# Security Management in Network Visualization Environment by using modified root management algorithm for Creation of Virtual Node and Virtual Link

Navin Mani Upadhyay
Department of Computer Science and Engineering
Ashoka Institute of Technology & Management
Varanasi, Uttar Pradesh, India-221007.

Kumari Soni
Department of Computer Science and Engineering
Ashoka Institute of Technology & Management
Varanasi, Uttar Pradesh, India-221007.

Arvind Kumar
Department of Computer Science and Engineering
Ashoka Institute of Technology & Management
Varanasi, Uttar Pradesh, India-221007.

## ABSTRACT
In the present days the data on particular topic availability is huge and massive. The network virtualization plays very important role in the field of internet. Since Virtual networks have emerged as a powerful and flexible platform for the future network. The dependability of virtual services relies on the network's capabilities and capabilities include virtual nodes and links to maintain the virtualization. Due to existence of the multiple confliction policies, services and alternations to the existing internet there are some limitations occur according to the following features: robust routing, efficient search, scalability, decentralization, fault tolerances, trust and authentications; so this era needs network virtualization technique. But the difficulties with the network virtualization are Instantiation means creating virtual networks, logistics means runs them; Management means manage them, and Interactions. The creation of virtual networks is very difficult but the researchers from all over the globe will always trying to resolve it according to their way. So this is referred as future work also. The proposed algorithm in this paper is useful to create virtual node and link for network virtualization. There are already some techniques available to create the virtual network but they are not showing the exact structure which will be required. This paper introduces an algorithm to managing the virtual node and virtual link in any virtual network.

## General Terms
Virtual LANs, Virtual Private Network, Algorithm.

## Keywords
Network virtualization; Virtual networks; Virtual Node; Virtual Link; InPs; ISPs;

## 1. INTRODUCTION
Since Internet is almost ossified and there are lots of Band-Aids and makeshift solutions. So there is a need of new architecture, and it is hard to come up with a one-size-fit-all architecture because almost it is impossible to predict what future might unleash. So all the architectures created to till today are open and expandable architectures and they are the test-bed for the future networking architectures and protocols. According to the services and applications like: large scale data sharing, multimedia services, parallel accessing of USB-devices, internet etc. In different operation systems, our current internet need modifications, and this new architecture is referred as Network Virtualization or future internet.

Network virtualization environment is a collection of multiple heterogeneous Virtual Networks (VNs) from different service providers, which share the Substrate network resources. The traditional Internet Service Providers (ISPs) are decoupled into two independent entities: first one is Infrastructure Providers (InPs), who manage the physical network and Provide resources, and the second one is Service Providers (SPs), who create virtual networks by aggregating resource form multiple InPs, deploy customized protocols and offer end-to-end services [3], [4].

In these prospects the network virtualization plays a very important role. According to the features like: robust routing, efficient search, scalability, decentralization, fault tolerances, trust and authentications, performance etc. the virtualization of network is very useful. Basically network virtualization is a process to combining the two different types of resources such as hardware and software. The term Network virtualization has two distinct components which are used in two distinct aspects also, the first is virtualization of hardware on the network entities and the second one is the virtual network. The virtualization of hardware on the network is used to provide virtual server capacity onexisting hardware using some software like XEN, VMware or virtual Box.

The virtual network act as enablers by providing the addressing and routing substrates needed to implement a virtual network structure. As mentioned before, the network virtualization is defined as a decoupling the role of ISPs (The internet service providers) into two distinct entities as: Infrastructure provider and Service providers.

The infrastructure provider manages the physical infrastructure whereas the service providers create the virtual network by aggregating the resources from multiple network virtualizations have been done on three major principles: Co-existence, Recursion and Inheritance. Up to now the concept of network virtualization has been explored essentially in test-beds, on a limited scale. Several proposals for network virtualization architecture or for the utilization of network virtualization in several contexts have been put forward [6], [7], [8], [13]. The similar ideas are VLANs, VPNs, active programmable networks, and overlay networks. The main benefits of the network virtualization are it provides privacy,

security, independent set of policies which increases the service level and the routing decisions.

*VLANs*-VLANs are group of logically networked hosts with a single broadcast domain regardless of their physical connectivity. They have a VLAN ID in the MAC header. Generally VLAN enabled switches use for both destination MAC address and VLAN ID to forward the frames to the destination station.

*VPNs*-A dedicated network connecting to multiple sites using private and secured tunnels over shared or public communication networks like Internet. VPNs fulfill the basic goal of providing different logical networks over a shared infrastructure, but suffer from a few limitations, among others like all virtual networks are based on the same technology and protocols. A real isolation of virtual network resource is not possible and A clean separation of the roles of infrastructure provider and VPN service provider is not possible and in practice they are played by the same entity [9]. Some types of VPN are Layer 2VPN Layer 1 VPN L3VPN. Layer 2 VPN: works at transport layer (typically Ethernet frames between participating sites. The advantage is that it is a gnostic about the higher-level protocols and consequently, more exiles than L3 VPN. On the downside, there is no control plane to manage reachability a cross the VPN [10]. There are two different kind of layer2 VPNs services that a SP (service provider could offer to a customer. Virtual private wired services and virtual private LAN services. Virtual private wired services are layer2 point-to-point services. A virtual private LAN also a Point to multipoint Layer service that emulates LAN services across a WAN. There is also the possibility of IP-only LAN-like services (IPLS).

*Layer1 VPN*: these are emerged in recent years from the need to extend Layer2 or Layer3 packet-switching VPN concepts to advantaged circuit-switching domains. It provides a multi-service backbone where customers can offer their own services, whose payloads can be of any layer (for example: ATM, IP, and TDMs). This ensures that each of the service networks has independent address space, independent Layer1 resource view, separate policies, and complete isolation from other VPNs. Layer 1 VPN can be of two types: Virtual private Wire Services (VPWS) and Virtual Private LAN Services (VPLS). The Virtual private wire services are point-to-pint, while VPLS can be point-to-multipoint. One another similar conceded model is Active and programmable Networks: these are motivated by the need to create, deploy, and manage novel services on the yet response to user demands. Bu the ideas never materialized to real implementations due to concerns about technical feasibility and economic viability as well as lack of willingness from network operators. Two separate schools of thought emerged on how to actually implement such concepts: one form telecommunications community and the other from IP networks community.

The paper is organized in such a way that any-body (nave users) can easily understood and take use it as there research work. So Reminder section will be set as follows. Section 2 provides a generalized introduction to the network virtualization architecture. The present design goals behind the network virtualization are described in Section 3. Section 4 describes the problems occurred in network virtualization while designing of the protocols and a high-level overview of security section followed by a detailed specification of the basic attack and operations. Similarly section 5 discusses about related work with some general example. Section 6 presents experimental results from initial evaluation. Section 7 summarizes the whole work, as conclusion.

## 2. VIRTUAL ARCHITECTURE

Network Virtualization goes some step further by enabling independent programmability of virtual network. Virtual architecture is generally design on the basis of user level, transport level, and according to the services. Generally there are two types of network virtualization environment model. These are programmable network virtualization environment and business model for network virtualization.The Entities of a network virtualization environment are Service Provider: Actually has already discussed in the previous section it manages one or more Virtual Networks by aggregation virtual resources from multiple $InP_S$ and provide deployed services to end users based on specific agreements. The second one is virtual Network: If any of the Virtual network is instantiated and managed by a single service provider. The virtual network has finite time span associated with it and is dissolved after that period. Third one is Virtual Resources: In this entity any end user connected his device to a particular virtual network which is logically considered to be in a virtual resource of the network. Fourth one is Infrastructure Provider or Physical Network which have been already discussed in this paper as it has one-to-one relationships with the physical network resource. For that reason only it will be considered as a single entity. Fifth one is physical Resource: Actually these are the hardware component which is helpful to create the virtual network resource as logical function according to working of hardware. The last entity of any network virtualization is End users: the users the network to connect to Virtual networks provided by different Service Providers managed by the Infrastructure Providers. The services ensure that the network is secured or not. Actually some attacks like Distributed Denial of Services (DDoS / DOS) attack will affect all the virtual networks hosted on those networks. It is centralized, decentralized and one another type is semi-decentralized which is categorized by the hasher and stiller. The centralized is efficient but vulnerable against attacks and attacks and not scalable. Whereas the decentralized extensible fault tolerant but prone to malicious behavior and in efficiency. This third type of the service policy is double auction based called semi-decentralized; all are focuses on the virtual links. The open challenge is to leaving virtual nodes to the economic model. Before designing the network virtualization some of the principles are required to be added into the networking paradigm: coexistence of multiple heterogeneous Virtual Networks to introduce diversity; virtual resources to enable reselling, inheritance of architectural attributes to promote value-addition; and finally, re-visitation to simplify network operations and management. Co-existence: Coexistence of multiple Virtual Networks is defined as the characteristic of the network virtual environment [12],[11]. This refers as several virtual networks from different service providers co-exist together over the part of fully of the existing physical network provided by the infrastructure providers. Fig. 3 shows the example to tow co-existing Virtual Networks.Recursion: When one or more Virtual networks are spawned form another Virtual network hierarchy with parent-child relationships, it is known as recursion as well as nesting of virtual networks [11]. The Re-visitation allows a physical node to host multiple virtual node of a single virtual network. It can also be useful for creating test-bet networks shown in fig. 2. Use of several logical routers to handle divers' functionalities in a large complex network allows a service provider to connect it logically. To design a virtual network the following principle will be required:

First one is Concurrency of multiple heterogeneous virtual networks which introduces the diversity of the networks.

Second Recursion of virtual network opens the door for network virtualization economics. Third Inheritance of architectural attributes which promotes the value-addition of the node with their corresponding virtual link. And the fourth one is Re-visitation of virtual nodes which simplify the network operation and management. In the Fig. 2 there are two virtual networks corresponding to a single physical infrastructure ($InP_S$) which shows the physical link. According to the physical link of the physical infrastructure the parent virtual network and the child virtual network will be created, here the main thing which is important is the adjacent node of the virtual network corresponding to the physical node of the physical infrastructure are totally individuals (not overlapped) one recursion will be there in between the parent virtual network and the child virtual network.

## 3. DESIGNING GOALS

As per the above discussion it is clear that, Network Virtualization is composed of two main components as Link Virtualization and Node Virtualization. By Link Virtualization our transportation of data will be distributed among multiple separate virtual links over a shared physical link. Node virtualization is generally depends on isolation with partitioning of hardware resources. Virtualization of substrate nodes and virtualization of links are interconnecting all the substrate nodes, which enables the creation of virtual network which is logically equivalent to a physical network. Form the functional point of view, there are four types of substrate nodes according to their functionality. First one is Core Capable Node which hosts the virtual nodes and also supports the non-virtual traffic. Second one is Core Transport Node which is responsible for transport traffic. Third one is Edge nodes which are connected to end users, either directly or through an access point network provider, which may be virtualizes itself. So while designing the virtual network some important point that one have to keep in their mind are flexibilities which is actually service providers can choose according to the arbitrary network topology, routing and forwarding functionalities, customized control and data planes. Manageability gives the clear separation of policy from mechanism which promotes the services of the network virtualization [1]. The manageability also defines the accountability of infrastructure and services providers (ISPs and IPs).

The scalability which maximizes the number of co-existing virtual networks which increases the resource utilization and amortize CAPEX (Capital Expenditure) and OPEX (Operational Expenditure) [1],[2]. The Heterogeneity of the network virtualization defines the networking technologies as optical networks, sensor networks, wireless networks, virtual networks etc. it also gives the development facilities to deploy services in real world from the testing phases. The programmability of the network virtualization makes a good relationship between the different network elements like routers, switch etc. [1], [2]. It also make the devices more secure, private and isolated which complete the isolation between virtual networks according to the logical ability of the administrator and the resources available. The isolation makes it free from the faults, bugs and miss-configurations. The virtualization Environment model opposed to a single role: Internet Service Provider (ISPs) in the conventional model. The Infrastructure provider actually manages existing physical network resources and these resources are nothing but the programmable interfaces to different service providers. The service providers deploy existing virtual resources to offer end-to-end services to end users. They have authority to creating child Virtual Networks by partitioning its resources to other service providers.

## 4. DIFFICULTIES WITH NETWORK VIRTUALIZATION

The creation of virtual networks if very difficult and this is referred as future work. Many of researchers from all over world are working on this advance topic, the major problem is according to virtual link and node the network node existing in any network virtualization are simply the logical functions which acts as real routers/switches etc. Since it is very recent but vast topic in this era so the number of works mostly going on or very less. This paper introduces about an algorithm to create virtual node and link for network virtualization. There are already some techniques are available to create the virtual network but they are not showing the exact structure which will be required actually. The main problem is to differentiate between the adjacent nodes with their corresponding virtual link. Because In network virtualization creation of logical isolated network partitions overlaid on top of a common enterprise physical network infrastructure. Each partition is logically isolated from the others and most provides the same services that are available in a traditional dedicated enterprise network. The end user experience should be as if connected to a dedicated network providing privacy, security, an independent set of policies, services and even routing decisions. Because at the same time the network administrator can easily create and modify the virtual work environments for various users and adapt the business changing requirements for an enterprise. Also the virtualization of the transport must address the virtualization of the network decades as their interconnection. Fig. 4 shows the Virtual Nodes and Virtual Links with major principle such as: re-visitation, recursion, Inheritance and physical supports (Router/Switch).

*Proposed Algorithm*: Managing Virtual Node and Virtual Link in network virtualization.

*Let*virtual node is $\mathbf{V_1}$; adjacent of virtual node in virtual network is **V**.

*Case 1***:** IF*(Physical node is similar to the virtual node Index structure)*

THEN *Find adjacent node between physical infrastructure node and the parent virtual network node.*

IF*(adjacent node of physical infrastructure node =adjacent node of virtual network)*

THEN *link is in between those two nodes (adjacent of the virtual network node and virtual node.*

*(V<link<$\mathbf{V_1}$)*

*Repeat Case 1.*

IF *(link of virtual node and adjacent virtual node of virtual network = NULL)*

THEN *the link in not suitable for this case, go for case 2.*

*Case 2:* IF *(link is in between two different nodes)*

THEN IF *(adjacent node is NULL)*

THEN *generate virtual node.*

*Repeat all the above steps until one cannot found the structured network.*

IF *(Physical infrastructure node height =Parent Virtual network node height)*

THEN *this is not suitable for this case, go for case 3.*

*Case 3:* IF *(Physical infrastructure node height= Parent virtual network node height)*

THEN *create child virtual network by repeating the Case 1 and Case 2. And return the node and the link to the physical infrastructure corresponding to their virtual network structure.*

END.

For the abstraction of the virtual network one can use one another proposed algorithm to make process easier. We can press this algorithm in the case 2 and case 3 for the process of network virtualization.

FOR *(each node in virtual network, determine number of disjoint scoops and assign a virtual copy of the parent virtual network node to each scoops)*

FOR *(index node = 0: number of nodes in physical infrastructure network node)*

*Visit every node and find assigned virtual copy of the parent virtual network node.*

IF *(adjacent node has the assigned virtual copy)*

THEN *Swap with the real node from the physical infrastructure network node.*

END IF

END FOR

END FOR

Here the assumption is, there will be multiple infrastructure providers and service providers like internet today. Then this algorithm is very helpful to create and manage the virtual nodes and the virtual links for any virtual network corresponding to their physical infrastructure network. This algorithm is very helpful in case of security attacks, because once any one of node from any of layer will be compromised than all the above node will get down and service will be interrupted. To resolve this problem there is a need of such an algorithm which creates the virtual link, node automatically when ever this type of situation will be occurred.

## 5. RELATED WORK

Since Network virtualization is not a completely new concept for this age of study. The Virtual Nodes and virtual links are working on the basis of distributed networks principles where installed systems allowing for creation of Virtual Networks that are planned towards experimenting with new virtual network architectures [5]. Due to this, the Physical network is not aimed towards the features of the network virtualization. Actually the virtual network is scales in a setting with multiple competing infrastructure providers on the ground of physical network. Actually The Virtual network assignment problem is similar to the previous works on embedding VPNs in a shared provider topology and the network test-bed mapping problem. So the VPN request consists only of bandwidth requirements, specified in terms of traffic matrix without any constraint on its nodes. As a result, most Virtual Private Network designing algorithms come down to finding paths for source/destination pairs. On the other hand, the Network Virtualization model works on the basis of shared substrate node [2],[8]. This is nothing but the logically created function according to the concern hardware/router. In order to assign the nodes and the links to the end user one has to keep some necessary protocols according to the entities involved in virtualization environment. The X-Bone's global approach to network virtualization [12] allows for virtualization in presence of competing infrastructure providers but also aims for virtual test-beds and does not consider the attachment of end users to virtual networks. Further approaches of network virtualization are briefly summarized in [12]. Most approaches, however, do not consider an architectural framework and control interfaces to support it as networking paradigm on a global scale [8].

Fig.5. shows the sequence of the Network Virtualization. To make this model working it would be needed to connect the virtual network with an physical access network and the Access network contains some access node which are responsible to give the response to the end users. It also has one controller which is responsible to communicate with the SPs and InPs (Service Providers and Infra-Structure Providers).

## 6. CONCLUSION

To design the integral part of the future internet there is a need of some efficient and practical oriented algorithms to creating the virtual network. In the previous work done by the various researchers and groups, Lots of other network virtualization approaches are briefly summarized in [1-6]. Most approaches do not consider about the architecture of the virtual network and controlling of the services and policies. A recently published paper [2-4] tells about the connectivity of virtual nodes and architecture that is used to build the virtual networks. This algorithm differentiates between the Infrastructure providers and the service providers according to the Physical infrastructure networks. And with the help of this algorithm network administrator successfully creates and manage the virtual node and links between more than one virtual networks.

This helps to obtain the optimal complexity to create and manage the virtual networks. For the future work this paper introduces a lot of criteria as scalability, robust routing, and compatibility with routing algorithms, and performance where one can put this algorithm to obtain a good and effective virtual network environment.

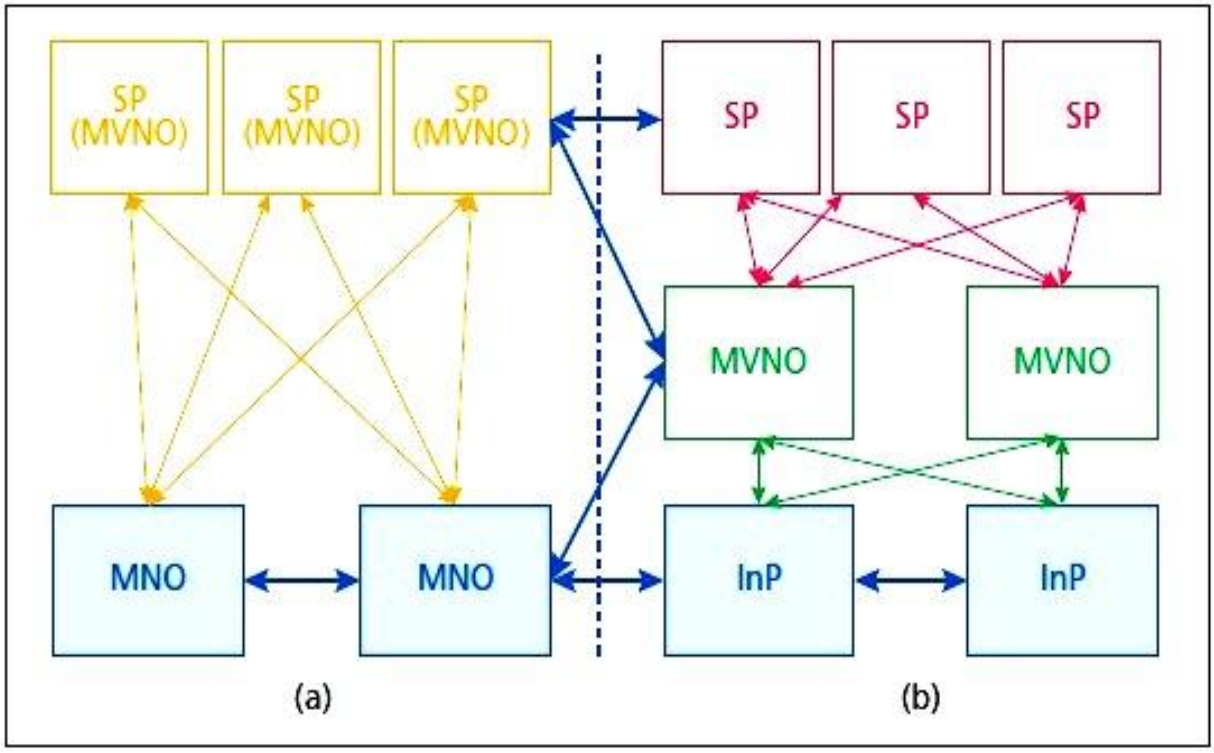


**Fig 1: Business model of Network virtualization Environment.**

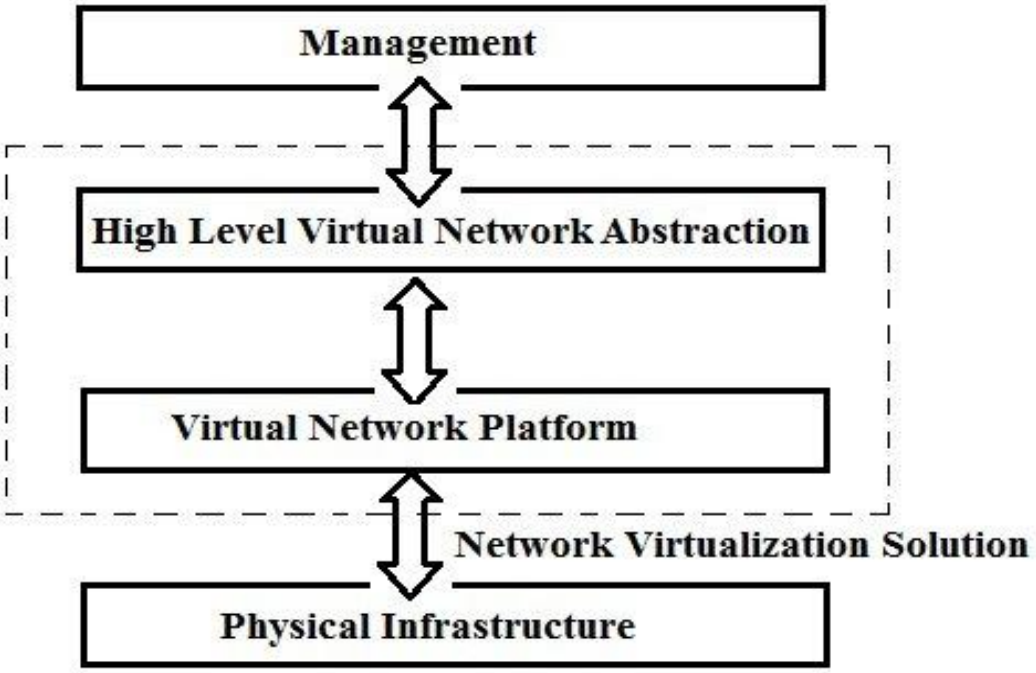


**Fig 2: Network Architecture. [12].**

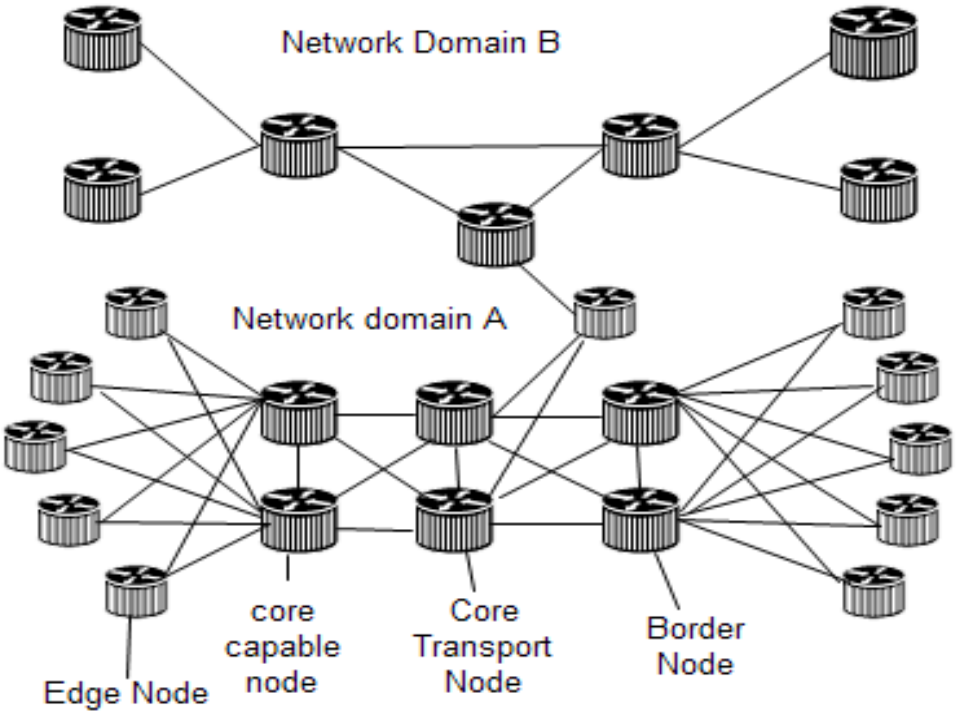


**Fig 3: Substrate Nodes in Network virtualization.**

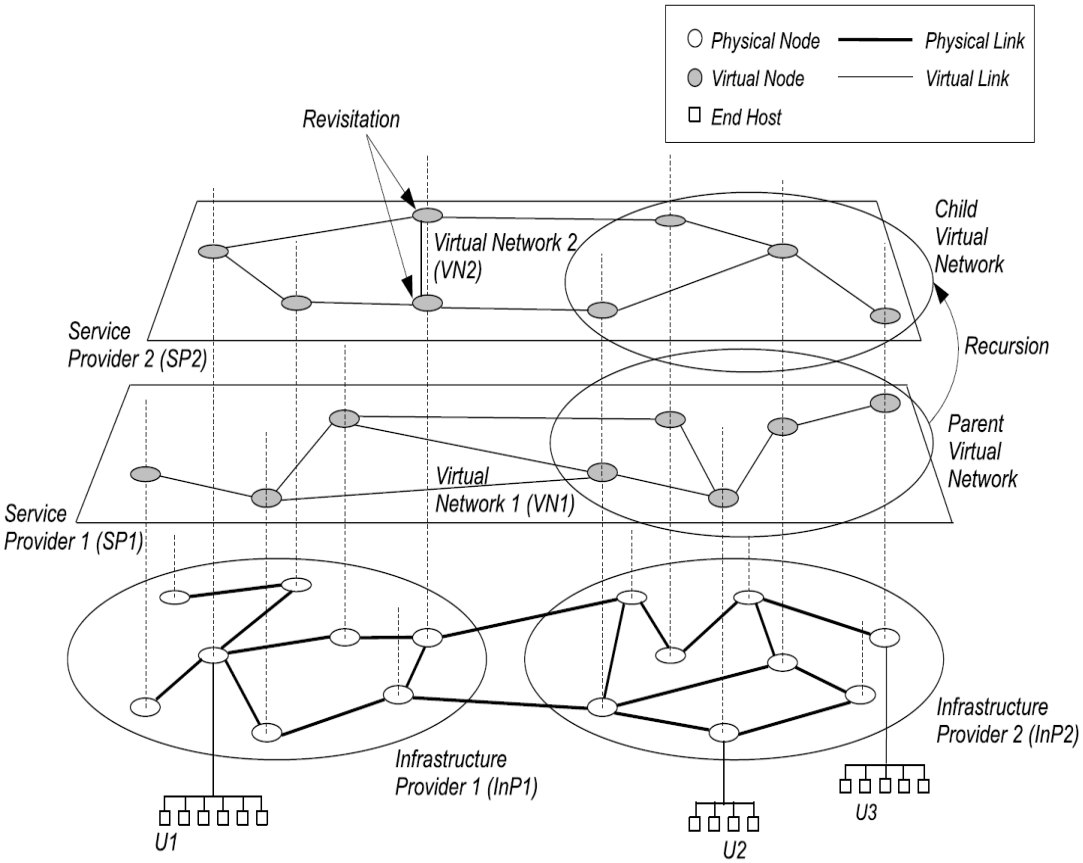


**Fig 4: Virtual Nodes and Virtual Links.**

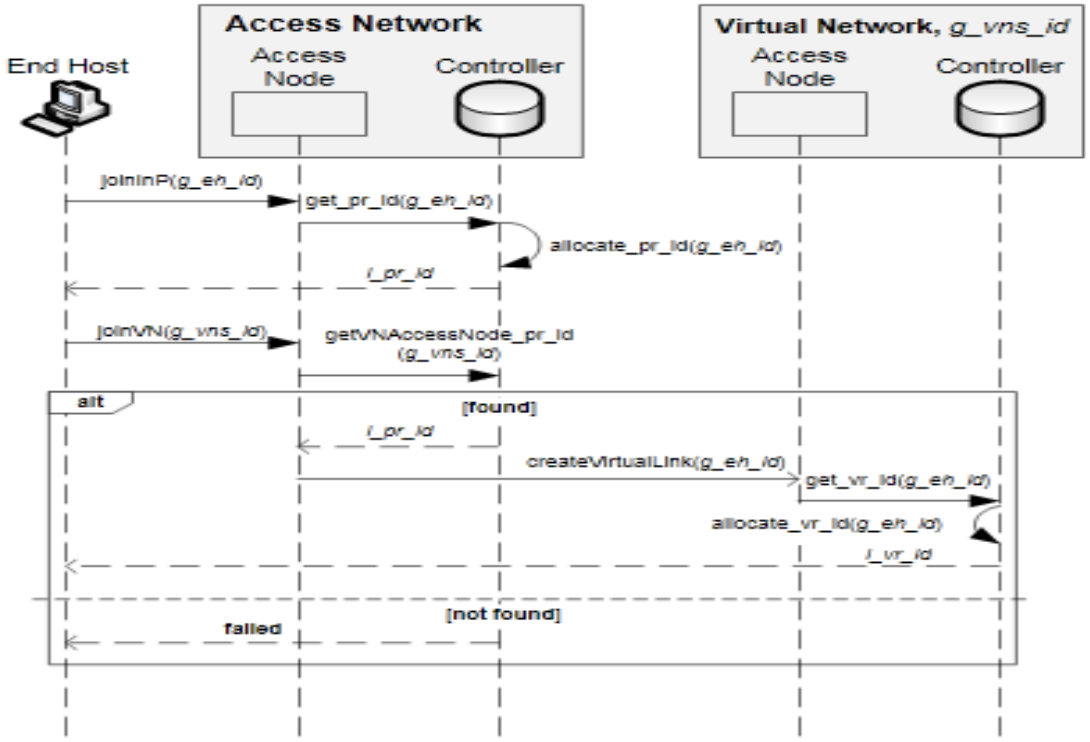


**Fig 5: Sequence Diagram [1]**

## 7. REFERENCES

[1] Peterson, L., Shenker, S., Roscoe, T., Anderson,T. 2005. "Overcoming the Internet impasse through virtualization." in IEEE Computer Magazine, vol. 38., , pp. 34-41.

[2] Gao, L., Rexford, J., Feamster, N. 2006. "How to lease the Internet in your spare time",in ACM Computer Communication Review, January, pp. 114-121.

[3] Boutaba, R., Chowdhury, N. M. K., 2008."A Survey of network Virtualization.," David R. Cheriton School of computer Science, University of Waterloo., Technical Report CS-2008-25.

[4] Taylor, D., Turner, J., 2005."Diversifying the internet," in IEEE Globle Telecommunications Conference (GLOBECOM'05), Vol. 2.

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

[6] Boutaba, R., Chowdhury, N. M. K., 2009. "Network Virtualization: State of the art and research challenges",in IEEE Communications Magazine 47 (7), pp. 20-26.

[7] R. Zhang-Shen, S. Rangarajan, J. Rexford. Y. Zhu, 2008. "Cabernet: Connectivity architecture for better network services", in Workshop on Re-architecting the Internet (ReArch, 08), ACM SigComm, Madrid.

[8] Al-Fares, Mohammad, Loukissas, Alexander, Vahdat, Amin, 2008. "AScalable, Commodity Data Center Network Architecture", In Proc. ACMSIGCOMM Conference on Data Communication, Seattle, WA.

[9] Barabash, Katherine, Cohen, Rami, Hadas,David, Jain,Vinit, Recio, Renato, Rochwerger , Benny, 2011. "A case for overlays in virtualization. InProceedings of the 3rd Workshop on Data Center", Converged and Virtual Ethernet Switching, DC-CaVES '11, pages 30–37. ITCP

[10] Birke, R. Crisan, D., Barabash, K., Levin,A., DeCusatis, C., Minkenberg, C., Gusat M., 2012."Partition/aggregate in commodity 10g Ethernet software-defined networking. In *High Performance Switching andRouting (HPSR)", IEEE 13th International Conference on*, pages 7–14.

[11] Wang, L., Zhang, F., Hou, C., Aroca, J.A., and Liu, Z. 2013. "Incorporating Rate Adaptation into Green Networking for Future Data Centers", 12th International Symposium on Network Computing and Applications, pp. 106-109.

[12] D. Bethanabhotla *et al.*, 2014. "User Association and Load Balancing for Cellular Massive MIMO," Proc. Information Theory and Applications Workshop (ITA), pp. 1–10.

[13] Upadhyay N.M. , Mittal, G., Saurabh, S.K., Gupta, P.K., 2011. "Creation of virtual node, virtual link and managing them in network virtualization". In WICT, University of Mumbai, Mumbai, India.

[14] Upadhyay N.M., Gaurav,K., Saurabh, S.K., 2013. "Security in Network Virtualization Concept and Challenges-A Survey", in Procd. NCRTCSG, Ambala, India.