An Introduction to the Network of the Future

Guy Pujolle

University Pierre et Marie Curie (UPMC) – Laboratoire d'Informatique de Paris 6 (LIP6),
4 Place Jussieu, 75005 Paris, France
Guy.Pujolle@lip6.fr

Abstract. This paper deals with important paradigms for the future post-IP generation: Knowledge and piloting planes, network virtualization and strong closed authentication. We describe these four paradigms and finally we can deduce what could be the future post-IP generation. We first introduce the architecture and a high security scheme that can be deduced from a strong closed authentication where the customers can get a perfect privacy. Then, we describe network virtualization that can provide a powerful way to run multiple networks, each customized to a specific purpose, at the same time over a shared substrate. Finally, we describe the meta control environment based on Autonomic Networking, associated with a knowledge plane and a piloting plane. This piloting system will be able to control the Quality of Service (QoS) in IP networks and consequently responds to users' requirements.

Keywords: Network architecture, future Internet.

1 Introduction

The main objective of this paper is to present the design of a new Post-IP architecture that merge networks and clouds into a common and cohesive framework. The boundaries between networks and services as well as between future networks and clouds are frontiers that should vanish. Indeed, the two areas should merge. This will result in unprecedented flexibility, extensibility and elasticity in composition of public, private and hybrid infrastructures. Protocol stacks, services, applications and information systems will be deployed and instantiated on a need basis. Acquired or leased hosting platforms and execution environments will be released to reduce investment and operating expenses.

The focus of this paper is what makes this new architecture original and different from proposals and research that address services referred to as Software as a Service (SaaS) or Platform as a Service (PaaS) or Infrastructure as a Service. So, we propose a new architecture that could be at the basis of a post-IP Network and Cloud environment. This post-IP architecture is mainly based on

- a high degree of security,
- virtual networking within the cloud,
- a distributed piloting system.

The paper is divided into four main sections. Section 2 will describe the global architecture and introduces what could be the security in this network and cloud

architecture. Section 3 will describe the virtualization paradigm. Section 4 is devoted to the piloting system, and finally the last section will describe a very first test bed of the architecture.

2 The Architecture and its Security

The envisioned network and cloud architecture is depicted in Figure 1. This architecture is composed of :

- A security plane allowing a high-level and mutual authentication of users and servers.
- A cloud plane involving the provisioning of dynamically scalable and virtualized resources as a service over the network.
- A knowledge plane storing information (data and metadata) and high level instructions, detecting when something goes wrong, and automatically feeding the piloting plane for fixing the encountered problem
- A piloting plane acting as intelligent intermediary between control and management entities and the knowledge plane taking into account network and service context.
- A management and control plane containing all algorithms ensuring management and control of virtual and physical resources.
- A virtualisation plane enabling the coexistence of multiple virtual networks on top of the data plane
- A data plane responsible for packet forwarding. This plane contains physical and radio resources to be optimized.

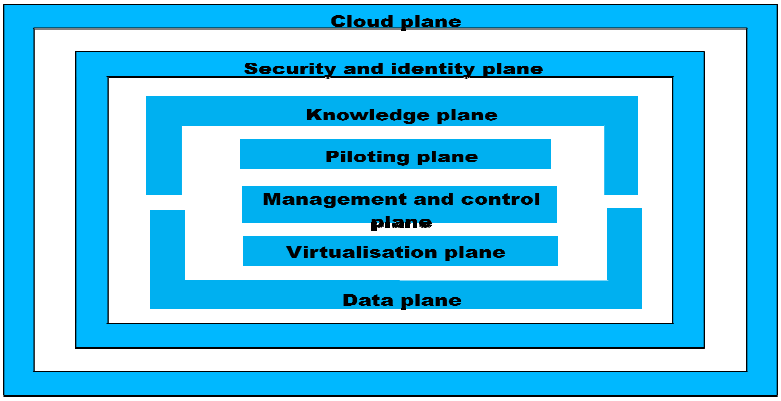

Figure 1 – The Network & Cloud seven-plane architecture

The cloud plane permits to work within the different cloud providers as if they were just one virtual cloud provider. This allows to see the virtual cloud as a service. This vision is described in Figure 2.

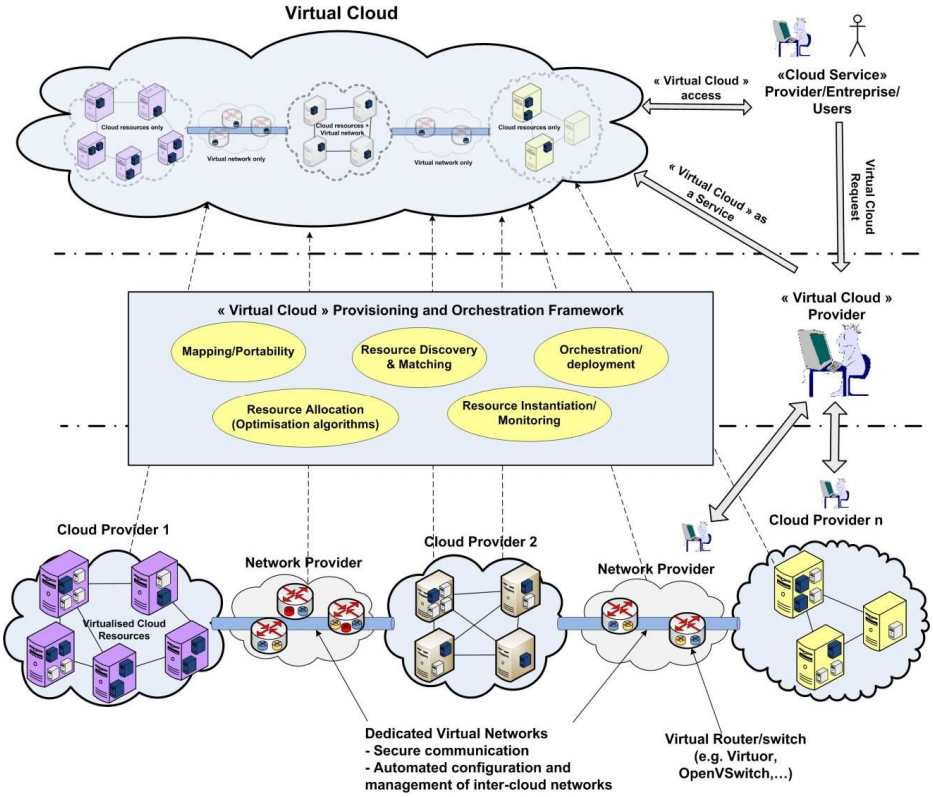

Figure 2 – The cloud environment

The security plane is based on SSL/TLS mutual authentication method and the new paradigm is the execution of SSL/TLS within a smartcard that must be available in all machines connected to the network. Privacy is realized through couples of smartcards so that the connections are anonymous but every connection can be controlled. So a key is necessary to enter the network as shown in figure 3. This solution avoids all logins and passwords and cannot be attacked by viruses and co.

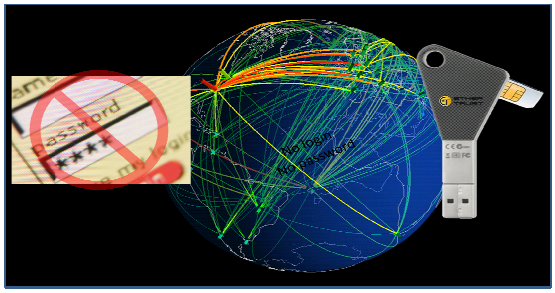

Figure 3 – The Network & Cloud global security

All accesses and mainly web accesses could be realized through an OpenID server or any other identity server with a high security and using the keys of the users. The user will need only his own key protected by his fingerprint (no login, no password, no attack).

3 Virtualization plane

The virtualisation plane is of a prime importance: all equipments will be virtualized from routers to servers including boxes, firewall, PBX, gateways, etc. Then, the network element hardware is virtualised, enabling different virtual machines on a single device. The virtual networks are isolated from each other and are unaware of their virtualisation, the underlying physical network, or their concurrency to other virtual networks. Virtual machines may be created, destroyed, moved, cloned, started, and stopped on the underlying hardware.

The National Science Foundation (NSF) in the United States announced the Global Environment for Networking Investigations (GENI) [NSF-GENI]. Research that falls under the broad conceptual umbrella of this initiative will focus on designing new network architectures and services that range from new wireless and sensor devices to customized routers and optical switches to control and management software. The GENI project attempts to "de-ossify" the Internet and develop and architecture that will allow an easy migration strategy such that users and applications can migrate effortlessly from the current Internet to a future more robust and secure environment. This ''de-ossification ''is mainly based on the concept of network virtualisation.

Virtual machines provide the illusion of an isolated physical machine for each of the guest operating systems. A Virtual Machine Monitor (VMM) takes complete control of the physical machine's hardware, and controls the virtual machines' access to it.

Most projects on virtualization envisage a clear separation of roles between infrastructure provider and virtual network provider. The latter uses the former like an airline uses airport facilities. A virtual network provider allocates virtual resources provided by a number of different infrastructure providers.

The *OpenFlow* initiative is an alternative approach to providing facilities to test new network architectures. This was initiated by *the Stanford Clean Slate* project and is gaining support from both academia and major vendors. The idea is to exploit the fact that most switches and routers contain flow tables. The structure of these tables differs between vendors but all can support a certain common set of functions. OpenFlow provides the means for experimenters to act on the flow tables to alter the way the router forwards packets of certain flows. This conceptually simple facility can be used to create virtual networks.

Virtual network (VN) embedding or mapping has been addressed with various assumptions and scenarios by [Fan][Zhu][Yu][Ricci][Lu][Chowdhury][Houidi]. The general aim is to allow a maximum number of VNs to co-exist in the same substrate while reducing the cost for users and increasing revenue for providers. Optimal VN embedding satisfying multiple objectives and constraints can be formulated as an NP-hard problem.

To circumvent this difficulty, heuristic algorithms were used to assign VNs to substrate resources including greedy algorithms in [Zhu][Yu][Ri], customized algorithms in [Yu], iterative mapping processes in [Lu] and coordinated node and link mapping in [Chowdhury]. Since the underlying physical network can be highly dynamic, authors in [Hon] propose to decentralize the VN mapping by distributing the algorithm in the substrate nodes. The latter act as autonomous agents making decisions based on partial information built from their local knowledge and cooperation with neighbouring nodes.
The future Post-IP network will also look into the choice of the virtual resources to form virtual networks. The server where the virtual resources are stored could contain several thousand of different virtual objects.
Advanced algorithms must be developed to gather information about virtual networks, the load of virtual resources, the physical network, the remaining capacities of the physical network, and the currently supported and required services. Control schemes are crucial tasks in virtual networks since resources are shared by the different virtual networks. Two kinds of control could be addressed: resources control inside the physical networks and optimization of the performance of each virtual network.

4 The knowledge and piloting environment

The knowledge and piloting plane imply an intelligence-oriented architecture using mechanisms able to control automatically placement of all virtual machines into the physical network. The approach is a particularly attractive solution as it involves the development of an automatic piloting system with intrinsic properties as autonomy, proactivity, adaptability, cooperation, and mobility.
The piloting system is definitely a new paradigm. Indeed, this system includes two sub planes that are aggregated in the piloting system. The two sub-planes are the knowledge plane and the configuration plane. So, within the piloting system some mechanisms have to be integrated to drive control algorithms. Indeed, the partition of the piloting system into two sub-planes has the advantage of simplifying the presentation but indeed these two sub-planes are strongly related: the knowledge and the configuration planes are developed in an integrated way. This piloting system has to drive the network through the control plane. For this purpose, the piloting system has to choose the best algorithms available within the control plane to reach the goal decided by the system. Due to the emergence in network environments of virtual control algorithms the choice of the best control algorithm is crucial. The second action of the piloting system is to decide about values to be given to the parameters of the different algorithms. As a summary, the piloting system has to configure the control plane which itself configures the data plane. Currently, in traditional networks the control algorithms are not chosen and the values of the parameters are selected through information collected directly by the algorithms themselves. The advantage of the piloting system is to react in real time on the behavior of the control algorithms. This piloting process aims to adapt the network to new conditions and to take advantage of the piloting agent to alleviate the global system. We argue that a distributed intelligent agents system could achieve a quasi optimal adaptive control

process because of the following two points: (1) each agent holds different processes (behaviour, dynamic planner and situated view) allowing to take the most relevant decisions at every moment; (2) the agents are implicitly cooperative in the sense that they use a situated view taking into account the state of the neighbours.
This architecture has several advantages. First there is a simplification for recovering knowledge necessary for feeding the piloting system. Indeed, in current systems, every control algorithm has to retrieve by itself all the information necessary to execute the algorithm. This behaviour is shown in Figure 4.

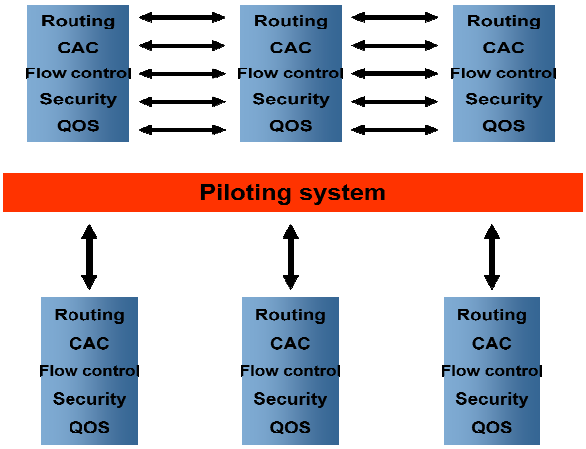

Figure 4 – Advantage of knowledge plane

In this situation, all the control algorithms (routing, CAC, flow control, quality of service, security, availability, mobility management, etc.) have the obligation to look for their own information to decide what is the best routing algorithm, what is the best flow control scheme, what is the best parameters for security control, etc. Indeed, all these algorithms need the same information or knowledge with a strong probability. Thus, in parallel, these algorithms have specific signalling packets to retrieve the same information. Moreover, the different algorithms are not correlated and could decide somewhat contradictory decisions. In the piloting architecture, the decision process is definitely different. This process is outlined in Figure 4. We see in this figure that the control algorithms are fed by the distributed Piloting System encapsulating the Knowledge plane where all the knowledge is. Moreover, this process permits to add new knowledge to pilot the control algorithms. For example, for a routing algorithm in a wireless mesh network, it is possible to add some knowledge on the electromagnetic field if available. This could be crucial in a real time or critical control process.
More precisely, the platform can be built on a multi-agent system to offer some intelligence. The multi-agent system is formed with agents situated in all network equipment (common to all virtual instances). The architecture is shown in Figure 5.

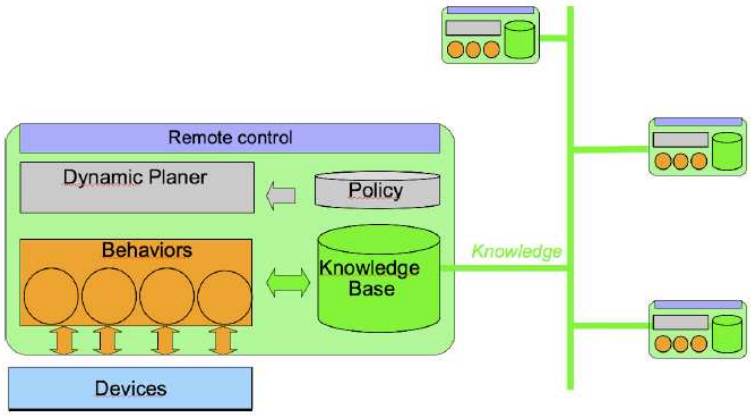

Fig. 5 - The agent architecture

The different entities of the agent architecture are as follows. Each agent maintains its own view of the network on the basis of information obtained through the knowledge plane. This agent-centric view of the network is called the situated view, and is focusing on the agent's close network environment. This produces the knowledge basis that forms the knowledge plane.

The behaviours are autonomic software components permanently adapting themselves to the environment changes. Each of these behaviours can be considered as a specialized function with some expert capabilities. Each behaviour is essentially a sense->decide->act loop. Typical categories of behaviours are as follows:

• Producing knowledge for the situated view in cooperation with other agents.

• Reasoning individually or collectively to evaluate the situation and decide to apply an appropriate action, e.g. a behaviour can simply be in charge of computing bandwidth availability on the network equipment (NE). It can also regularly perform a complex diagnostic scenario or it can be dedicated to automatic recognition of specific network conditions.

• Acting onto the NE parameters, e.g. behaviour can tune QoS parameters.

Behaviours have access to the situated view which operates within each agent as a whiteboard shared among the agent's behaviours. Moreover, some behaviours can or cannot be used depending on the memory space and real time constraints. This behaviour exploits the tolerance for imprecision and learning capabilities. At this juncture, the principal constituents are fuzzy logic, neural computing, evolutionary computation machine learning and probabilistic reasoning.

The activation, dynamic parameterization and scheduling of behaviours (the rule engine is seen as a behaviour) within an agent is performed by the dynamic planner**.** The dynamic planner decides which behaviours have to be active, when they have to be active and with which parameters. The dynamic planner detects changes in the situated view and occurrence of external/internal events; from there, it pilots the reaction of the agent to changes in the network environment.

Finally a policy repository is necessary for defining the rules associated with the physical and the virtual networks..

5 Results and conclusion

A very first prototype of the environment described above was realized. With this prototype a large number of new algorithms and paradigms have been tested. The platform assembles all the elements described in this paper and mainly the virtualisation process, the autonomic plane, the customized virtual networks and all the control schemes through the piloting system. The platform contains between 20 physical machines (industrial PC with quite a high potential). A physical machine is able of supporting 200 virtual machines. So for a total of 20 machines in the network we have been able to experiment a global network with 4 000 virtual resources. The first tests performed of this testbed show that the global throughput of the network can be doubled keeping the same quality of service.
Moreover, when the situated view is reduced to one hop, the piloting system is able to adapt the network in real time.
As a conclusion, we think that the future Post-IP architecture will contain a virtual plane and a piloting system able to optimize the placement of the virtual resource. A virtualized cloud will also necessary to permit the customer to get information in a quite simple and optimized manner.

6 References

1. [Fan] ”Dynamic topology configuration in service overlay networks: A study of reconfiguration policies”, J. Fan and M. Ammar, In Proceedings of the IEEE INFOCOM 2006.
2. [Zhu] ”Algorithms for assigning substrate network resources to virtual network components”. Y. Zhu and M. Ammar, In Proceedings of the IEEE INFOCOM 2006.
3. [Yu] ”Rethinking virtual network embedding: Substrate support for path splitting and migration”, M. Yu, Y. Yi, J. Rexford, and M. Chiang, ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 17-29, April 2008.
4. [Ricci] ”A solver for the network testbed mapping problem”, R. Ricci, et al., ACM Computer Communication Review, vol. 33, no. 2, pp. 65-81, January 2003.
   [Lu] ”Efficient mapping of virtual networks onto a shared substrate”. J. Lu and J. Turner, Washington University, Technical Report WUCSE- 2006-35, 2006.
5. [Chowdhury] ”Virtual Network Embedding with Coordinated Node and Link Mapping”, N.M. Chowdhury, et al, IEEE INFOCOM 2009.
6. [Houidi] ”A Distributed Virtual Network Mapping Algorithm”. I. Houidi, W. Louati and D. Zeghlache, In Proceedings of the 2008 IEEE International Conference on Communications, May 19-23, 2008, Beijing, China, p 5634-5640.