Virtual Wireless Network Urbanization

Othmen Braham, Guy Pujolle

Virtual Wireless Network Urbanization

Othmen Braham
VirtuOR
Paris, France
Email: Othmen.Braham@virtuor.fr

Guy Pujolle
Pierre and Marie Curie University (Paris VI)
Paris, France
Email: Guy.Pujolle@lip6.fr

***Abstract*—Adapting virtualization concepts to satisfy many of today's network telecommunication challenges receives more and more attention. We have developed virtual environment design to allow the coexistence of virtual networks and their respective operators. In our approach, virtualized wireless access equipment are deployed to provide users more flexibility to access their services delivered by the allocated virtual networks. In this paper, we describe how we improved virtual network urbanization by including virtualized access point equipment. We developed this approach for supporting wireless network advantages such as mobility, coverage areas, installation speed and simplicity. The relevant results of the deployment are exposed.**

***Index Terms*—Virtualization, Wireless, Network, Urbanization**

I. Introduction

The virtual network environment is formed by the amount of bounded virtual resources provided by physical network equipment. The physical nodes are connected through physical network link. Each physical node offers its virtualized resources via a hypervisor. The hypervisor guarantees concurrent virtual machines running in isolation conforming to their allocated resources. The virtual machines share physical host resources in term of CPU, memory and I/O network interface.

In our approach, virtual machine could be any kind of network equipment used within real network: Routers, Label Switch Router, firewall, access point, SIP router, IP PBX, etc. A virtual machine could implement any stack protocol such as: IPv4, IPv6, MPLS, etc. A virtual network is created by the instantiation of each virtual machine that composes its topology. These virtual machines are linked through virtual links. A virtual network router could use any protocol stack associated with a routing protocol such as: OSPFv2, OSPFv3, Rip, RIPng, BGP, etc.

This paper describes the integration of wireless virtualization concepts to facilitate the management of a high evolutive virtual network environment. Each device could be connected to several virtual providers using its multiple physical or virtual network interfaces. Although many applications and protocols have been developed to offer specific features and tools for virtual wireless access point interface [12], few works has been reported on providing virtualization support for wireless environment. We have developed that kind of software[3]. This software permits the instantiation of virtual networks within a virtualized environment and the ability to configure each part. We have improved our previous work by taking into account the wireless network behaviour.

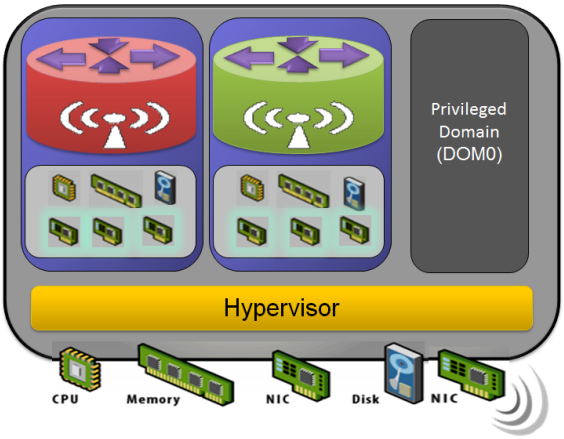

Fig. 1. Router virtualization.

Aiming to provide a complete network environment based on virtual networks, we developed this architecture under the following specifications:

- Virtual network isolation based on hypervisor isolation;
- Defining a gap between physical and virtual resource management;
- The virtual machines that compose virtual networks could be any network equipment;
- Each virtual network could be accessed independently.

To present an overview of our virtual wireless network approach, this paper focuses on adapting the virtual network management application to fulfil wireless network needs. The rest of this paper is structured as follows. Section 2 describes the virtual network environment platform. Section 3 presents the virtual wireless network approach. Section 4 presents the experimental evaluations. Finally, Section 5 concludes the paper with the description of our future work.

II. Virtual Network Environment Platform

The Physical Node is the component upon which all virtual machines reside. This component corresponds to the physical machine with a physical location and hardware specification. Physical nodes are characterized in terms of CPU, memory, wireless and wired network I/O since we are focusing on

network equipments. We used in our platform physical equipment with 4 GByte RAM, C2D-2.4 Ghz CPU and six 1 Gbps Ethernet network interface.

We adopted XEN [1] as hypervisor because it is open source and XEN is increasingly popular among virtual network infrastructure researches. XEN is also a high performance resource-managed virtual machine monitor (VMM) [4]. The VMM provides isolation and safety for running virtual machines. Despite the advances in virtualization technology and its applications [13] , the overhead of network I/O XEN virtualization [2], [5] still have a negative impact on the performance of network intensive applications. However, the performance is close to the performance of non-virtualized software routers if the need for processing overhead is satisfied and allocated resources are oversized to support unfairness in resources sharing.

An instantiation of a virtual machine needs the following items: kernel, file system, network application and the configuration description of resources that will be allocated. We used small size virtual machines that can support different network applications. We have integrated some available open source projects inside virtual machines such as: Xorp [6], Quagga [7], Asterisk [8], MPLS-Linux [9], Opensip [11]. We elaborated a virtual machine list that covers different kind of network equipment. We have adapted the virtual machine operating system to support several types of protocol stacks. We deleted unused operating system modules to eliminate their effect on network traffic. Using light weight virtual machines increases routing performance and allows actions such as instantiation, migration, and backup.

The virtual network environment as shown in Fig. 2 consists of several virtual networks. Each virtual network can guaranty different kinds of service to satisfy the requested Service Level Agreement (SLA). The virtual network creation is achieved by the instantiation of each virtual machine. The virtual machines must correspond to the offered network service in terms of protocol stacks and network application.

As described in Fig. 2, we have different protocol stacks IPv4, IPv6 and MPLS network running on the same physical nodes and isolated down to hypervisor isolation. The IPv4 network is extended by IP PBX functionalities to support video conference service. MPLS network is used for video streaming service due to its minimal delay guarantee. The IPv6 network guarantees data exchange service between its users. The clients of each virtual network use the same protocol stack and are able to self-configure to get simultaneous connections to their virtual networks. They can be connected to several virtual networks at the same time to take advantages of the different proposed services.

This platform could be used by several operators. They can share the deployed physical infrastructure by allocating the virtual available resources. The amount of allocated resources could be used to create different instantiation of virtual networks. Depending on resources needed by each machine that compose the network, virtual machines have to be placed appropriately to an available resource location that satisfies the virtual network topology.

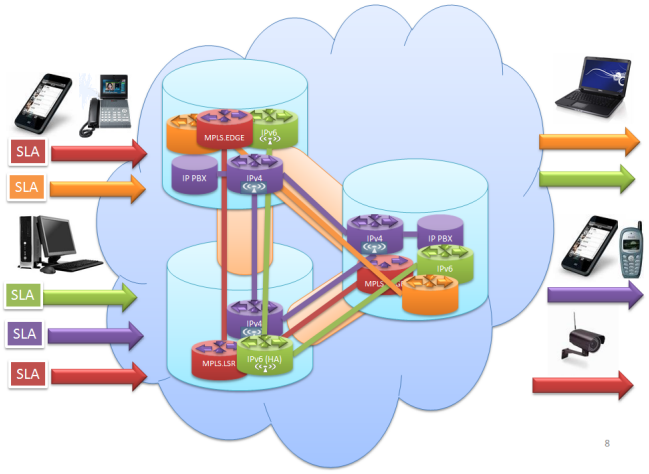

Fig. 2. Virtual network environment platform.

The network is distributed by nature. Due to virtualization level capability, the network becomes also dynamic. A new operator can allocate available virtual resources and can instantiate a new virtual network with a new kind of service. Another operator could delete a virtual network that is not any more in use to free the allocated resources. The virtual machine migration could be used for different purposes in this kind of platform to ensure high availability and load-balancing. In the next section, we describe our virtual wireless network architecture which creates multiple virtual access points implementing different network protocol and providing heterogeneous services.

III. Virtual Wireless Network Deployment

We have integrated wireless network virtualization within our virtual environment. Each user, depending on their wireless interface capabilities, could be connected to several virtual networks simultaneously. Those virtual networks are extended with virtual access points. The virtual access points implements the same stack protocol as the virtual network that they belong to. Each virtual network could be allocated by a independent virtual wireless operator and extended as possible by other virtual network services within virtual environment or from Cloud services.

The physical wireless interface offers the ability of creating multiple virtual wireless interfaces as virtual acces point (master mode) with different SSID and MAC addresses. In our case, the physical wireless interface is limited to four virtual wireless interface. Each virtual wireless interface is connected to a virtual machine access point through a dedicated bridge. The virtual access point is named the same as the SSID affected to its virtual wireless interface. The creation of virtual wireless interface and the configuration of the channel and the SSID are done in the privilege domain DOM0. The virtual access points have their virtual access interface isolated by the wireless interface hardware capabilities. The virtual machine access point are isolated down to the hypervisor isolation.

The global architecture of the virtual access point is shown in Fig. 3.

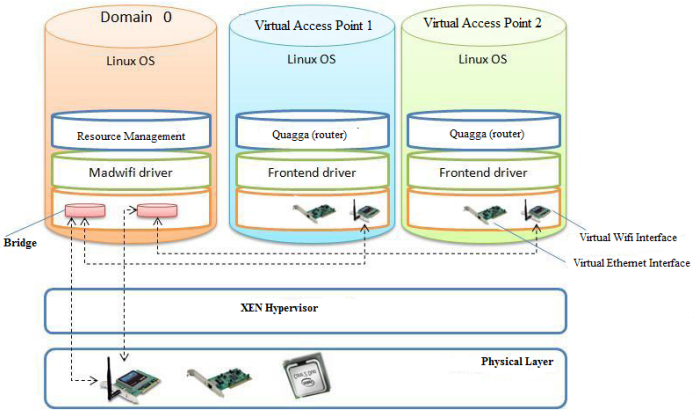

Fig. 3. The architecture of the virtual access points.

The virtual access point allocates at least one virtual wireless interface allowing it to reach connected users in its coverage area. Each virtual access point is detected by user transparently as a physical access point using native system tools. The virtual access point implements a DHCP server which provides IP addresses (IPv4 or IPv6) for users asking for a connection. This virtual machine includes also the access router to the rest of the virtual network. The physical node could instantiate simultaneously different type of access points. In fact each physical WiFi interface could be shared between several virtual machines including access point functionalities. We developed mesh virtual networks over a physical mesh network. A mobile device can be connected simultaneously to the different mesh network using virtual access point: a virtual access point possesses on a hypervisor permitting to support different stacks of protocol. Virtual access points deployement is described in Fig. 4.

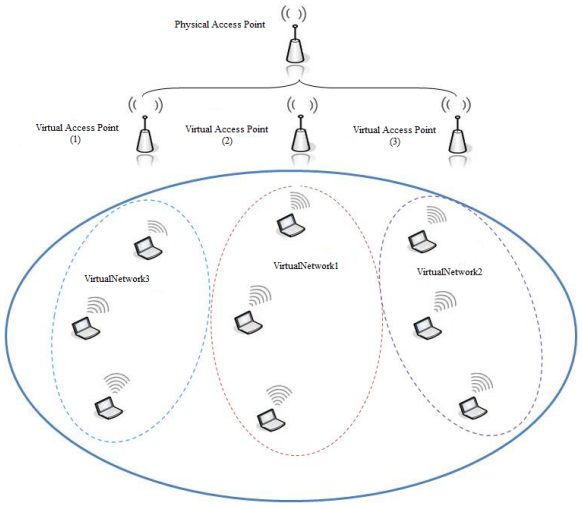

Fig. 4. Virtual access points deployement.

We developed this architecture aiming the following advantages:

- Reducing the number of visible physical access point which are deployed by different operator;
- Sharing the deployed wireless resources between operators by using similar technique for allocating physical nodes resources;
- Allocating a virtual access point to serve an area for a period of time with a specific network services implementing diverse stack protocols reduces cost and time for such service deployment;
- Extending virtual networks which provide virtual services within an area occupied by wireless users.

The virtual access points are managed the same as for the other virtual machine. This means that all actions are supported such as: creation, migration, destruction, pausing, unpausing, etc. However, for virtual wireless network urbanization, we have to take in consideration that the allocated channel, SSID and MAC address must be different to avoid packets transfer error and access conflict.

IV. Experimental Evaluation

After describing our virtual wireless network architecture, we have done some measurement on throughput, and jitter to have an idea about the behavior of such deployment. It's important to have an observation about the isolation between the instantiated virtual access points and how this approach supports several virtual networks transmissions. It indicates us how many virtual operator would probably be accepted to share wireless physical resources.

Our experimental testbed consists of 4 physical machines. The physical node provides the necessary virtual resources for three instantiated virtual access points. Three client laptops are connected to their virtual access point respectively. Each one has C2D 1.6 GHz CPU, 2 GByte RAM and 54 Mbps wireless network interface. The Physical node that will host all virtual access points has 4 GByte RAM, C2D-2.4 GHz CPU, six 1 Gbps network interface and D-Link DWL-G520 Wifi card. All instantiated virtual access points have this configuration: one x86 virtual CPU, two 100 Mbps virtual interfaces, 20 MByte image disk size, 80 MByte RAM, DHCP server and Quagga router as network application.

We evaluated the virtual wireless network access using three virtual WiFi access points independently of the mesh virtual networks. A first ll gives us the results depicted in Fig. 5. In the use experiment, we begin with one virtual access point working then after 180 seconds a second one is working, then a third one after 360 seconds. After 720 seconds the first one is stopped and finally after 900 seconds the second one is stopped. The three flows are three different MPEG 2 flows to study the intrinsic performance of the access. On this picture, we see that with just one virtual access point working, we get between 22 and 24 Mbps on the average. This depends on the movies going through the virtual access point. With two flows the total average rate decreases a little bit to a total of 21 Mbps. Finally with the three flows in the same time the total throughput is approximately 20 Mbps. We can conclude

that the hypervisor takes a part of the power of the physical access point.

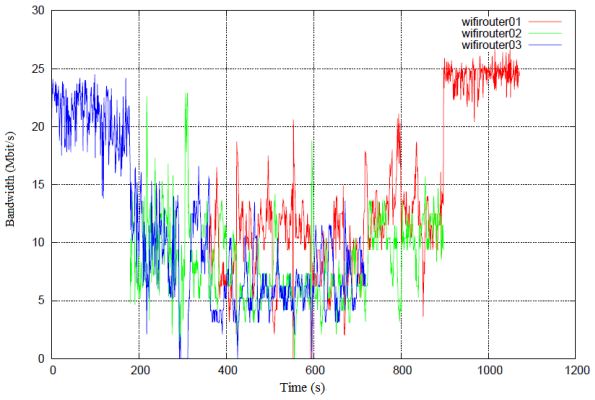

Fig. 5. Throughput measurement of the three flows.

A second experiment considers a unique application with different flows: the virtual networks are adapted to the characteristics of the flows. In this experiment, we were interested in the jitter associated to the different flows. Indeed, the MPEG-2 movie could be reproduced at the receiver with some delay. However, we are interested in evaluating the jitter coming from the three virtual access points. The difficulty of the solution we proposed comes from the impossibility to address priority between the virtual access points. This is due to the isolation strategy we used in our solution. The results are described in Fig. 6 concerning the three flows of the MPEG 2 application. We can observe that the jitter of the three flows are comparable since they are scheduled with the same privileges. If we want to give some priorities to some flows we need to introduce in the privilege node (DOM0) an algorithm allowing to prioritize the demands of access of the different flows. The drawback of this solution is the obligation to know the semantic of the flows to be treated in the access point.

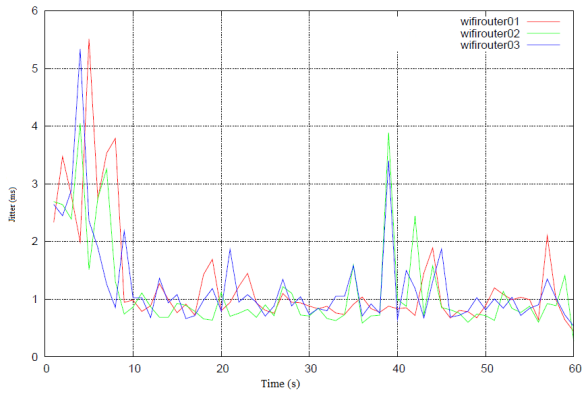

Fig. 6. The jitter of the three flows.

V. Conclusion

Advances in virtualization technologies have created new opportunity for network operators to take advantage of network resources more efficiently. We try to adapt virtualization concepts to satisfy many of today's network telecommunication challenges.

We have proposed virtual network environment based on virtual access points. We have presented the design of the mechanisms underlying the virtual network platform. We have implemented this approach in a real prototype. Using experiments with realistic virtual router network applications and benchmarks, we demonstrated the performance/cost benefits and the effortless applicability of wireless network virtualization within virtual environment. We have measured the performance of this architecture with a real Testbed.

Our future work will also investigate different means to improve virtual wireless network behaviour, interaction and reactivity.

Acknowledgment

We would like to acknowledge VirtuOR to have supported our researches. They help us to develop our architecture and validate it on a real platform.

References

[1] P. Barham, B. Dragovic, K. Fraser et al., *Xen and the art of virtualization*, ACM Symposium on Operating Systems Principles (SOSP), 2003.
[2] F. Anhalt and P. Primet, *Analysis and evaluation of a XEN based virtual router*, HAL-CCSD, 2008.
[3] O. Braham, A. Amamou and G. Pujolle, *Virtual Network Urbanization*, IFIP World Computer Congress (WCC), 2010.
[4] T. Deshane, Z. Shepherd, J.N. Matthews et al., *Quantitative Comparison of Xen and KVM*, Xen Summit, Boston, 2008.
[5] J.R. Santos, G. Janakiraman and Y. Turner, *Xen Network I/O Performance Analysis and Opportunities for Improvement*, HP Labs, 2007.
[6] *Xorp*, http://www.xorp.org
[7] *Quagga*, http://www.quagga.net
[8] *Asterisk*, http://www.asterisk.org
[9] *MPLS-Linux*, http://sourceforge.net/apps/mediawiki/mpls-linux
[10] *Opensips*, http://www.opensips.org
[11] *madwifi-project*, http://madwifi-project.org/
[12] M. Vipin and S. Srikanth, *Analysis of open source driver for IEEE 802.11 WLANs*, Wireless Communication and Sensor Computing ICWCSC, 2010.
[13] G. Wang and T.S.E. Ng, *The Impact of Virtualization on Network Performance of Amazon EC2 Data Center*, IEEE INFOCOM'10, San Diego, 2010.