

# Metamorphic Networks

Guy Pujolle\*

Division of IT Convergence Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Korea  
 Guy\_Pujolle@postech.ac.kr

## Abstract

In this paper, we focus on a novel Internet architecture, based on the urbanization of virtual machines. In this approach, virtual networks are built linking specific virtual elements (router, switch, firewall, box, access point, etc.). A virtual network represents a network with an independent protocol stack that shares resources from the underlying network infrastructure. Virtualization divides a real computational environment into virtual computational environments that are isolated from each other, and interact with the upper computational layer, as would be expected from a real, non-virtualized environment. Metamorphic networks enhance several concepts related to future networks, and mainly the urbanization of virtual machines. We present this new paradigm, and the methodology, based on the worldwide metamorphic network platform “M-Net”. The metamorphic approach could solve many complex problems, especially related to Cloud computing services.

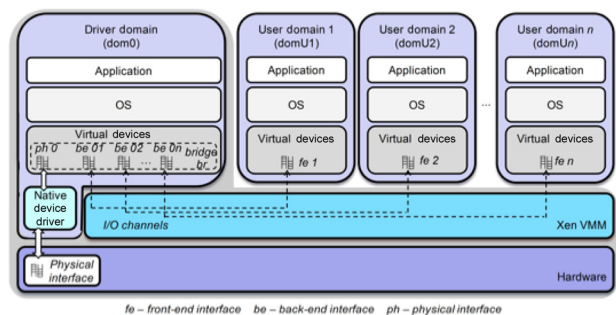
**Category:** Ubiquitous computing

**Keywords:** Automous; Virtualization; Urbanization; Metmorphosing; Network

## I. INTRODUCTION

In network virtualization, different virtual machines (a router for example) share a physical machine, in order to simultaneously provide several network services. Key aspects of this paradigm are isolation, and performance of packet forwarding. Isolation ensures independent virtual network operation, preventing malicious or flawed interferences between different virtual networks. Xen is a virtualization platform that can be used to create virtual machines, each with its own operating system and protocol stack, in commodity computers. Fig. 1 shows the entities relationship in the proposed architecture for Xen virtual networks, while Fig. 2 shows the software architecture in each physical node. The decision was made for the adoption of a modular architecture, to guarantee the easy upgrade of a tool, without disturbing other services.

Moreover, it is easy to add new features to the proposed model, since the basis for the developed modules is virtual network management for the Xen-based testbed tool (for example VNEXT [1]), which aggregates all the pro-



**Fig. 1.** Xen architecture.

**Open Access** <http://dx.doi.org/10.5626/JCSE.2013.7.3.198>

<http://jcse.kiise.org>

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Received 12 June 2013, Accepted 4 July 2013

\*Corresponding Author

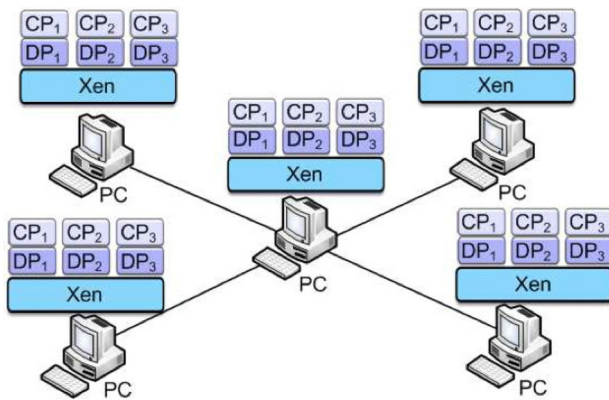


Fig. 2. Xen virtual networking.

posed control modules.

The architecture of the node is based on a client-server model, in which virtual machines are clients of a server located in Domain-0 (dom0). Available services are optional, and can be selected according to the administrator requirements. Moreover, some services run only in dom0, and do not interfere with others in the virtual machine.

Most of the client-server functions used in metamorphic networks (M-Net) are based on the plane separation paradigm, in which data forwarding and control mechanisms are decoupled. Thus control, such as routing, is accomplished in the virtual machine (user domain [domU]), ensuring flexibility in the design of control mechanisms, while packet forwarding is performed in the privileged domain, dom0, providing quasi-native performance. The main advantage of plane separation is the provision of quasi-native packet forwarding performance. A drawback, however, is the fact that the infrastructure administrator imposes a common forwarding plane for all virtual machines. Instead, we offer the virtual network operator the option of using, or not using, the plane separation paradigm, which is responsible for creating a valid copy of the forwarding table of the virtual machine in dom0. The quality of service (QoS) operator module creates a copy of the forwarding rules of the virtual machine, such as queuing disciplines and filtering rules, inside dom0. Hence, these modules accomplish the transfer of the data plane from the virtual machine to dom0. Both modules use the secure channel module, to ensure secure communication between domU and dom0.

Several works focused on defining general policies and rules that serve as an input for the self-management and self-configuration processes. This paper proposes a pioneering solution that is based on a dynamic instantiation of the access network equipment, depending on different criteria, such as the user context, physical environment behaviors, and specifications of the different provided services. The metamorphic network offers different ways of allowing the operators to provide their customers with the requested services, independently from their environ-

mental context. The user will be natively connected in the same way. The entire network configuration at different levels will be assumed by the network itself. The different instances will be autonomously adapted to the user environment, traffic requirement and context events.

## II. METAMORPHIC NETWORK ARCHITECTURE

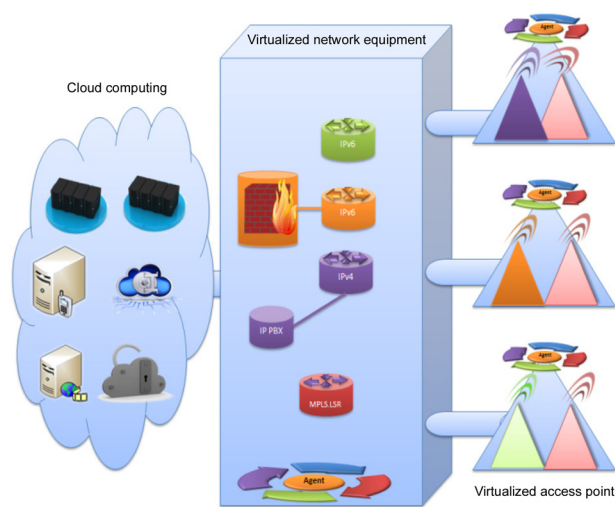
Metamorphic network architecture highlights the increasing constraints for a user to properly connect to Cloud services independently of the environment. In our approach, a virtual machine could be any kind of network equipment used within a real network: router, switch, firewall, access point, session initiation protocol (SIP) server, Internet protocol-private branch exchange (IP-PBX), etc. Virtual machines could implement any protocol stack, such as IPv4, IPv6, multiprotocol label switching (MPLS), or even Post-IP stacks, if available. A virtual network is created by the instantiation of different virtual machines that compose the network topology (Fig. 3). These virtual machines are linked through virtual links. For example, a virtual network router could use any protocol stack associated with a routing protocol.

Metamorphic networks are based on urbanization. Here, urbanization [2] means populating virtual resources in a network, by analogy to urbanizing an area. The objective is to make efficient use of physical resources to support customized flows. Virtual resources should be assigned to physical nodes in an efficient and optimal way. The virtual resources can be moved from one physical machine to another, to increase performance, for maintenance, or to redress performance degradation.

M-Net mainly considers urbanization of the access machine, which can be a broadband router, an Internet box, an xDSL or optic fiber access appliance, etc. This box can accept virtual machines, to customize each user access. Our virtualization level architecture consists of



Fig. 3. Virtual network environment. QoS: quality of service, VoIP: voice over Internet protocol.



**Fig. 4.** M-Net environment. IP-PBX: Internet protocol-private branch exchange, MPLS: multiprotocol label switching, LSR: label switching router.

the components illustrated in Fig. 4.

An agent is installed on the privilege domain of the physical machines, to be able to maintain a local view, and to execute privilege instructions on virtual resources. The agent has access to the entire physical node resources, and can manage from outside the running of virtual machines. All the running virtual resources are automatically discovered, and the related information is then stored into the corresponding knowledge base. A virtual operator would not share routing information tables inside virtual machines with any other agent. This information could give indications about its client's activities and location. To guarantee virtual network isolation, our deployment allows only administrators to configure the inside of their virtual machine instantiation, such as routing table, network application or other configurations. However, to keep more flexibility, the virtual instances could be built by a well-qualified administrator, a local organization such as an enterprise where the user is located, or by a service provider itself. This will improve the adaptation of the instances to the local connection. The administrator has to be recognized by the identification system of the virtual machine to configure it. The agent can manage the instantiation of a virtual machine, but cannot access inside, or interfere with the execution behavior of the running network applications.

The metamorphic network concept is similar to an autonomic computing middleware that is able to monitor (observe runtime states and behaviors), to reason (analyze the states and behaviors, then decide when and what to change, based on predefined rules), to control (perform changes on runtime states and behaviors), and finally to inform about the analysis cause, and decision taken to the management level. In addition, it profits from the flexibility and huge amount of functionalities supported by

virtualization. The network metamorphoses from one state to another, from providing some functionality to others, and from one local network connection mechanism to another. Always, the autonomic behavior aims to optimize, and to guarantee the user access to his or her hosted services on the Cloud. The metamorphosis of the virtual resources is based on semantic information collected from the environment, user context, operator services and defined rules reaction. The final decision will establish a set of management rules on physical and virtual resources, to satisfy the context. Several configurations could be investigated. However, one common aspect is that the management behind the network metamorphic has to provide appropriate actions on the physical and virtual resources each time this is required by the system. A description of the management and control of virtual resources is given in [3].

A typical scenario concerns network customization to follow different users' requirements. Firstly, a user supporting IPv4 protocol needs to perform data transfer. In response to this event, the autonomous local agent will create a new virtual network access equipment implementing IPv4 routing protocol, such as open shortest path first (OSPF), in order to ensure packet transfer. Then, the IPv4 network could be extended by other functionalities, such as SIP signaling through a virtual PBX instance, when the user wants to have local or distant video conferencing. In parallel, an MPLS network is broadcasting a video stream created to satisfy other user requests for watching a video from another provider. The autonomous agent could choose this virtualized access to be more adapted to a transfer, with a service level agreement (SLA) requesting a reduced delay. The instantiation of an MPLS network could be the best solution to this type of service, within these circumstances. Finally, some users supporting only IPv6 protocol stack could ask for an application hosted in the Cloud. To satisfy their requirement, an instance of a virtual IPv6 network access point is used for data exchange between subscribers and their provider. Generally, clients must support the same protocol stack as virtual networks to which they are connected. Users can be connected simultaneously to several virtual networks, if they request multiple heterogeneous services. A metamorphic network environment, as described in Fig. 4, shows a coexistence of multiple instances. Each virtual network provides a specific service to meet the quality of service defined by the SLA. Creating a virtual network is completed by instantiating each virtual machine of the virtual network. These machines must match the service offered for the layer protocol and application. Virtual links that connect them share the physical links that connect the physical equipment.

The development and validation of the protocol to be deployed to achieve interconnection between the physical equipments could take advantages from link virtualization. The connection has to support all the network proto-

col over the link layer. Many works focus on link virtualization, and several protocols are being finalized to meet similar objectives in Cloud computing platforms, such as TRILL [4] and LISP [5].

### III. WIRELESS METAMORPHIC NETWORK

Let us describe in this section metamorphic access networks (Fig. 5). The migration of a virtual access point could be the solution for the wireless access challenges of today. This new type of access point allows the network to instantiate on the fly virtual access instances, guaranteeing connectivity requirements. A virtual access point offers more access facilities to services, by a self-adaptation to connection features supported by the user. The connection is then established through the created virtual access point. Each physical access point is virtualized, and could host virtual access points, as described in a previous paper [6]. Depending on the service requirements, any item of network equipment could be virtualized, and instantiated on the access equipment. This concept allows a single physical device to have multiple Wi-Fi access points, with protocols that can be totally different from each other. Unlike an access point that has multiple service set identifiers (SSIDs)—i.e., several names—with only one protocol stack, the virtualized physical access point may include different protocol stacks that are totally isolated.

The virtualized access point can be conveyed to the client, and used anywhere in the world. The access box may receive, among others, virtual network equipment, and virtual access points (Telco or private APs). These virtual devices allow user connection anywhere in the world, as if the access point was in his or her house or office. This solution will also help to extend the operator coverage area, to meet other potential customers requirements. The allocation of virtual resources to create different virtual networks could never exceed the available resources on each physical device.

From one side, the operator connects its customers to provide them with their services, by transparently adapting the network infrastructure to the customer demand from their context. From the other side, the provider could get more control over the clients' devices. Moreover, certain functionalities are complicated to provide, before becoming native with the metamorphic paradigm. For example, updates can adapt the instances to the services on a real time basis, and can extend the Wi-Fi covering area. The last advantages are similar to those added by a Femtocell [7] solution. However, this is not only localized in just one place, but happens wherever the customer is located. This solution allows the operator to support more customers with its services worldwide. The clients could also carry with them the access box to get native access to their services hosted on the Cloud, and to avoid the hidden complexity. They are not obliged to

know how to work out, and how to establish access without considering the local connection configuration. The access box is based on the network metamorphic concept. The autonomic agent in which decision rules are constantly updated by the operator and neighborhood agents will proceed following these steps:

1. The agent starts sensing available network access to the Internet;
2. The agent monitors traffic exchanged with the user to determine his or her provider, and the connection profile to help him or her to reach his or her services;
3. The agent contacts its operator through the local connection;
4. The operator sends an optional recommendation, which describes the virtual devices that the consumer could use;
5. Depending on the type of services and the operator recommendations, the agent tries to create a tunnel through the local connection to the user provider. The tunnel should support the different flows delivered to the user;
6. The agent instantiates virtual network equipment, to fulfill the service level agreement SLA of the provider with the required quality of services and experience;
7. The available resources on the equipment could be used by the agent to allocate other virtual access points for other providers, if they asked for.

A user already known can be easily connected with the adequate configuration to a virtual access point. The configuration can also take into account some specific features, to customize his or her access to the requested services. The example shown in Fig. 4 presents how comfortable it is for a user to reach his or her services. In his or her office, the user can exploit a virtual access point instance created by his or her operator, to be connected to his or her services. The operator is using the local network infrastructure to go through, and to guaranty the requested connections. When the user tries to access his or her services at home, the connection could also be fulfilled by the same virtual access point instance, but the autonomous agent can transparently adapt this instance to the user settings. In fact, the user context has changed, and the local connection is no longer the same. So, several decisions could be taken to solve such a situation, and guarantee the access of the user to his or her provider. After establishing access to the provider, the operator could suggest the migration of the virtual access point hosted within the user office. This situation could be also solved by the instantiation of a new virtual access point, but keeping the same configuration adapted to the local home connection.

The user connects with a unique configuration to the virtual instances independently from his or her location,

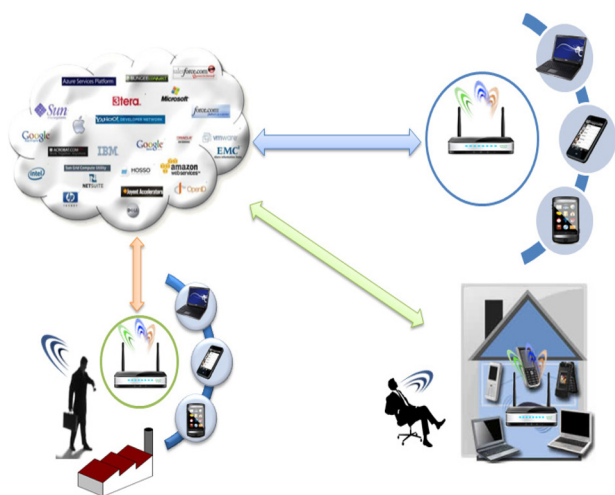


Fig. 5. Metamorphic network scenario.

using the local access connection. The operator can share physical resources with other operators that can deploy their own virtual access points to their clients, and to potential users around. The network infrastructure offered by our solution is self-adapting to meet the specific needs of user’s services. The other operators may allocate available resources to guarantee their user accesses to their services. These operators may also propose some available resources to new clients. The clients could profit by already deployed infrastructure supporting a metamorphic network, through the nearest access box deployed by registered users.

This new generation of metamorphic network equipment allows several operators to share the same physical Wi-Fi access point, while being definitely independent from each other. Each operator can modify its protocol stack and supported functionalities. Another possible use of this kind of access point could be: applications requiring very high security, or requesting real-time QoS, or providing streaming video transmissions. Depending on the capacity of the physical access point, three to ten virtual access points can be considered. The capacity of a virtual access point depends on the resources assigned. The first generation of physical access points that can be virtualized based on the IEEE 802.11 protocols, g or n, are limited by the flows to be supported, and will generally hold between three and five internal virtual access points. New generations, such as 802.11ac or 802.11af, will support much more virtual access points, if the processor and memory performance are sufficiently powerful.

The access points prevent reconfiguration when a client moves, and transparently provide the same services. By adopting the metamorphic network scheme for wireless networks, some problems remain to be solved, such as load balancing between virtual access points, development of urbanization strategies, efficient resistance to attacks, assessment of the overhead of para-virtualiza-

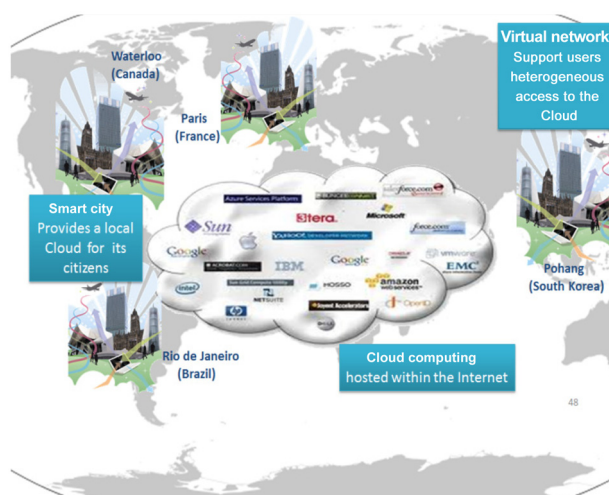


Fig. 6. The M-Net platform.

tion, and migration management and real-time applications with strong constraints.

#### IV. M-NET PLATFORM

The M-Net platform has already received support from different partners: Université Pierre et Marie Curie (UPMC, France) and VirtuOR (France) with 4 nodes, POSTECH (South Korea), Waterloo (Canada), and Universidade Federal do Rio de Janeiro (UFRJ, Brazil) [8] (Fig. 6). As described in this paper, the M-Net platform is based on the metamorphic network concept. So, each physical node is virtualized into at least 100 virtual machines, and many more, if they are not strongly active all the time. The physical resources are linked over the Internet by an overlay based on virtual eXtensible local area network (VXLAN) tunneling. We operate a VXLAN solution as already described, within the Open vSwitch tool maintained by the ovs-vxlan project.

A typical scenario that this infrastructure can provide is the migration of different access machines. For example, a user working usually into the UPMC premises (France), can use the UPMC network infrastructure when working in another place, when hosted within the M-Net platform. The user is identified by his or her virtual access point, as if he or she was in his or her office. The agent embedded into the access box will take into consideration the user context, and will adapt the virtual network access equipment to the different events. After migration in this case, the virtual access point will appear identically as if it was into the UPMC premises. However, the virtual instances are metamorphosed, to fit better with the local network infrastructure connection. The virtual access point will use the available local connection to guarantee the user access to his or her services hosted in the M-Net platform. Virtual Wi-Fi access points

belonging to Internet providers can be reached from M-Net.

The M-Net platform will be extended and improved by innovative ideas, based on the network metamorphic approach. After a stabilizing period, the platform will be available for other academic researchers, to allow them to work on more complex scenario tests. The distributed autonomous agents will be improved by new behaviors to fulfill their objectives of providing all the necessary actions for user access to the provided services hosted in the Cloud, independently from user context, or changing events.

## V. CONCLUSION

Advances in network virtualization and autonomous network piloting could be integrated within the metamorphic network concept. This gives a new opportunity for network operators to take more advantages of network resources. We exposed the challenging ideas that this new concept opens. Indeed, this new paradigm could satisfy many of today's networks telecommunication challenges, especially access guarantees to Cloud computing services. We have developed a use case of metamorphic networks with access points. We have started a new worldwide M-Net platform supporting this approach in a real environment. Our future work will investigate different incomes, to improve the M-Net platform. One of the goals is to develop international scenarios to validate the metamorphic network behavior, interaction and reactivity.

## ACKNOWLEDGMENTS

This research was supported by the World Class University program funded by the Ministry of Education,

Science and Technology, through the National Research Foundation of Korea (R31-10100). Development has been realized by O. Braham (VirtuOR), and through cooperation with Professor Otto Carlos Duarte and his team at Universidade Federal do Rio de Janeiro (Brazil).

## REFERENCES

1. O. C. Duarte and G. Pujolle, *Virtual Networks: Pluralistic Approach for the Next Generation of Internet*, Hoboken, NJ: Wiley-ISTE, 2013.
2. O. Braham, A. Amamou, and G. Pujolle, "Virtual network urbanization," in *Communications: Wireless in Developing Countries and Networks of the Future, IFIP Advances in Information and Communication Technology vol. 327*, A. Pont, G. Pujolle, and S. V. Raghavan, editors, Heidelberg: Springer, 2010, pp. 182-193.
3. O. Braham and G. Pujolle, "The metamorphosing network (M-Net)," in *Global Information Infrastructure and Networking Symposium*, Choroní, Venezuela, 2012.
4. Transparent Interconnection of Lots of Links Working Group, "<http://datatracker.ietf.org/wg/trill/charter/>."
5. D. P. Chi, S. Seed, G. Pujolle, P. Raad, and P. Gallard, "An open control-plane implementation for LISP networks," in *Proceedings of the 3rd IEEE International Conference on Network Infrastructure and Digital Content*, Beijing, China, 2012, pp. 266-270.
6. O. Braham and G. Pujolle, "Virtual access point to the Cloud," in *Proceedings of the 1st IEEE International Conference on Cloud Networking*, Paris, France, 2012, pp. 206-208.
7. J. H. Yun and K. G. Shin, "CTRL: a self-organizing femto-cell management architecture for co-channel deployment," in *Proceedings of the 16th Annual International Conference on Mobile Computing and Networking*, Chicago, IL, 2010, pp. 61-72.
8. M-Net, "<http://www.m-net.org/>."



### Guy Pujolle

Guy Pujolle received the Ph.D. and "Thèse d'Etat" degrees in Computer Science from the University of Paris IX and Paris XI on 1975 and 1978, respectively. He is a computer science professor at Pierre et Marie Curie University-Paris 6 during 1981-1993 and from 2000 to the present day, a member of the Institut Universitaire de France from 2009, a member of The Royal Physiographical Academy of Lund, Sweden, and a distinguished visiting professor at the Division of IT Convergence Engineering of the Pohang University of Science and Technology (POSTECH).

Guy Pujolle is the French representative at the Technical Committee on Networking at IFIP. He is an editor for ACM International Journal of Network Management, Telecommunication Systems, and Editor in Chief of "Annals of Telecommunications". Guy Pujolle is a pioneer in high-speed networking having led the development of the first Gbit/s network to be tested in 1980. He was participating in several important patents like Deep Packet Inspection (DPI), virtual networks or virtual access points. Guy Pujolle is co-founder of QoS MOS ([www.qosmos.fr](http://www.qosmos.fr)), Ucopia Communications ([www.ucopia.com](http://www.ucopia.com)), EtherTrust ([www.ethertrust.com](http://www.ethertrust.com)), Virtuor ([www.VirtuOR.fr](http://www.VirtuOR.fr)), and Green Communications ([www.green-communications.fr](http://www.green-communications.fr)).