Cloud Computing in Carrier Grade Networks

Ioan DRĂGAN, Răzvan ZOTA
The Bucharest University of Economic Studies
dragan_ioan1989@yahoo.com, zota@ase.ro

This paper is presenting a method of applying Infrastructure as a Code concept in the case of the carrier grade networks in order to orchestrate and automate the deployment of Network as a Service. Even though shared network services have been on the market for a while, a complete automated deployment of virtualized network services and equipment has not been developed yet, so, in our opinion, the new methods of delivering services would permit traditional Ethernet carriers to deliver new service packages to their customers. These new service packages would include connectivity services, Internet connection, virtual router capabilities, network storage and a diversity of cloud computing services.

Keywords: *Cloud Services, Ethernet Networks, Virtualization, Carrier Ethernet*

1 Introduction

In the beginning we will describe shortly the evolution of carrier grade network and network equipment virtualization. Since the first release of legacy Ethernet in 1970s, it has proven itself to be a technology that can adapt to evolving technology needs. Initially, it was developed as a LAN standard connecting devices at 10Mbps and then evolved to 100Mps (Fast Ethernet) and finally into Metro Area Networks (MAN) of 10Gbps and 100Gbps.

Carrier Grade Ethernet is a standardized service offer, delivered not only by traditional Ethernet based networks, but also on other underlying mechanisms: MPLS based L2 networks, IEEE802.1ad Provider Bridges, Ethernet over SDH/SONET [1].

Carrier Grade Ethernet is defined by five attributes [2]:

- Standardized Services
- Scalability
- Reliability
- Service Management
- Quality of Service

Since Ethernet evolved from a technology to a service, the network equipments that carriers used evolved accordingly. Scalability and Service Management drove the initial old Ethernet hubs and switches to very complex equipments that support various technologies and most important, multi-tenancy.

Carriers have started offering this kind of transport and/or Ethernet services, so various standards and technologies have been used as an enabler for traffic separation and multi-tenancy: IP-MPLS, 802.1ah, 802.1ad, Ethernet over SDH/SONET [3].

Even though all this technologies offer various services, none of them is capable of offering a “network as a service” option, where the end customer can configure its own virtual network equipments. Similar to other cloud solutions, networks and network equipments should be able to be virtualized and offered as a service.

Cloud computing has been documented since the 1950 when large scale mainframe computers were seen as the future of computing. Terminals (clients) were able to perform basic operations with very limited processing resources and connect to the mainframes. The resource sharing was basically done on a time-sharing algorithm rather than a parallel processing [6].

Even though the concept of virtual resource is used nowadays mainly in describing computing and storage sharing, the concept was firstly deployed on a wide scale by telecommunications companies in the means of virtual private networks (VPN) [7].

Nowadays, cloud computing is mostly identified by three concepts:

- Infrastructure as a Service (IaaS) - Is the most basic cloud-service model and according to the IETF (Internet Engineering Task Force). Providers of IaaS offer computers – physical or more often virtual machines including other resources like storage or internet connections.

- Platform as a Service (PaaS) - cloud providers deliver a computing platform, typically including operating system, a programming language execution environment, a database and/or a web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying, managing the underlying hardware and software layers and passing the complex process of security compliance and certification.
- Software as a Service (SaaS) - is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. In this model the cloud service provider is responsible top to bottom: application, operating system, infrastructure, hardware, Internet connection etc.

2 Infrastructure as a Code Concepts

The concept of Infrastructure as Code was born in the same time with the appearance of tools like *CFengine*, *Puppet*, and *Chef*. Such software tools could enable developers and system administrators to abstract their problems around maintaining modular and automate infrastructure, by using a high-level language. In the following stages, the development of such tools and techniques has begun to resemble the way software developers build and maintain application source code. "All of the testability, repeatability, and transparency of a modern software development process suddenly became available for people who were building infrastructure. The lofty goal for many of these cutting edge organizations was to be able to completely rebuild a business' software systems with nothing more than physical server resources, a complete backup of their databases, and source code. Today, that's how many modern successful tech businesses operate. They have the ability to do exactly that."[4]

Infrastructure as a Code provides at a high level:

- A configuration management system
- A system integration platform
- An API for all your infrastructure

This new concept allows system administrators to configure and maintain their infrastructure in a source code/implementation mode. By having all instances configured based on a standard "recipe", upgrade and configuration of the whole infrastructure becomes a simple "one node deploy".

In order to illustrate the principles of Infrastructure as a Code, we're going to sketch the basic implementation of "Chef" tool.

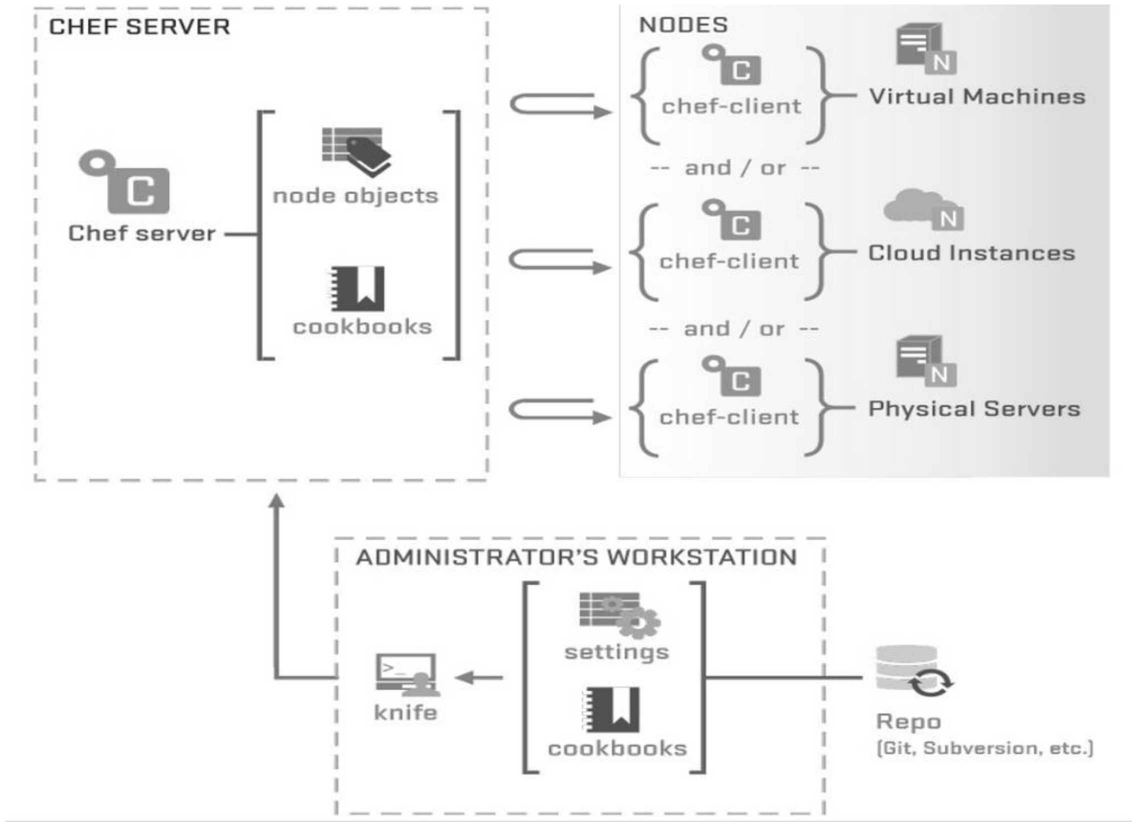

Fig. 1. Chef Infrastructure [5]

Main components of Chef are [5]:

- *Chef server* –The Chef server acts as a hub of information. Cookbooks and policy settings are uploaded to the Chef server by users from workstations. The chef-client accesses the Chef server from the node on which it's installed to get configuration data, perform searches of historical chef-client run data, and then pulls down the necessary configuration data. After the chef-client run is finished, the chef-client uploads updated chef-client run data to the node object and generates reporting data about that chef-client run.
- *Chef client* – A chef-client is installed on every node that is under management by Chef. The chef-client performs all of the configuration tasks that are specified by the run-list and will pull down any required configuration data from the Chef server as it is needed during the chef-client run.
- *Cookbook* – the Cookbook is the fundamental unit of configuration. It contains recipes, templates, files, custom resources and others needed to fully configure a node.
- *Node* –A node is any physical, virtual, or cloud machine that is configured to be maintained by a chef-client.

3 Applying IaaC on Network Nodes

Even though IaaC was mainly designed for Operating Systems and applications, it can be applied to other various devices. Virtualization and deployment of standard configurations have been available for routers for a while already, mainly testing configurations and implementations in laboratories.

SmartEdgeOS was the first to offer virtualization of instances and binding to hardware interfaces, but this is possible only on one router, not being deployable on an infrastructure scale, in order to bind interfaces from different equipments.

As to apply the IaaC mechanism on an infrastructure scale we have to implement the following points:

- Virtualization of network equipment software (for simplicity we'll choose router operation systems);
- A cluster of hardware, not necessarily network equipments capable of running high number of virtualized instances of software from above point;
- A network management system (NMS) capable of adapting the configuration of "on premise" network equipments to switch/route traffic to the hardware cluster for cloud processing;
- Chef architecture can apply on the above model:
    - Chef server – network management system and cloud management system
    - Chef clients – hardware cluster and all network equipments
    - Cookbook – configurations that can be virtualized by the Chef server

Creating virtual instances of network elements would allow various implementations to be deployed in a matter of minutes, based on a predefined "code based" configuration. It allows enterprises and/or customers to rent an infrastructure from carriers instead of renting carrier services and deploying their own equipments to implement the desired configurations.

Figure 2 shows the actual carrier infrastructure and how the customer endpoints are linked together from hardware point of view. This is the classic implementation of an *E-Tree*, the carrier providing only connectivity between the different customer endpoints and eventually traffic separation.

Figure 3 shows a proof of concept implementation that comes as an extra layer of complexity on the hardware infrastructure. Apart from connectivity and traffic separation, the carrier offers virtual routers as a service.

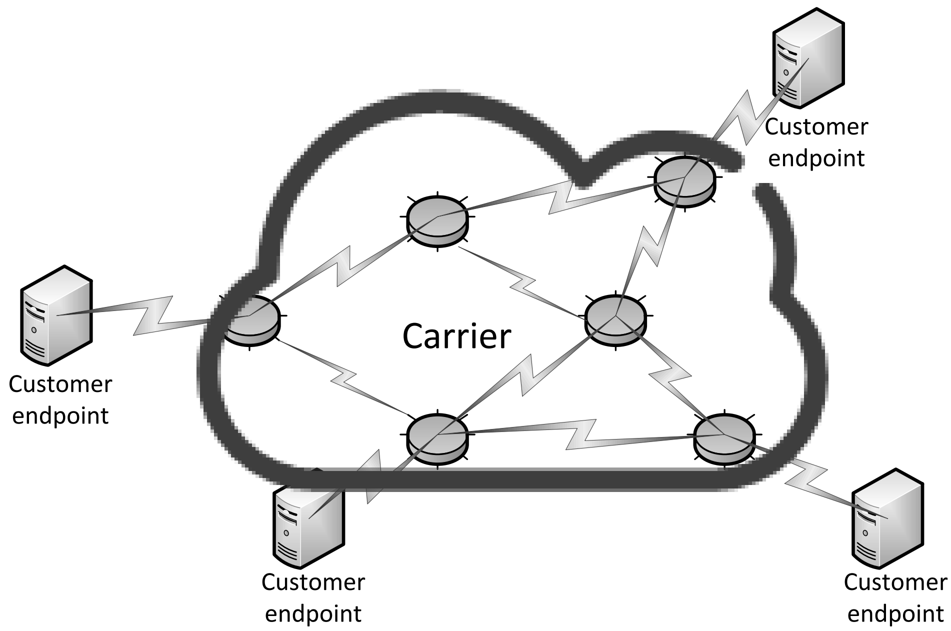

Fig. 2. Carrier Infrastructure

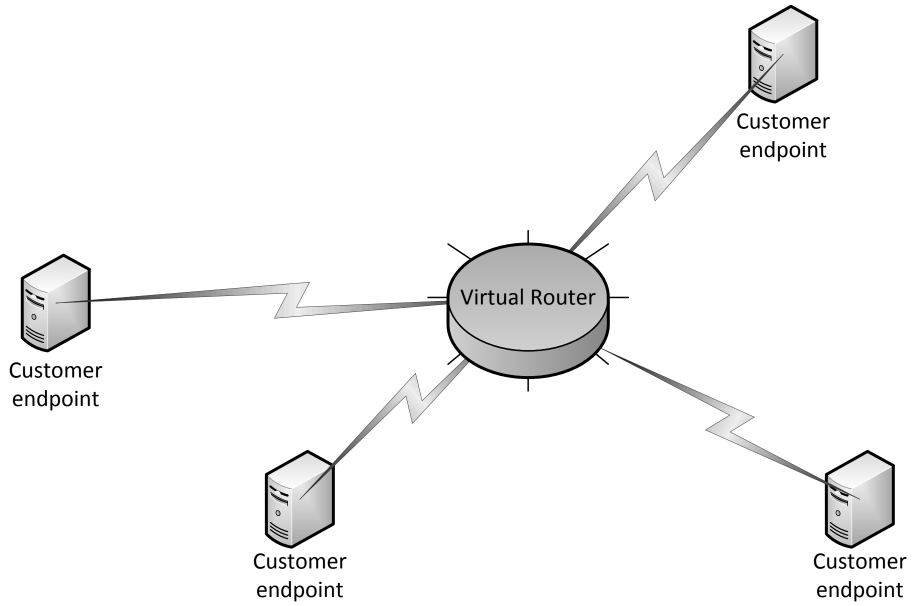

Fig. 3. Virtualized environment

Mainly routers were used as standalone equipment due to their modular design and scalability capabilities. Having an extra virtual layer would separate the concern of having capacity expansion and monitoring on numerous network nodes and rather expanding capacity on virtual instances.

A first step towards this complete virtualization has been described as being Software Defined Networks (SDN). In a software-defined network, switches and routers take some form of direction in a centralized software management element. A centralized controller, which maintains a real-time, overall holistic view of the network, defines network paths as "flows" and distributes this flow data to individual switches and routers. With these flows, rather than using IP and MAC addresses, the controller coordinates the forwarding of data across all network devices, enabling the automation and granularly managed dynamic provisioning necessary in virtualized environments and cloud networks. This approach contrasts with today's networks, which have a distributed and uncoordinated control plane, or at least not at a network level. The switches and routers each maintain routing or MAC address tables with data about the network elements around them, and they make forwarding decisions based on that data. This approach has worked well, up to a point. But IT infrastructure is much more dynamic than it used to be, thanks to virtualization, and the network needs to adapt [8].

Virtualization has made IT infrastructure more and more dynamic, so networks need to be responsive to changes. It must be able to automatically adjust VLANs, QoS policy and ACLs when a server administrator moves a virtual machine from one server to another or when additional resources are needed in a certain area of the network.

Traffic engineering would be at a virtual level, much easier to monitor and redirect. Carrier’s concerns would be transporting aggregated traffic between their data centers without having to separate it at layer 2 or layer 3 OSI. This traffic is tagged and separated now at application level.

One proposed solution is to centralize a connection policy using SDN. In SDNs, the endpoints have no implicit right to connect, so nothing on the network is connected at first. Instead, a software control function decides what connections to permit, and which route traffic will take for those connections [9].

4 Main Benefits of Using a Cloud Infrastructure and Software

A cloud approach would also cover the five key attributes of “Carrier grade Ethernet” and extend them to the new "carrier grade" services.

- *Standardized Services* – a service catalogue can be issued and Cookbooks can be created based on this
- *Scalability* – since it's a cloud approach, the number of network equipments and hardware clusters can be scaled to the needed size. The only limitation would be the transport capacity of the links in the actual network.
- *Reliability* – by having all the configurations on Cookbooks, if a major failure occurs (which cannot be fixed by existing routing and protection mechanisms), the configuration can be deployed on another "chef client" in a matter of minutes, without losing any configuration
- *Service Management* – since we have a cloud infrastructure, each service can be activated, deactivated and modified automatically. Service upgrades are also available via existing/new Cookbooks.
- *Quality of Service* – policies can be applied on customer edge network equipments to limit bandwidth and on virtualized instances to limit processing capacity. Also, several QoS policies can be applied on the network infrastructure to prioritize different kind of traffic.

The infrastructure orchestration and automation would provide a simple and easy to use configuration portal to cover the customer business needs without having in depth knowledge of networking and routing protocols.

Automating business processes has been a trend in IT industry in order to reduce costs and improve quality. Even though the interaction between a sales team and the customer can be productive, in some cases this might lead to misunderstandings and wrong service orders which increases rework and customer frustration. By offering a standardized service catalog, the customer can choose and configure his own services from a standard offering. If the outcome is not as expected, an immediate rollback/restore can be performed, thus reducing lead times in implementations and also service restorations.

The current configuration process is the one depicted in Figure 4.

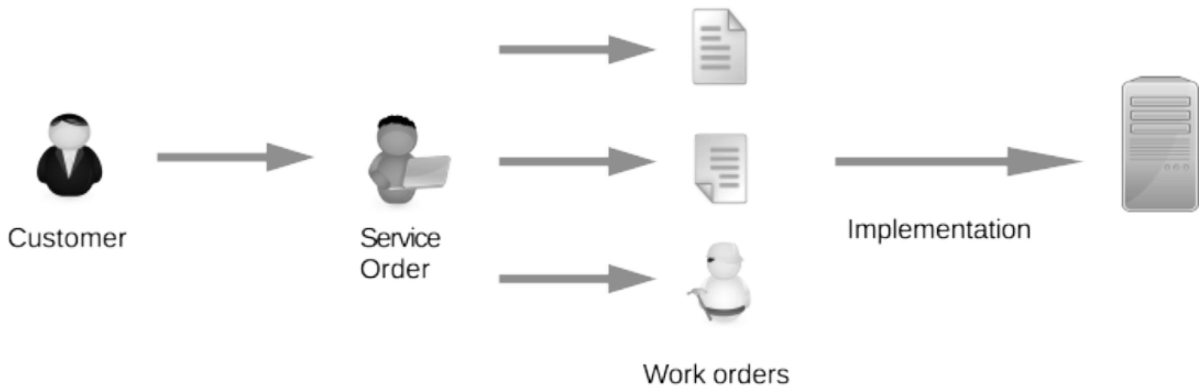

Fig. 4. Resource order and configuration

The desired position in the configuration process is represented in Figure 5 below.

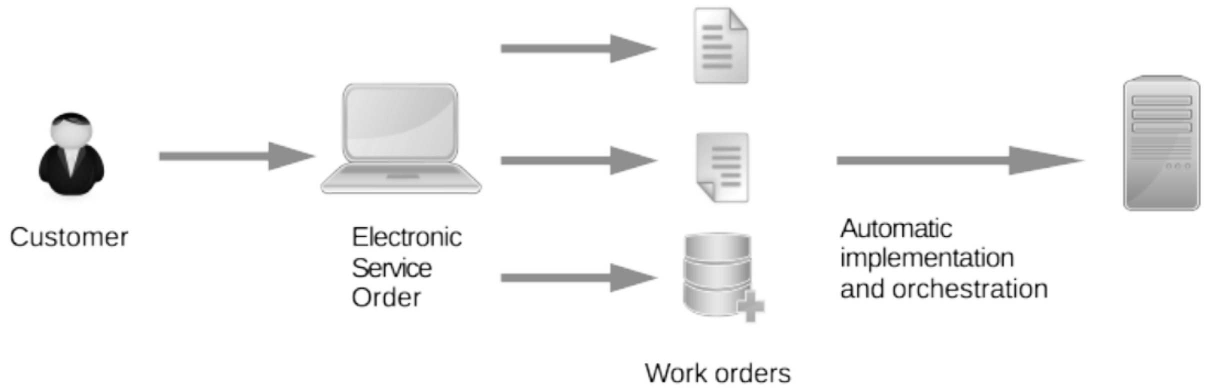

Fig. 5. Automatic resource configuration and orchestration

By using a self service business approach, the carrier may reduce lead time for certain implementations like new service activations, new interconnections to locations that already have an Internet connection and not least, decommissioning or isolating locations that do not require access to the customer's private network.
This new concept of delivering everything as a service (XaaS) [10] has multiple advantages, starting from reduced CAPEX for startup enterprises, reduced complexity in IT infrastructure and a very flexible billing model, based mostly on usage.
Another step forward to buying XaaS services from big service providers is the Date Privacy and Protection Regulation adopted at European Union level. This increases the burden on startup enterprises to comply with data protection regulations if they process personal data. Being compliant with this regulation is expensive and requires a number of assessments and certifications. XaaS service providers offer compliant off the shelf services that do not require extensive knowledge on Security and Risk Management.
Delivering a Network as a Service to companies that need to interconnect several sites would come packed with security compliance and would limit the need of security design rules. Since the CPE (Customer Premise Equipment) is virtualized into the Carrier's datacenter there is little or no need for the customer to act on maintaining, upgrading and patching this kind of equipment.
As stated in the previous paragraphs, the billing process requires a complete new strategy. Ethernet Carriers used to bill customers based on bandwidth, number of locations, customized services and needed service availability using fixed monthly fees. For a new startup enterprise this could mean expensive equipment acquisitions - CPE (CAPEX) and monthly charges for an infrastructure scaled based mostly on their business forecast, not their current needs.
By delivering a virtualized cloud network infrastructure, customers can pay based on usage rather than monthly fees. Also, since the equipment is virtualized there is no need for high initial investment. Expanding capacity can be done with a simple self-service request (e.g. ordering extra processing capacity or redundancy for a virtual router).
Also, by grouping this kind of services, the acquisition process is simplified for small and medium enterprises (SME). Instead of addressing to several service providers and analyzing the compatibility between their services, the SME will have to choose a package that suits his business needs.
For traditional carriers this would mean entering a new market where they will deliver services rather then hardware or infrastructure. This has been proven by the latest mergers or partnerships in IT industry: Cisco and VMware, Ericsson and Mirantis, etc.

5 Conclusions

Currently, enterprises and customers that have data centers or offices in more than one location have to rent networking services from carriers (e.g. VPLS) and deploy equipments capable of performing other kind of functions in each of their locations (e.g. traffic filtering, RADIUS authentication, IPSec VPN, MPLS VPN, proxy servers, etc.).

A virtualized approach of the *"Network as a service"* model would allow carriers to offer line connectivity to each of this sites and also virtualized network equipment (routers, for example), having all interconnected sites bind as virtual ports/interfaces, that can perform all the above functions.

In this case, customers can configure their on services without having to manage a various number of network nodes.

Moreover, Ethernet carriers could become more and more involved in delivering other kind of services that are billed based on usage rather than onetime fees or monthly fees.

The regulations in IT industry are forcing small and medium enterprises (SMEs) to comply with strict standards of data privacy and protection. By choosing to acquire external software or infrastructure delivered as a service, enterprises can delegate the security standards responsibility and implementation to service providers, thus reducing costs and securing compliance.

This new ways of delivering services would provide the opportunity for the traditional Ethernet carriers to enter to a new market where they can deliver several service packages. An example of such a package would comprise the following: connectivity services, Internet connection, virtual router capability, network storage and, last but not least, cloud computing services.

References

[1] Brocade, whitepaper, 2009, *"Carrier grade Ethernet"*, http://www.brocade.com/

[2] IEEE Standards Association, 2004, Reaffirmed in 2011, IEEE Standard 802.1D-2004, *"Local and Metropolitan Area Networks, Media Access Control (MAC) Bridges"*, Available at: http://standards.ieee.org/findstds/standard/802.1D-2004.html

[3] IEEE Explore Digital Library, IEEE Standard 802.1Q, *"Local and Metropolitan Area Networks, Virtual Bridged Local Area Networks"*, 2003, Available at: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8557

[4] M. Pronschinske, *"Infrastructure as Code: When Automation isn't Enough"*, 2014, Available at: http://java.dzone.com/articles/infrastructure-code-when

[5] CHEF documents, *"An overview of Chef"*, Available at: https://docs.getchef.com/chef_overview.html

[6] C. Strachey (June 1959), *"Time Sharing in Large Fast Computers"*, Proceedings of the International Conference on Information processing, UNESCO, paper B.2.19: 336–341.

[7] A. G. Mason, (2001), *Cisco Secure Virtual Private Network*, Cisco Press.

[8] S. McGillicuddy, techtarget.com, 2011, *"OpenFlow hype and the software-defined network"*, Available at: http://searchsdn.techtarget.com/news/2240036862/OpenFlow-hype-and-the-software-defined-network

[9] T. Nolle, techtarget.com, March 2012, *"Software-defined networking could make Network-as-a-Service a reality"*, Available at: http://searchsdn.techtarget.com/tip/Software-defined-networking-could-make-Network-as-a-Service-a-reality

[10] T. Blomfield, techcrunch.com, August 2014, *The World of Everything-As-A-Service*, Available at: http://techcrunch.com/2014/08/09/everything-as-a-service/

Ioan DRAGAN has graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2011 at the Bucharest University of Economic Studies. He also graduated the IT&C Security Master in 2013 from the same faculty. Currently he is a Ph.D. candidate in the field of Economic Informatics at the Bucharest University of Economic Studies. His present research in-

terests are focused on the deployment of telecom Business Support Systems (BSS) within private cloud environments.

Răzvan Daniel ZOTA has graduated the Faculty of Mathematics Informatics at the University of Bucharest in 1992. He holds a Ph.D. in Economic Informatics from 2000 and now is professor at the Department of Economic Informatics and Cybernetics from the Bucharest University of Economic Studies. From 2010 he is Ph.D. supervisor in the field of Economic Informatics. His last published books in 2004 are “IT Basics” and “Computer Networks” in ASE Publishing House, Bucharest, Romania. His recent work focuses on business cloud computing, computer networks and applications.