a customer of a local cloud service provider that delegates the provision of the service to a remote cloud service provider for reasons quality of service to the sub-contractor. Whenever high volumes of data have to be transferred between the two sites a FNS can be dynamically instantiated by means of an appropriate network service, e.g. a L2/L3 VPN service. The dynamic properties of cloud networking allow the allocation of network resources only when needed, to permit the cost efficient and secure transfer of high volumes of data. Using currently available solutions, this scenario would be either prohibitively expensive or outright impossible.

The service provisioning workflow in this use case is composed of three main phases:

Service Request: Through the infrastructure service interface, the customer is able to request virtual infrastructure resources, and later modify already deployed resources, or obtain the current status of those resources.

Request translation, decomposition and delegation: The service provider analyses the submitted request and maps it down to the resource level. If required the request is broken down to multiple infrastructure providers. Part of the resources to be instantiated are explicitly indicated in a user request (e.g. CPU, memory, storage), whereas some resources (typically, network resources) may be indirectly derived from service requirements (e.g. guaranteed performance, maximum delay/jitter).

Service enforcement on the infrastructure: At this stage the virtual resources are actually enforced in the infrastructure by several infrastructure providers involved in the process, including computing, storage or networking resources, the latter being typically in the form of a provider-provisioned VPN service, potentially encompassing several network infrastructure domains. Once the bulk of data transfer is completed, the capacity allocated to network service may be reduced, or simply released.

6. Related Work

Challenges of cloud networking spans over architecture, methodology and interfaces, management, QoS handling, and security. These aspects have been the focus of research for number of projects. GEYSERS [3] defines an architecture, NSI [4] focuses on methodology, CloudAudit [5] deals with interface challenges, RESERVOIR [6] focuses on Management aspects, ETICS [7] deals with QoS aspects and CCM [8] and OrBAC [9] dig into security aspects.

GEYSERS defines an architecture for managing virtual infrastructure by integrating network and IT resources based on GMPLS and PCE. It extends the virtual infrastructure concept to optical layer to share the physical infrastructure among different operators and granting them isolation.

CloudAudit focuses on creating a common interface for automating the audit, assertion, assessment and assurance of IaaS, PaaS and SaaS.

RESERVOIR aim at building a cloud federation for data centres connected via best effort IP network by defining a layered architecture including service, virtual execution environment and resources. This work is not addressing different aspects of quality of experience that can be achieved by tighter interaction between the data centre and the network operator or between network operators themselves.

ETICS focus on QoS by creating the interconnection of multiple network service providers. It defines a seven layer SLA life cycle for "creation", "certificate publications", "negotiation", "validation", "provisioning", "monitoring" and "termination".

Our cloud networking in SAIL [1] follows the experience of 4WARD [10] which developed a layered architecture for network virtualisation. The concept of in-network management introduced in 4WARD is to a large extent the foundation of our management processes as we also follow the principles of decentralised operation, addressing the challenges of scalability, adaptability, control, reliability and resource usage efficiency.

In comparison, GEYSERS model also addresses the cloud networking challenges but differs in focus and the layer of the protocol stack where the solution is proposed. On the other hand CloudAudit is proposing removal of the repetitive and costly operation which the cloud networking security framework can benefit from. Unlike RESERVOIR, quality of experience has been addressed in CloNe. This can be achieved by tighter interaction between data centres and the network operator or between network operators themselves. The principles of CCM are aligned with industry-accepted security standards such as ISO and can serve as the base for evaluating the security levels of the cloud networking architecture.

There is a natural tendency to compare Cloud and Grid and some publications such as [11] focus on different aspects of this comparison. According to [11] the business model differs between Cloud and Grid. The Cloud-based model is pay-per-use while the model for Grid is project-oriented. Grid architecture was built to address large-scale computation using resource sharing while the Cloud goal is to create the perception on unlimited resources based on virtualisation techniques. They also differ in resource management as Grid relies on scheduling of resources while Cloud is based on virtualisation for sharing resources. The models differ further on the details of data model, monitoring and security techniques among others. As cloud networking follows the fundamental concepts of cloud computing, the same differences are equally apparent.

7. Concluding Remarks

Our cloud networking architecture provides a framework for collaboration across cloud infrastructure providers that addresses multi-domain operation, heterogeneity, scalability, autonomous management, and security. For the user it provides the ability to create infrastructure on-demand, in centralised or distributed configurations as dictated by high level service objectives. The architecture describes management and security aspects that address the delegation of infrastructure provision.

The FNS is introduced as a network resource type that can be linked across administrative boundaries, providing the ability to partition virtual infrastructures into isolated administrative domains, and can be realised on multiple network technologies, allowing a migration path to future Internet implementations.

The cloud networking architecture is the basis of on-going prototyping in the SAIL project. The implementation uses concrete interfaces and models that show the practical applicability in multiple scenarios and demonstrate interoperability with widespread network technologies (e.g. MPLS VPNs). This work will provide proof points for future cloud service deployment and will form the basis for standardisation for inter-provider virtual infrastructure operation.

References

[1] "SAIL." http://www.sail-project.eu/, December 2011.

[2] P. Murray et al., "D-D.1 Cloud Network Architecture Description." http://www.sail-project.eu/deliverables, July 2011.

[3] "GEYSERS: Generalised Architecture for Dynamic Infrastructure Services." http://www.geysers.eu/index.php/theproject/goals, December 2011.

[4] "Inter-Domain Controller (IDC) Protocol Specification, Open Grid Forum Network Service Interface (NSI) Working Group." http://www.controlplane.net/idcp-v1.1-ogf/draft-gwdi-nsi-idcp-2010-sep-01.pdf, September 2010.

[5] "CloudAudit." http://cloudaudit.org/, June 2011.

[6] B. Rochwerger, D. Breitgand, A. Epstein, D. Hadas, I. Loy, K. Nagin, J. Tordsson, C. Ragusa, M. Villari, S. Clayman, E. Levy, A. Maraschini, P. Massonet, H. Munoz, and G. Toffetti, "Reservoir - when one cloud is not enough," *Computer*, vol. 44, pp. 44–51, 2011.

[7] "ETICS: Economics and Technologies for Inter-Carrier Services." https://www.ict-etics.eu/overview.html, December 2011.

[8] C. C. L. Team, "Cloud security alliance cloud controls matrix v1.1," tech. rep., Cloud Security Alliance, 2010.

[9] A. Kalam, R. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miege, C. Saurel, and G. Trouessin, "Organization Based Access Control," in *4th IEEE International Workshop on Policies for Distributed Systems and Networks (Policy'03)*, June 2003.

[10] "4WARD." http://www.4ward-project.eu/index.php, December 2011.

[11] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop, 2008. GCE '08*, pp. 1 –10, nov. 2008.