International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2017, pp. 622-628
e-ISSN:2278-621X

A COMPREHENSIVE INVESTIGATION OF NETWORK VIRTUALIZATION

AthokpamBikramjit Singh[1], SathyendraBhat J[2], RageshRaju[3] & Prithvi V Shet[4]

Abstract-Due to the existence of multiple stakeholders with conflicting goals and policies, alterations to the existing Internet architecture are now limited to simple incremental updates; deployment of any new, radically different technology is next to impossible. To fend off this ossification, network virtualization has been propounded as a diversifying attribute of the future inter-networking paradigm. By introducing a plurality of heterogeneous network architectures cohabiting on a shared physical substrate, network virtualization promotes innovations and diversified applications. In this paper, we survey the existing technologies and a wide array of past and state-of-the-art projects on network virtualization followed by a discussion of major challenges in this area.
Keywords-Network, Virtualization

1. INTRODUCTION

The Internet has been stunningly successful over the course of past three decades in supporting multitude of distributed applications and a wide variety of network technologies. However, its popularity has become the biggest impediment to its further growth. Due to its multi-provider nature, adopting a new architecture or modification of the existing one requires consensus among competing stakeholders. As a result, alterations to the Internet architecture have become restricted to simple incremental updates and deployment of new network technologies have become increasingly difficult [1,2]. To fend off this ossification, network virtualization has been propounded as a diversifying attribute of the future inter-networking paradigm. Even though architectural purists view network virtualization as a means for evaluating new architectures, the pluralist approach considers virtualization as a fundamental attribute of the architecture itself [1]. They believe that network virtualization can eradicate the ossifying forces of the Internet and stimulate innovation [1,2].

1.1 What is Network Virtualization?

A networking environment supports network virtualization if it allows coexistence of multiple virtual networks on the same physical substrate. Specifically, network virtualization is a networking environment that allows multiple service providers to dynamically compose multiple heterogeneous virtual networks that coexist together in isolation from each other. Service providers can deploy and manage customized end-to-end services on those virtual networks for the end users by effectively sharing and utilizing underlying network resources leased from multiple infrastructure providers [4].

2. TECHNOLOGIES

The concept of multiple coexisting networks appeared in the networking literature in different capacities. In this section, we discuss four such incarnations: Virtual Local Area Networks (VLAN), and Virtual Private Networks (VPN).

2.1 Virtual Local Area Network

A Virtual Local Area Network (VLAN) [5] is a group of hosts with a common interest that are logically brought together under a single broadcast domain regardless of their physical connectivity. Since VLANs are logical entities, i.e., configured in software, they are flexible in terms of network administration, management, and reconfiguration. Moreover, VLANs provide elevated levels of trust, security, and isolation, and they are cost-effective.

2.2 Virtual Private Network

A Virtual Private Network (VPN) [6–8] is a dedicated communications network of one or more enterprises that are distributed over multiple sites and connected through tunnels over public communication networks (e.g., the Internet). Each VPN site contains one or more Customer Edge (CE) devices (e.g., hosts or routers), which are attached to one or more Provider Edge (PE) routers. Normally a VPN is managed and provisioned by a VPN Service Provider (SP) and known as Provider-Provisioned VPN (PPVPN) [9].

[1] Department of Computer Applications, St Joseph Engineering Computer ApplicationsCollege, Mangaluru, Karnataka, India
[2] Department of Computer Applications, St Joseph Engineering College, Mangaluru, Karnataka, India
[3] Department of Computer Applications, St Joseph Engineering College, Mangaluru, Karnataka, India
[4] Department of Computer Applications, St Joseph Engineering College, Mangaluru, Karnataka, India

3. LAYER OF VIRTUALIZATION

3.1 Physical Layer: UCLP

UCLP is a distributed network control and management system for CA*NET 4 network that allows end users to treat network resources as software objects, and lets them provision as well as dynamically reconfigure optical networks (at Layer 1). Users are able to join or divide light paths within a single domain, or across multiple independent management domains to create customized logical IP networks. UCLP takes a modular approach to resource management by introducing three distinct service layers. Customers and administrators configure and use end-to-end UCLP resources through the user access layer. The service provisioning layer manages service logic and data regarding light paths. Finally, the resource management layer deals with actual physical resources. UCLPv1.4 [11] introduced dynamic topology discovery process and enabled auto-routing through intelligent algorithms alongside already available manual light path configuration capabilities. Later, UCLPv2 [12,13] extended UCLP with the use of Service Oriented Architecture (SOA) and workflow technologies with an aim to form the underpinning architectural framework for extending UCLP to allow the interconnection of instruments, time slices, and sensors; and for incorporating virtual routers and switches.

3.2 Link Layer: VNET

VNET [14] is a Layer 2 overlay network for Virtual Machines (VMs) that implement a Virtual LAN (VLAN) spread over a wide area using Layer 2 Tunnelling Protocol (L2TP). Each physical machine hosting a virtual machine (VM) runs a VNET process that intercepts VM traffic and tunnels it to the appropriate destination. The destination is either another VM that can be contacted directly through VNET or an address external to the overlay. Traffic destined for an external address is routed through the overlay to a VNET proxy node, which is responsible for injecting the packets onto the appropriate network. The overlay thus consists of a set of TCP connections or UDP peers (VNET links) and a set of rules (VNET routes) to control routing on the overlay. Since VNET operates at Layer 2, it is agnostic to Layer 3. As a result, protocols other than IP can be used. In addition, VNET also supports migration of a VM from one machine to another without any participation from the VM's OS and all connections remain open after migration.

3.3 Network Layer: AGAVE

The main objective of the AGAVE [15-17] project is to provide end-to-end QoS-aware service provisioning over IP networks following the theme of QoS forwarding mechanisms such as IntServ [18] and DiffServ [19,20]. To achieve this, AGAVE proposes a new inter-domain architecture based on the novel concept of Network Planes (NPs), which allows multiple IP Network Providers (INPs) to build and provide Parallel Internets (PIs) tailored to end-to-end service requirements. NPs are internal to INPs and are created based on the service requirements described by the SPs. An NP can be engineered for routing, forwarding, or resource management. To enable end-to-end services over multi-provider environment, NPs from different INPs are connected together to form PIs based on inter-INP agreements. One of the interesting features of AGAVE is that it does not require all the NPs participating in a PI to be homogeneous resulting in greater flexibility. AGAVE replaces node-centric provisioning/configuration approach in favour of a more centralized network based configuration, which ensures configuration consistency between participating INPs and reduces configuration errors. Also, it supports an NP emulation function that assesses the status of the network and evaluates the impact of introducing new NPs before accepting new IP-connectivity provisioning requests.

4. CHARACTERISTIC COMPARISON OF VARIOUS NETWORK VIRTUALIZATION PROJECTS

Project	Influences of existing concepts	Architectural domain	Networking technology	Layer of virtualization	Granularity of virtualization
VNRMS	Programmable networks, VPN	Virtual network management	ATM/IP		Node/link
Tempest	Programmable networks	Enabling alternate control architectures	ATM	Link	
NetScript	Active networks	Dynamic composition of services	IP	Network	Node
Genesis	Programmable networks	Spawning virtual network architectures		Network	Node/link
VNET	VLAN, L2VPN	Virtual machine grid computing		Link	Node
VIOLIN	L2VPN, overlays	Deploying on-demand value-added services on IP overlays	IP	Application	Node
X-Bone	L3VPN, overlays	Automating deployment of IP overlays	IP	Network	Node/link
PlanetLab	Overlays	Deployment and management of overlay-based testbeds	IP	Application	Node
UCLP	L1VPN, SOA	Dynamic provisioning and reconfiguration of lightpaths	SONET	Physical	Link
AGAVE	IntServ, DiffServ, VPN, overlays	End-to-end QoS-aware service provisioning	IP	Network	
GENI	VPN, active and programmable networks, overlays	Creating customized virtual network testbeds	Heterogeneous		
VINI	VPN, overlays	Evaluating protocols and services in a realistic environment		Link	
CABO	DiffServ, VPN, active and programmable networks, overlays	Deploying value-added end-to-end services on shared infrastructure	Heterogeneous		Full
4WARD	Overlays, SOA, autonomic networks	Instantiation,deployment, and management of virtual networks in a commercial setting	Heterogeneous	Network	Full
NouVeau	DiffServ, overlays, active and programmable networks, VPN, autonomic networks	Deploying end-to-end virtual networks on shared infrastructure	Heterogeneous		Full
FEDERICA	SOA, IaaS, VPN	Experimental facility with reproducibility	Heterogeneous	Link	Node/link

Figure 1. Comparison of Network Virtualozation Projects

5. KEY RESEARCH DIRECTIONS

5.1 Interfacing

Service providers synthesize physical resources from one or more infrastructure providers to create virtual networks. Infrastructure providers must provide well-defined interfaces to allow service providers to communicate and express their requirements. For interoperability, such interfaces should follow a standard that should be able to express virtual network requests in terms of virtual nodes and virtual links along with their corresponding attributes. An XML-based specification language can be a possible candidate in this respect. Appropriate interfaces between end users and service providers, between infrastructure providers, and between multiple service providers must also be identified and standardized.

5.2 Signalling and Bootstrapping

Before creating a virtual network, a service provider must already have network connectivity to one or more infrastructure providers in order to issue its requests. This introduces circularity where network connectivity is a prerequisite to itself [3]. As long as a network virtualization environment is not mature enough to support itself, signalling must be handled through out-of-band communication mechanisms (e.g., the current Internet). Bootstrapping capabilities are required to allow service providers to customize the virtual resources allocated to them. Standard methods to make programmability of the network elements available to the service providers must also be developed [28]. Both signalling and bootstrapping call for at least another network that will always be present to provide connectivity to handle these issues.

5.3 Resource Allocation

Resource allocation in a network virtualization environment refers to static or dynamic allocation of virtual nodes and links on physical nodes and paths, respectively. It is also known as the virtual network embedding problem in the existing literature. Embedding of virtual networks with constraints on nodes and links can be reduced to the NP-hard multi-way separator problem [29] even when all virtual network requests are known in advance. In order to provide efficient heuristics, Internet

clean-slate design: what and why?, SIGCOMM Computer Communication Review 37 (3) (2007) 59–64 New Generation Network Architecture: AKARI Conceptual Design (ver1.1) (June 2008).s been restricting the problem space in different dimensions, which include: (i) considering offline version of the problem (i.e., all the requests are known in advance) [30–32], (ii) ignoring either node requirements or link requirements [33,30], (iii) assuming infinite capacity of the substrate nodes and links to obviate admission control [33,30,31], and (iv) focusing on specific topologies [30]. Yu et al. [34] addressed these issues by envisioning support from the substrate network through node and link migration as well as multi-path routing. Chowdhury et al. [27] proposed embedding algorithms based on the mathematical formulation of the embedding problem that outperform the previous algorithms in terms of acceptance ratio and total revenue. Unlike others following a centralized approach, Houidi et al. [35] proposed a distributed embedding algorithm but could not achieve competitive performance. All of these algorithms perform static resource allocation.

5.4 Resource Discovery

In order to allocate resources for requests from different service providers, infrastructure providers must be able to determine the topology of the networks they manage as well as the status of the corresponding network elements (i.e., physical nodes and interconnections between them) [3]. Furthermore, adjacent infrastructure providers must also share reachability information to be able to establish links between their networks to enable inter-domain virtual network instantiation. UCLP promotes a combination of event-based and periodic topology discovery using an additional topology database [11]. Events update the topology database of an infrastructure provider, and a periodic refresh ensures that even if some events were not notified, the topology database is fresh. CABO argues for the use of a separate discovery plane run by the infrastructure providers as proposed in the 4D network management architecture [36]. Efficiently gathering and dissemination of such information in decision elements could be achieved via discovery techniques discussed in existing distributed computing literature (e.g., Remos [37]).

5.5 Admission Control and Usage Policing

Infrastructure providers must ensure that resources are not over-provisioned to uphold QoS guarantees. Consequently, they have to perform accurate accounting and implement admission control algorithms to ensure that resources allocated to the virtual networks do not exceed the physical capacity of the underlying network. Existing solutions perform admission control while statically embedding virtual networks [34,27]. However, they do not allow dynamic resizing of allocated resources (i.e., adding or removing virtual nodes or links, increasing or decreasing allocated capacities). In order to avoid constraint violations by globally distributed virtual networks, distributed policing mechanisms must be employed to make sure that service providers cannot overflow the amount of resources allocated to them by direct or indirect means. Raghavan et al. [97] presented such a global rate limiting algorithm coordinated across multiple sites in the context of cloud-based services in the existing Internet. Similar mechanisms need to be developed in the context of network virtualization too.

5.6 Resource Scheduling

When establishing a virtual network, a service provider requires specific guarantees for the virtualnodes' attributes as well as the virtual links' bandwidth allocated to its network [3]. For virtual routers, a service provider might request guarantees for a minimum packet processing rate of the CPU, specific disk requirements, and a lower bound on the size of the memory. On the other hand, virtual link requests may range from best-effort service to fixed loss and delay characteristics found in dedicated physical links. To provide such guarantees and to createan illusion of an isolated and dedicated network to each service provider, infrastructure providers must employ appropriate scheduling algorithms in all of the network elements. Existing system virtualization technologies provide efficient scheduling mechanisms for CPU, memory, disk, and network interface in each of the virtual machines running on the host machine [39]. Network virtualization can ex tend these mechanisms to implement resource scheduling in the physical infrastructure. Previous results from research on packet scheduling algorithms for IP networks can also be useful in the design of schedulers.

5.7 Naming and Addressing

Due to potential heterogeneity of naming and addressing schemes in coexisting virtual networks, end-to-end communication and universal connectivity is a major challenge in a network virtualization environment. In addition, end users can simultaneously connect to multiple virtual networks through multiple infrastructure providers using heterogeneous technologies to access different services, which is known as über-homing [26]. Incorporating support for such heterogeneity in multiple dimensions is a fundamental problem in the context of network virtualization. Recently proposed iMark [26] separates identities of end hosts from their physical and logical locations to add an additional level of indirection and, with the help of a global identifier space, provides universal connectivity without revoking the autonomy of concerned physical and virtual networks. However, while conceptually possible, iMark is not physically implementable due to excessive memory requirements. Therefore, one key research direction in naming and addressing is to find a viable global connectivity enabling framework.

5.8 Dynamism and Mobility Management

Network virtualization environment is highly dynamic.At macro level, virtual networks with shared interests can be dynamically aggregated together to create federation of virtual networks. Multiple federations and virtual networks can also come together to form virtual network hierarchies [26]. Aggregation and dissolution of control and data planes (e.g., naming, addressing, routing, and forwarding information) for macro level dynamism is an unresolved issue. At micro level, mobility of end users from one physical location to another and migration of virtual routers for operation and management purposes [24] poses the biggest challenge. Finding the exact location of any resource or end user at a particular moment and routing packets accordingly is a complex research challenge that needs efficient solution. In addition, network virtualization allows end users to move logically from one virtual network to another, which further complicates the problem.

5.9 Virtual Network Operations and Management

Network operations and management has always been a great challenge for the network operators. Division of accountability and responsibilities among different participators in a network virtualization environment promises increased manageability and reduced scopes for error [3]. Keller et al. [25] propose proactive and reactive mechanisms to enforce accountability for hosted virtual networks. Considerable flexibility must be introduced from the level of Network Operations Centers (NOCs) to intelligent agents at network elements, to enable individual service providers configure, monitor, and control their virtual networks irrespective of others. The concept of MIBlets [22] used in VNRMS to gather and process performance statistics for each of the coexisting virtual networks instead of using a common MIB can be a good starting point. Since a virtual network can span over multiple underlying physical networks, applications must also be developed to aggregate information from diverse, often conflicting, management paradigms followed by participating infrastructure providers. Introducing a common abstraction layer, to be followed by all the management software's, can be an effective solution [40]. Failures in the underlying physical network components can give rise to cascading failures in the virtual networks directly hosted on those components. For instance, a physical link failure will result in failures of all the virtual links that pass through it. Similarly, any physical node failure might require re-installations of all the service provider's custom software's. Detection and effective isolation of such failures as well as prevention and recuperation from them to stable states are all open research challenges.

5.10 Security and Privacy

Even though network virtualization strives for isolation of faults and attack impacts, it does not necessarily obviate existing threats, intrusions, and attacks to physical and virtual networks. In fact, to some extent, network virtualization gives rise to a new array of security vulnerabilities. For instance, a Denial-of-Service (DoS) or a Distributed DoS (DDoS) attack against the physical network in a virtualized environment will affect all the virtual networks hosted on that network. Programmability of network elements – powerful and expressive in trusted hands – can increase vulnerability if there are security holes in programming models. To avoid such pitfalls, recent proposals (e.g., CABO) argue for controlled programmability by trading off flexibility for security without any definitive answer to permissible levels access to programmable hardware. A detailed study of possible security vulnerabilities can give insights into developing programming paradigms[41] and virtualization environments that are secure and robust against known attacks. Established secured tunnelling and encryption mechanisms (e.g., IPSec [10]) in VPNs can also be used in this context to increase security and enforce privacy.

5.11 Heterogeneity of Networking Technologies

Each networking technology has its own set of unique characteristics and poses challenges that require specific solutions for provisioning, operation, and maintenance of virtual network on those platforms. For instance, UCLP virtualizes optical networks capitalizing on the property of light paths that can be physically sub-divided into smaller light paths. Virtual Sensor Networks (VSN) [42], on the other hand, deals with providing protocol support for dynamic formation, usage, adaptation, and maintenance of subsets of sensors under unique power constraints. Similarly, virtualization of wireless networks using different multiplexing techniques creates different complications, e.g., node synchronization and managing device states [43]. End-to-end network virtualization requires framework that handle interactions between such contrasting underlying infrastructures while providing a generic and transparent interface for service providers to easily compose and manage virtual networks.

6. CONCLUSION

Most researchers agree that the Internet has reached a tipping point where most of their time and effort is spent in putting band aids on its existing flaws rather than in cultivating novel ideas. To fight back this ossification, redesign of the Internet is a bare necessity [44]. Instead of creating yet another one-size-fits-all architecture, a versatile networking paradigm must be established that will be flexible enough to support multiple coexisting architectures through network virtualization [1,2]. As a result, major initiatives on next-generation networks (e.g., FIND 6 projects in the US, FIRE 7 projects in the EU, Asia Future Internet (AsiaFI 8), New Generation Network (NWGN) forum [45] in Japan, and Future Internet Forum (FIF 9) in South Korea) all around the world are promoting inclusion of network virtualization concepts in their core architectural designs. Moreover, network virtualization stands at a unique point in the current virtualization landscape as the missing link that will

interconnect all other virtualized appliances, ranging from operating systems, storage systems to servers and even large data centres, to create a complete semblance of a virtualized computing environment. In this paper, we have surveyed the past and the state of the art in network virtualization research. It is evident that even though network virtualization promises an open, flexible, and heterogeneous networking environment, it will also pose a string of challenges in terms of instantiation, operation, and management that will require coordinated attention from researchers working in networking and other related fields for its success and wide acceptance.

7. REFERENCES

[1] T. Anderson, L. Peterson, S. Shenker, J. Turner, Overcoming the Internet impasse through virtualization, Computer 38 (4) (2005) 34–41.

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

[3] N. Feamster, L. Gao, J. Rexford, How to lease the internet in your spare time, SIGCOMM Computer Communication Review 37 (1) (2007) 61–64.

[4] N.M.M.K. Chowdhury, R. Boutaba, Network virtualization: state of the art and research challenges, IEEE Communications Magazine 47 (7) (2009) 20–26

[5] L.S. Committee, IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks, IEEE Std 802.1Q-2005 (May 2006).

[6] P. Ferguson, G. Huston, What is a VPN?, Tech. Rep., Cisco Systems(1998).

[7] E. Rosen, Y. Rekhter, BGP/MPLS VPNs, RFC 2547 (March 1999).

[8] E. Rosen, Y. Rekhter, BGP/MPLS IP Virtual Private Networks (VPNs),RFC 4364 (February 2006).

[9] L. Andersson, T. Madsen, Provider Provisioned Virtual Private Network (VPN) Terminology, RFC 4026 (March 2005).

[10] S. Kent, K. Seo, Security Architecture for the Internet Protocol, RFC 4301 (December 2005).

[11] J. Recio, E. Grasa, S. Figuerola, G. Junyent, Evolution of the usercontrolled lightpath provisioning system, in: Proceedings of the Seventh International Conference on Transparent Optical Networks, vol. 1, 2005, pp. 263–266.

[12] B. Nandy, D. Bennett, I. Ahmad, S. Majumdar, B. St-Arnaud, User Controlled Lightpath Management System based on a Service Oriented Architecture (2006). <http://www.solananetworks.com/UCLP/files/UCLPv2-SOA.pdf>.

[13] E. Grasa, G. Junyent, S. Figuerola, A. Lopez, M. Savoie, Uclpv2: a network virtualization framework built on web services, IEEE Communications Magazine 46 (6) (2008) 126–134.

[14] A. Sundararaj, P. Dinda, Towards virtual networks for virtual machine grid computing, in: Proceedings of the Third USENI Virtual Machine Research and Technology Symposium (VM'04),2004, pp. 177–190.

[15] M. Boucadair, B. Decraene, M. Garcia-Osma, A.J. Elizondo, J.R. Sanchez, B. Lemoine, E. Mykoniati, P. Georgatsos, D. Griffin, J. Spencer, J. Griem, N. Wang, M. Howarth, G. Pavlou, S. Georgoulas, B. Quoitin, Parallel Internets Framework, AGAVE Deliverable (2006) (Id: AGAVE/WP1/FTRD/D1.1/public).

[16] L. Andersson, E. Rosen, Framework for Layer 2 Virtual PrivateNetworks (L2VPNs), RFC 4664 (September 2006).

[17] N. Wang, D. Griffin, J. Spencer, J. Griem, J.R. Sanchez, M. Boucadair, E. Mykoniati, B. Quoitin, M. Howarth, G. Pavlou, A.J. Elizondo, M.L.G. Osma, P. Georgatsos, A framework for lightweight QoS provisioning: network planes and parallel Internets, in: Proceedings of the 10th IFIP/IEEE International Symposium on Integrated Network Management (IM'07), 2007, pp. 797–800.

[18] R. Braden, D. Clark, S. Shenker, Integrated Services in the Internet Architecture: An Overview, RFC 1633 (Informational) (June 1994).

[19] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, An Architecture for Differentiated Services, RFC 2475 (December1998).

[20] D. Grossman, New Terminology and Clarifications for Diffserv, RFC 3260 (Informational) (April 2002).

[21] W. Ng, R. Boutaba, A. Leon-Garcia, Provision and customization of ATM virtual networks for supporting IP services, in: Proceedings of the IEEE ATM Workshop'1999, 1999, pp. 205–210.

[22] W. Ng, D. Jun, H. Chow, R. Boutaba, 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.

[23] M. Kounavis, A. Campbell, S. Chou, F. Modoux, J. Vicente, H. Zhuang, The Genesis Kernel: a programming system for spawning network architectures, IEEE Journal on Selected Areas in Communications 19(3) (2001) 511–526.

[24] Y. Wang, E. Keller, B. Biskeborn, J. van der Merwe, 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.

[25] E. Keller, R. Lee, J. Rexford, Accountability in hosted virtual networks, in: Proceedings of ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures (VISA), 2009.

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

[27] N.M.M.K. Chowdhury, M.R. Rahman, R. Boutaba, Virtual network embedding with coordinated node and link mapping, in: Proceedings of the 28th Conference on Computer Communications (INFOCOM), 2009.

[28] J. Mogul, P. Yalagandula, J. Tourrilhes, R. McGeer, S. Banerjee, T. Connors, P. Sharma, Orphal: API Design Challenges for Open Router Platforms on Proprietary Hardware, Tech. Rep. HPL-2008-108, HP Labs (2008).

[29] D. Andersen, Theoretical Approaches to Node Assignment, Unpublished Manuscript (2002).

[30] J. Lu, J. Turner, Efficient Mapping of Virtual Networks onto a Shared Substrate, Tech. Rep. WUCSE-2006-35, Washington University (2006).

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

[32] A. Gupta, J.M. Kleinberg, A. Kumar, R. Rastogi, B. Yener, Provisioning a virtual private network: a network design problem for multicommodity flow, in: ACM Symposium on Theory ofComputing, 2001, pp. 389–398.

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

[34] E.K. Lua, J. Crowcroft, M. Pias, R. Sharma, S. Lim, A survey and comparison of peer-to-peer overlay network schemes, IEEE Communications Surveys & Tutorials 7 (2) (2005) 72–93.

[35] I. Houidi, W. Louati, D. Zeghlache, A distributed virtual network mapping algorithm, in: Proceedings of IEEE ICC, 2008, pp. 5634–5640.

[36] L. Peterson, T. Anderson, D. Culler, T. Roscoe, A blueprint for introducing disruptive technology into the Internet, SIGCOMM Computer Communication Review 33 (1) (2003) 59–64.

[37] P.A. Dinda, T. Gross, R. Karrer, B. Lowekamp, N. Miller, P. Steenkiste, D. Sutherland, The architecture of the remos system, in: Proceedings of the 10th IEEE International Symposium on High Performance Distributed Computing (HPDC'01), 2001, p. 252.

[38] B. Raghavan, K. Vishwanath, S. Ramabhadran, K. Yocum, A.C. Snoeren, Cloud control with distributed rate limiting, in: Proceedings of the SIGCOMM'07, 2007, pp. 337–348. [98] D. McPherson et al., Core network design and vendor prophecies, in: NANOG 25, 2003.

[39] J.D. Touch, Y.-S. Wang, L. Eggert, G. Finn, A Virtual Internet Architecture, Tech. Rep. TR-570, USC/Information Sciences Institute (2003).

[40] N. Fujita, J.D. Touch, V. Pingali, Y.-S.Wang, A dynamic topology and routing management strategy for virtual IP networks, IEICE Transactions on Communications E89-B (9) (2006) 2375–2384.

[41] J.E. van der Merwe, S. Rooney, I. Leslie, S. Crosby, The Tempest—a practical framework for network programmability, IEEE Network Magazine 12 (3) (1998) 20–28.

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

[43] G. Smith, A. Chaturvedi, A. Mishra, S. Banerjee, Wireless virtualization on commodity 802.11 hardware, in: Proceedings of the Second ACM International Workshop on Wireless NetworkTestbeds, Experimental Evaluation and Characterization (WinTECH'07), ACM, New York, NY, USA, 2007, pp. 75–82.

[44] A. Feldmann, Internet clean-slate design: what and why?, SIGCOMM Computer Communication Review 37 (3) (2007) 59–64

[45] New Generation Network Architecture: AKARI Conceptual Design (ver1.1) (June 2008).