Scientific Journal of Impact Factor (SJIF): 4.72
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 2, February -2017

Network Virtualization: Design Issues and Solutions

Isha Pathak[1] & Atul Tripathi[2]

[1]*Miranda House College, University of Delhi*
[2]*Mahatma Gandhi Central University of Bihar, Motihari*

Abstract: *Network virtualization has emerged as an attractive and important concept in various networking technologies. It combines various physical networks to give the illusion of single network to network users. Given the increasing importance of this technology, we examine some of the design issues and solutions that have been recently proposed in this area. We also identify some of the challenges that still need to be addressed in the future to ensure its cost-effective deployment.*

Keywords- *Virtualization, Cloud, Networks, Processor, Performance*

I. Introduction

Over the years, virtualization has evolved from enabling the sharing of large mainframes to various application environments. Presently, various types of virtualization are being used in many areas including operating system, storage, and network to improve to improve system security, reliability, availability, flexibility and costs. Virtualization aims to provide services, in a timely, on demand manner transparently to users, by sharing the underlying hardware resources. In virtualization, there is no need to own the hardware but it can be rented on an on-demand basis from a cloud computing environment available to the users. Network Virtualization is an emerging technology that enables the creation of several co-existing logical network instances (or virtual networks) over a shared physical network infrastructure to make them appear as a single network [1]. With network virtualization, all hardware and software in the virtual network appear as a single collection of resources. In classical systems different servers are used by different operating systems as depicted in Figure1 [2]. Network Virtualization enables only one server for different operating systems. Thus, virtualization technology enables users to access any facility at any time, from any location, with a minimum amount of management. Leading drivers of network virtualization technology are data, server and licensing consolidation because they result in easier management and decreased hardware. Another aspect is disaster recovery which also cannot be provided by physical servers. In contrast network virtualization can play a helping role here as actually virtual machines are nothing more than files that can be backed up on to tape. As a result, in a disaster-recovery situation, all one has to do is rebuild a single host computer and reinstall the hypervisor (virtual machine manager) software. Then one can restore the virtual machine backups from tape, restart the virtual machines, and be backing up and running in a matter of days instead of weeks.

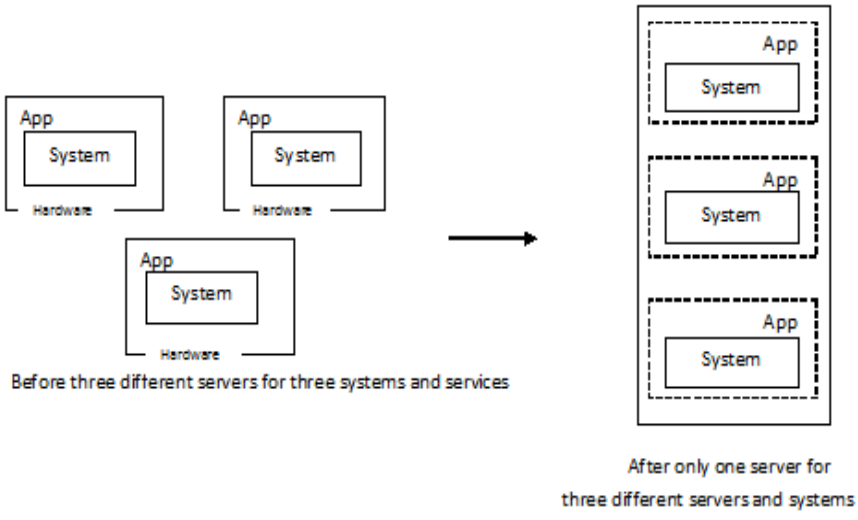

Figure 1: Virtual Network as a Single Collection of Resources

Network Virtualization has several motivations behind it that includes cost-effective sharing of resources, customizable networking solutions and the convergence of existing network infrastructures. Thus deploying network virtualization

provides various benefits that include de-ossification of the current network architecture, reduced cost of ownership, resource usage optimization, coexistence of multiple virtual networks over a shared physical infrastructure and so on.

To support Network Virtualization and enable its deployment, various issues must be addressed. We discuss these issues below and describe some of the recent solutions that have been proposed to enable their deployments.

II. Basic Operation of Network Virtualization

A virtualnetwork is a computernetwork that consists of virtual network links. A virtual network link is one that does not consist of a physical (wired or wireless) connection between two computing devices but is implemented using logical connections. The aggregation of the various network resources to offer an effective service to the network users is called a Virtual Network.

Network virtualization is required to provide multiple partitions of the network that appear to be isolated from each other. These partitions, also referred as Logically Isolated Network Partitions (LINP), may be created over a single physical infrastructure. Figure 2 shows multiple LINPs created in a network virtualization framework. Each LINP is isolated from each other on the functionality and amount basis and is programmable to satisfy the user's demand. The users' demand is conveyed to an entity known as LINP manager which coordinates the infrastructure's resources so that the appropriate LINP is provided to the user based on the user's demand requirements.

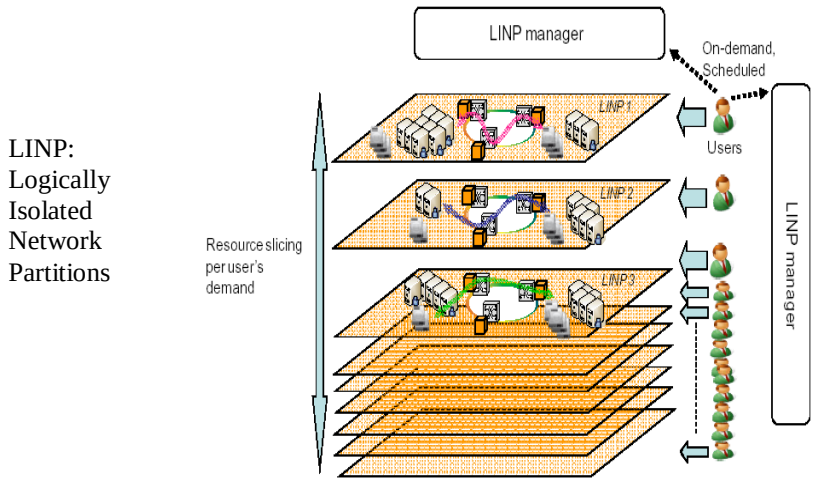

Figure2: Network Virtualization [3]

III. Network Virtualization Research Issues

There are various research issues and challenges that need to be addressed in order to enable the wide deployment and adoption of network virtualization. We discuss some of these issues and challenges below along with recent solutions that have been proposed recently to address them.

Interfacing

Service Providers (SP) create physical infrastructure from one or more Infrastructure Providers to build their virtual networks. Thus, it is essential for every Infrastructure Provider to provide a well defined interface that follows some standard so that service providers can submit their requirements based on the standard. In order to enable this goal, the virtual network request should ideally be in terms of virtual nodes, virtual links etc along with their corresponding attributes. In the same way, the interfaces between the service providers and end users must be clearly identified. Examples of such interfaces between these collaborating entities have been described in the AGAVE [4] framework. AGAVE specifies an open connectivity service provisioning interface to allow Service Providers to interact with underlying IP Network Providers (INP) for the provision of end-to-end IP-based added-value services.

Visibility

Visibility is important for network troubleshooting and management. The capability to gaze into overlay tunnels and comprehend how they go across a particular physical path is crucial to optimizing the performance of the network.

Network Virtualization vendors advertise monitoring and analysis within their solutions, with the skill to examine traffic trends (throughput, latency) within the solution itself. Nevertheless, most of these implementations are comparatively elementary, concentrating on data capture.

Signaling and Bootstrapping

Signaling is the exchange of information between two points in the network involved in the setup, controls, and termination of each connection in the network. As service providers have to build their own virtual networks, they must already have network connectivity with the infrastructure providers to forward their requests and hence network connectivity is a prerequisite to virtual networks build up [5]. So far, the network virtualization environment is not mature enough to support itself for signaling. Therefore, signaling must be handled in the mean time by other means of communication such as through actual physical connections through the Internet.

Bootstrapping is the basic term referring to a self-sustain process that proceeds by itself. Bootstrapping capabilities are needed to allow service providers to customize the virtual nodes and the virtual links allocated to them to create their virtual networks. Both of these requirements (i.e. signaling and bootstrapping) need at least access to another network like a physical network such as the Internet that will always be present to provide connectivity to handle these issues. Genisis [6] and Tempest [7] follow this approach and provide a separate bootstrapping interface.

Admission Control accounting and Distributed Rate Limiting

To guarantee quality of service, infrastructure providers must not overbook the resources allocated to the service providers. Accurate accounting and admission control algorithms must be implemented so that the resources allocated to the virtual networks may not exceed the physical capacity of the underlying substrate network (physical network). In the present Internet scenario, admission control is performed for individual nodes or links. In contrast with network virtualization admission control is performed on the whole virtual network.

It is essential to employ distributed policing mechanism in order to avoid constraint violations by globally distributed virtual networks. This is done to ensure that service providers cannot overflow the amount of resources allocated to them. Raghavan et al. [8] presented a global rate limiting algorithm in the context of cloud-based services in today's Internet and the same concepts have to be developed in the case of network virtualization. Mori et al. [9] have proposed an admission control method to improve the network robustness of both the physical and virtual networks where users' requests are rejected when the network robustness of the physical networks becomes low.

Virtual Network Mapping

There are many possibilities for mapping of a given virtual network to physical network. To increase the number of co-existing virtual networks it is important to determine the way to translate a service provider's request to available resources on a physical network. Even though all the requests are known in advance, the constraints on nodes and links make this embedding problem a NP-hard problem (multi-way separator problem [10])

The solutions that exist today can broadly be categorized into two main categories; offline problems and online problems. Offline problems are those where all the service providers' requests are known a priori. Load balancing can be achieved in the underlying physical infrastructure by assuming that there are unlimited resources available [11]. Another proposed solution maps only one virtual network with the aim to minimize the cost involved in mapping [12]. Other solutions for the offline problem are based on multi commodity flow that exists in the VPN context [13, 14]. To brief, multi commodity flow problem is a network flow problem with multiple commodities (i.e. flow demands) between different sources and sink nodes.

In the case of the online problem, the requests are generated on-demand. Fan and Ammar [15] presented a solution to determine the dynamic topology reconfiguration for service overlay networks with the requirement of dynamic communication between the substrate network and the overlay networks. Zhu and Ammar [11] addressed the online problem by calculating the complete mapping of virtual networkperiodically. An algorithm to optimize the mapping of virtual network to physical network of specific topologies was also provided. Quite a few of the aforementioned algorithms considered admission control as an integral part of the solution.

Distinct topologies and possible opportunities to exploit them open up new research in this area that is computationally difficult to solve because of various constraints. Cheng et al. [16] have formulated a Markov random walk model to

compute the topology-aware resource ranking of nodes in a substrate network for a topology aware virtual network mapping. However, in [17] it is observed that only one walk is considered from a substrate node to itself or one of its neighbors because the impact is recursive in a Markov chain.

Resource Scheduling
A service provider requires specific guarantees from the infrastructure providers to support the attributes of the virtual routers as well as bandwidth allocated to the virtual links at the time of establishment of virtual network. For virtual routers, a service provider may request for a minimum packet processing rate of the CPU, specific disk requirements, and a lower bound on the size of the memory. For virtual links, their requests may range from best-effort service to fixed loss and delay characteristics found in dedicated physical links. Thus, to create an illusion of an isolated and a dedicated network to each SP and to offer such guarantees, Infrastructure Providers must employ appropriate scheduling algorithms in all of the network elements.

Efficient resource scheduling mechanisms become more important when resources are dynamically distributed to increase the utilization of resources as well as the revenue of the infrastructure providers. Such a dynamic allocation framework was presented in [18] where each network link of substrate periodically reassigns the bandwidth shared between the virtual links.

The existing system virtualization technology provides scheduling mechanisms for CPU, memory, disk, and network interface in each of the VMs running on the host machine. Network virtualization makes use of these mechanisms to implement resource scheduling in the physical infrastructure. An example of a resource scheduler is vSuit [19] which is proposed to improve the network performances. This new scheduler could monitor hardware usage periodically and adjust the resource allocation for each virtual machine in the next period.

Discovery of Topology
To allocate resources based on the service providers' requests, Infrastructure Providers must be able to determine the topology of the networks that they manage i.e. the physical nodes and their interconnections. It is also possible that two adjacent Infrastructure Providers must establish links between their networks to enable cross-domain virtual network instantiation.

In UCLP [20] a combination of event-based and periodic topology discovery is promoted using an additional topology database [21]. Here the topology database of an infrastructure provider is updated by the events.

Virtual Nodes/Routers
One of the primary issues in network virtualization is the virtualization of nodes that constitute the underlying physical network. Virtual routers allow multiple service providers to share same set of physical resources and implement protocols on them. Programmability techniques can be extended to create substrate routers that will allow each service provider to customize their virtual routers. A conceptual architecture of such substrate routers is given in [22].

The performance of these virtual routers on existing virtual machines has to be explored. Moreover, we need to investigate how the various virtualization techniques (such as full virtualization or para-virtualization) affect the performance. The scalability of the physical routers, used by the infrastructure providers, affects the scalability of the network virtualization environment

Migration of virtual routers is an effective solution [23] for handling of network failures and simplifies network manageability. Though, the destinations for these migrating virtual routers are restricted because of some physical constraints such as link capacity, platform compatibility issues, change of latency and sometimes the capabilities of destination physical routers. Dealing with all these aforementioned issues remains an open research challenge.

Virtual Links
Link virtualization is an important aspect in the implementation of virtual networks. Various protocols used for Virtual Private Network (VPNs) can be used for virtual networks too. The creation of an inter-infrastructure provider tunnel is a challenging task as it requires collaboration among multiple infrastructure providers.

The speed of network links plays an important role in packet transmission. The overhead for transporting packets across a virtual link must be minimal as compared to a native link resulting in minimal multiplexing cost and encapsulation. Optical fibers, a faster means of communication, can play an important role as it can be divided into smaller paths and the need of multiplexing or encapsulating packets from different virtual networks gets over by using these optical fibers. Further, virtual links must also be flexible enough to carry packets of any protocol. A protocol Virtual Link Setup Protocol (VLSP) is proposed in [24] that creates a platform for on-demand setup of virtual links with the establishment of

Quality-of-Service (QoS) guaranteed in the underlying substrate. This QoS and signaling performance is maintained by virtualization techniques and tunneling mechanisms.

Naming and Addressing

Due to heterogeneity of the coexisting networks, end-to-end communication and universal connectivity in the Network Virtualization Environment (NVE) becomes a major challenge. It is hard to use the Domain Name System (DNS) in today's Internet, with a network virtualization environment because of scalability, addressing and administrative issues. Mapping between different address contexts is a well known problem, and in the presence of different addressing requirements in different VNs, it becomes even more difficult.

Unlike the existing Internet architecture, where IP addresses carry locations as well as identifications, naming and addressing should be decoupled in the network virtualization environment. It is the decoupling of information that is needed so that any end user can move from one SP to another with a single identity. This problem is similar at a higher level to the problem of people using ISP provided email addresses, who discover that they have to get new email addresses as soon as they change their ISPs.

In NVE, any end user can simultaneously connect to multiple virtual networks through multiple infrastructure providers using heterogeneous technologies to access different services.
iMark[25] is an identity management framework for the network virtualization environment that separates the identities of the end hosts from their physical and logical locations, and with the help of a global identifier space provides universal connectivity without affecting the independence of the underlying physical and virtual networks.

Mobility and Dynamism in NVE

Network virtualization introduces a dynamic environment at all levels of networking, which starts from individual end users or network elements and continues up to the level of complete virtual networks. Such dynamism can broadly be classified into two classes:

1. Macro Level Dynamism

Virtual Networks that provide basic services and virtual networks with shared interests can be dynamically aggregated together to form compound virtual networks, also termed federation of virtual networks. Multiple federations and virtual networks can also come together to create a hierarchy of virtual networks.

2. Micro Level Dynamism

This is more influential than the macro level dynamism and requires more attention. Micro level dynamic behavior can be seen through two broad sets of activities:

- Dynamic join, leave, and mobility of end users within and in between virtual networks, and
- Dynamism introduced by the migration of virtual routers for different purposes [23]

To find the exact location of any resource at a particular moment and then routing packets is also a complex research problem that needs to be investigated. Xiao Ling Li et al. [26] gave a resource finding mechanism for Network Virtualization Environment (NVE) that helps users to find the optimal resource and also improves the efficiency of the overall virtual network.

Virtual Network Management and Operations

The management and operations of the networks have always been a great challenge for the network operators. Division of accountability and responsibilities among different participants in the network virtualization environment increases manageability, and reduces the scope for errors. Although, this requires a complete re-design of the existing network management architecture. Flexibility must be introduced from the level of network operations centers to intelligent agents at network elements, to enable individual service providers to configure, monitor, and control their virtual networks regardless of other participants of network virtualization environment. The concept of MIBlets [27], (i.e., partitioned Management Information Bases (MIBs)), to collect and process performance statistics for each of the coexisting virtual networks instead of using a common MIB can be used to start with.

Failure Handling and Event Notification

Failures in the underlying physical networks can cause problems in the network virtualization environment. Any such failure can cause a series of errors in the virtual networks on directly hosted components and in many others that are recursively generated from the affected ones. For example, a physical link will result in failures of all the virtual links that pass through it. In the same way, any physical node failure might require re-installations of all the SPs software. Detection, prevention, isolation of such failures are all open research issues.

Enabling Virtualization across Heterogeneous Networks
Each networking technology has its unique characteristics. Virtualization of networks on each of these technologies faces challenges that require specific solutions for operation and maintenance. For example, Virtual Sensor Networks (VSN) [28] deal with providing protocol support for the setting up, usage and maintenance of subsets of sensors that works together on specific tasks. Dynamic leaving and joining behavior of sensors and power constraints impose different challenges for virtual sensor networks that do not occur in optical networks. Similarly, virtualization of wireless networks using different multiplexing techniques creates different issues such as, node synchronization and managing device states [29].

End-to-end virtual networks cover multiple domains running over completely different type of network. The interaction between different infrastructures and the ability to provide a transparent interface for SPs to manage virtual networks is still a daunting task.

Inter Virtual Network Communication
Even though one of the main inspirations behind network virtualization is the isolation between co-existing virtual networks, there are cases when two virtual networks need to share resources or information. For example, a large multinational company may deploy a virtual network across the globe with child virtual networks for each of the continents to manage its operations. In this case, child virtual networks will need to communicate with the global one and also among themselves. There may be cases where communicating virtual networks might not be under the same administrative domain, (i.e. being managed by different service providers). Thus, attention needs to be paid on the necessity, scope and interface for such interconnections among service providers and corresponding virtual networks in future research works.

Network Virtualization Economics
In traditional networks, bandwidth is of high interest. But in the network virtualization environment virtual nodes are also very important entities along with the virtual links. Service providers are the buyers in this economy and infrastructure providers are the sellers. It is also possible that there may be brokers who will act as mediators between the buyers and the sellers. End users act as buyers of services from different service providers.

Traditionally, there are two types of marketplaces: centralized and decentralized. Centralized marketplaces are efficient; but prone to attacks, and are also not scalable. In contrast, fully decentralized marketplaces are extensible and fault-tolerant; but are also prone to nasty behavior and inefficiency. PeerMart [30], which combines both efficiency and scalability, is a semi-decentralized double-auction based marketplace for peer-to-peer systems. The same idea can also be developed for the network virtualization environment.

Security and Privacy
There are various attack vectors to network virtualization such as Hyperjacking, Virtual Machine jumping, Virtual Machines and Network Security, Compliance, Update etc. The solutions to thwart these attacks are Verified Launch and Secure Root of Trust, Segmentation and Hardening of Virtual Machines and so on. Security and privacy may be provided in virtual networks through isolation by using encryption, secured tunnels etc. It does not eliminate the prevalent threats and attacks to the physical layer and virtual networks. In addition, security and privacy issues specific to network virtualization must also be explored. For example, if secure programming models and interfaces are not available programmability of network elements may increase vulnerability. A good security evaluation process of the virtual network topology is described in [31].

Availability
Many networks are sensitive to jitter or latency, the examples of which can be networks supporting streaming media, voice, or critical apps (e.g., financial and medical), where the presence of QoS support (Layer 2/Layer 3) can be useful. In such environments, Network Virtualization solutions based on direct-fabric programming may be able to provide better QoS control than pure overlay solutions.

CONCLUSION

In today's Cyberworld, network virtualization has become an increasingly important technology with tremendous potential. For the future Internet design, it is a powerful tool that can bring numerous benefits for the enterprises. It is also an essential component for the emerging Cloud computing environment.

The paper has highlighted several research issues of network virtualization including: implementation, deployment, and design goals such as manageability, scalability, reliability, isolation, security, etc. We also identified and discuss the open problems with network virtualization that are being addressed by the research community and require more attention in the future.

REFERENCES

[1] MayEl Barachi, Nadjia Kara, and RachidaDssouli, "Towards a Service-Oriented Network Virtualization Architecture," Innovations for Future Networks and Services, 2010, pp. 1-7

[2] http://www.ibm.com/developerworks/cloud/library/hypervisorcompare/index.html?ca=drs

[3] Framework of network virtualization for Future Networks. Response to report of the 6th FGNGN meeting, pp. 6-17

[4] M. Boucadair , P. Georgatsos ,N. Wang , D. Griffin ,G. Pavlou , M. Howarth& A. Elizondo, "The AGAVE approach for network virtualization: differentiated services delivery," Ann. Telecommun.,2009, pp. 277–288

[5] N. Feamster, L. Gao, and J. Rexford, "How to lease the internet in your spare time," SIGCOMM Computer Communication Review, vol. 37, no. 1, 2007,pp. 61-64,

[6] Hugo Corbucci, Alfredo Goldman, Eduardo Katayama,FabioKon, Claudia Melo and Viviane Santos , "Genesis and Evolution of the Agile Movement in Brazil – Perspective from Academia and Industry" 25th Brazilian Symposium on Software Engineering, 2011, pp. 598-107.

[7] J. E. van der Merwe, S. Rooney, I. Leslie, and S. Crosby, "The Tempest-A practical framework for network programmability," IEEE Network Magazine, vol. 12, no. 3, pp. 20-28, 1998.

[8] B. Raghavan, K. Vishwanath, S. Ramabhadran, K. Yocum, and A. C. Snoeren, "Cloud control with distributed rate limiting," in Proceedings of SIGCOMM'07, 2007, pp. 337-348.

[9] Mika Mori, Takuji Tachibana, Kentaro Hirata, and Kenji Sugimoto, "A Proposed Topology Design and Admission Control Approach for Improved Network Robustness in Network Virtualization," in Proceedings of Global Telecommunications Conference (GLOBECOM 2011), 2011, pp. 1-5.

[10]D.Andersen, "Theoretical approaches to node assignment," Unpublished Manuscript,http://www.cs.cmu.edu/_dga/papers/andersen-assign.ps, 2002.

[11]Y. Zhu and M. Ammar, "Algorithms for assigning substrate network resources to virtual network components," in Proceedings of the IEEE INFOCOM'06, 2006.

[12] J. Lu and J. Turner, "Efficient mapping of virtual networks onto a shared substrate," Washington University, Tech. Rep. WUCSE-2006-35, 2006.

[13] W. Szeto, Y. Iraqi, and R. Boutaba, "A multi-commodity flow based approach to virtual network resource allocation," in Proceedings of the IEEE Global Telecommunications Conference (GLOBE- COM'03), 2003, pp. 3004-3008.

[14] A. Gupta, J. M. Kleinberg, A. Kumar, R. Rastogi, and B. Yener, "Provisioning a virtual private network: A network design problem for multicommodity flow," in ACM Symposium on Theory of Computing, 2001, pp. 389-398.

[15] J. Fan and M. Ammar, "Dynamic topology configuration in service overlay networks – a study of reconfiguration policies," in Proceedings of the IEEE INFOCOM'06, 2006.

[16] X.Cheng, S.Su, Z.Zhang, H.Wang, F.Yang, Y.Luo, and J.Wang, "Virtual network embedding through topology-aware node ranking," SIGCOMM Comput. Commun. Rev., vol-41, April 2011, pp. 38-47

[17] Sheng Zhang, Zhuzhong Qian, Jie Wu, and Sanglu Lu, "An Opportunistic Resource Sharing and Topology-Aware Mapping Framework for Virtual Networks," in Proceedings of the IEEE INFOCOM'12, 2012, pp. 2408 - 2416

[18] J. He, R. Zhang-Shen, Y. Li, C.-Y. Lee, J. Rexford, and M. Chiang, "Davinci: Dynamically adaptive virtual networks for a customized internet," in ACM CoNEXT, 2008.

[19] Feng Dan, Wang Xiaojing, Zhao Wei, Tong Wei and Liu Jingning, "vSuit: QoS-oriented scheduler in Netowrk Virtualization," in 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2012, pp. 423 - 428

[20] Univ. of Waterloo, "User controlled lightpathsproject,"http://uclp.uwaterloo.ca/.

[21] J. Recio, E. Grasa, S. Figuerola, and G. Junyent, "Evolution of the user controlled lightpath provisioning system," in Proceedings of 7th International Conference on Transparent Optical Networks, vol. 1, July 2005, pp. 263-266.

[22] J. Turner and D. Taylor, "Diversifying the internet," in Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM'05), vol. 2, 2005.

[23] Y. Wang, E. Keller, B. Biskeborn, J. van der Merwe, and J. Rexford, "Virtual routers on the move: Live router migration as a network-management primitive," in Proceedings of the ACM SIGCOMM'08, 2008, pp. 231-242.

[24] Roland Bless, Martin Rohricht and ChristophWerle, "Authenticated Setup of Virtual Links with Quality-of-Service Guarantees," in Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), 2011, pp. 1-8.

[25] M. K. Chowdhury, F. Zaheer, and R. Boutaba, "iMark: An identity management framework for network virtualization environment," in the 11th IFIP/IEEE International Symposium on Integrated Network Management (IM), 2009.

[26] Xiao Ling Li, Huai Min Wang, Chang GuoGuo, Bo Ding and Xiao Yong Li, "A Resource Finding Mechanism for Network Virtualization Environment," Advanced Materials Research, vols. 433-440, 2012, pp. 5078-5086.

[27] W. Ng, D. Jun, H. Chow, R. Boutaba, and A. Leon-Garcia, "Miblets: A practical approach to virtual network management," in Proceedings of the Sixth IFIP/IEEE International Symposium on Integrated Network Management (IM'99), 1999, pp. 201-215.

[28] A. P. Jayasumana, Q. Han, and T. H. Illangasekare, "Virtual sensor networks - a resource efficient approach for concurrent applications," in Proceedings of the International Conference on Information Technology (ITNG'07). Washington, DC, USA: IEEE Computer Society, 2007, pp. 111-115.

[29] G. Smith, A. Chaturvedi, A. Mishra, and S. Banerjee, "Wireless virtualization on commodity 802.11 hardware," in Proceedings of the the 2nd ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WinTECH'07). New York, USA: ACM, 2007, pp. 75-82.

[30]"PeerMart: Decentralized auctions for bandwidth trading on demand," http://ercimnews.ercim.org/content/view/100/254/, January 2007.

[31] R. Goyette and A. Karmouch, "A Virtual Network Topology Security Assessment Process," 7th International Conference on Wireless Communications and Mobile Computing (IWCMC), 2011, pp. 974-979.

