A Survey on Network Virtualization Span

Bilal Bin Ijaz
Department of CS and IT
The University of Lahore Gujrat, Pakistan
bilalbinijaz@gmail.com

Muhammad Asim Iqbal
Department of CS and IT
The University of Lahore Gujrat, Pakistan
ch.asim100@gmail.com

Mr. Jawad Ibrahim
Department of CS and IT
The University of Lahore Gujrat, Pakistan
jawad.ibrahim @cs.uol.edu.pk

Saad Bin Ilyas
Department of CS and IT
The University of Lahore Gujrat, Pakistan
muhammad.ilyas@cs.uol.edu.pk

ABSTRACT- Due to Excessive need of communication mediums tech scientist and companies are worried about the utilization of physical resources but due to billions of communications it's not possible to manage hardware and maintain the services with less hesitation and cost effective method. Virtualization is a term which came into existence in 60s.The future of computer networks and IT is clearly relay on abstraction. That's way the Virtualization has drawn significant attention in academia as well as in corporations. Due to multiple stakeholders on internet its need to provide a new thing which is overcome the simple incremental updates and readily changing architecture of existing internet.. In this paper, the existing paradigm virtual private network (VPN) and virtual local area network (VLAN) of networking are discussed. And we survey the Network function virtualization (NFV) and Software defined networking (SDN) that base on the comparisons and the change the service providing scenario in this era. presents a number of challenges that network operators face in virtualization and the research in networks abstraction.

Keywords Virtual Private Networks (VPN), Virtual Local Area Network (VLAN), Network Function Virtualization (NFV), Software Defined Network (SDN),Peer-To-Peer Tunneling Protocol(PPTP),Customer Edge (CE), Provider Edge (PE), Service Provider (SP).

I. Introduction

Network virtualization is the ability to create a logical and virtual network that are decoupled from hardware to ensure the better integration and support the abstract environment. These virtual hardware has ability just like traditional hardware solution.

It makes possible for a single hardware platform to support multiple virtual devices to use or leave as needed. As a result, the virtual environment is more reliable, cost effective and more responsive support than traditional hardware support.

A. Why virtualization in computing

In 1960s the concept of virtualization came into existence when the demand of high storage space is required. Memory was the expensive part of computers; It is the need of development to construct or design a memory which is effective complex scenarios. The computer Scientists work on virtualization from many years. In the result

we have a reliable and sophisticated memory for processing like cache. The concept of storage virtualization is virtual disks and Virtual compact disks, now this is leading to cloud storage.

Computer networking is the basic communicator of the computing. Through networking offered the new features to user by computing architecture. Virtualization in networking is not much older concept. Telecommunication networks like virtual channel in X.25 allow the multiple users to share the large a physical channel.

On internet there has been a need for protocols to keep data private and secure. Privacy protection on internet and web culture is record a secure network. To handle this problem first time, introduce the concept of virtualization to overcome this. For this introduce a VPN(Virtual Private Network) that typically a paid service that keeps your web browsing secure and private over public hotspots.

Virtualization of hardware is used to separate and make physical resources of hardware available to logical machines [26], these machines works same like physical machine does. Virtualization introduces a new layer of implementation to our traditional computer networks. The VLAN technology network, which is usually defined as a broadcast domain can be considered as a group of one of the regions of the terminal station.in this paper we discuss the VLAN working and the conditions in which it is suitable to use.

Network Functions Virtualization (NFV) and Software-defined networking (SDN) have changed the traditional communication concept. Future of networks is now transforming in the way of communication service providers design and their network infrastructure and services. SDN and NFV use standard virtualization technologies to virtualize entire classes of network functions that can be connected or chained together to create network services.

II.TECHONOLOGY

A. Virtual Private Network

History of Virtual private network technology dates back to 1996, when a Microsoft employee developed the peer-to-peer tunneling protocol(PPTP). Effectively the precursor to modern VPNs, PPTP creates a more secure and private connection between a computer and the internet.The Challenging thing to a computer user is the protection of privacy.

A virtual private network (VPN) [1–3] 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]. While VPN implementations exist in several layers of the network stack.

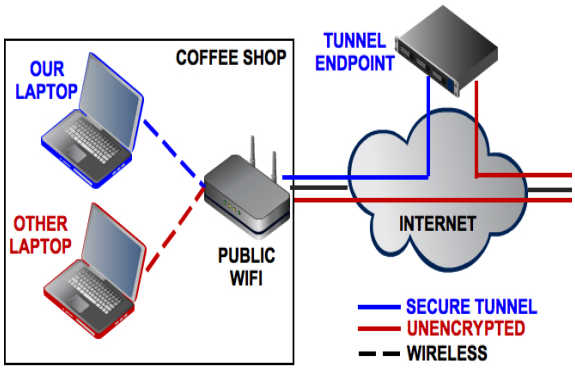


Fig.1 virtual private network secure working

In the Fig.1 a tunnel connection is shown that the secure connection can be achieved by VPN. Like on a public network you can spoof your location.

It is clear the need of VPN due to lot of unsecure and un reliable connection. But VPN has also some limits likeInternet-based VPN are not under direct control of an organization rather than which solution can provide by a ISP.There is an also issue of different vender's technology that paid of a computability issue.

B. 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.

Virtual local area networks (VLANs) acts like a physical LAN, but it allows hosts to be grouped together in the same broadcast domain even if they are not connected to the same switch with isolation. Virtual Private Network(VPN) technology is most widely used in corporate environments.Itsprovide elevated levels of trust, security, and isolation, and they are cost-effective. This virtual encrypted connection helps to ensure the safely transmission of sensitive data. Also used to prevent the unauthorized access and traffic. So the user can conduct remotely work in secure environment.

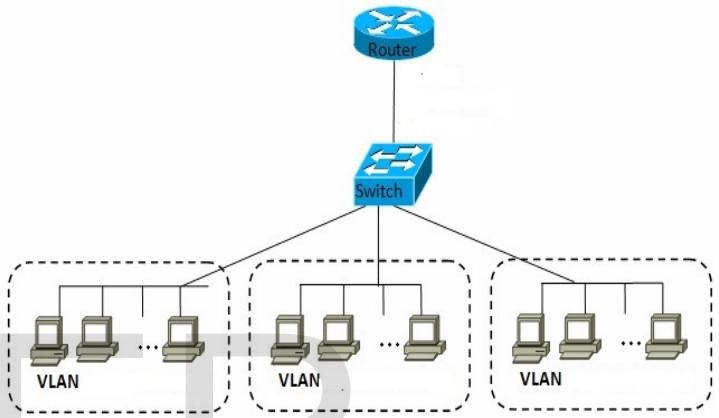


Fig.2 Virtual Local Area Network

In the Fig.2 A VLAN working is shown. This is used when we want to make a network but due to lake of ports we make a virtual environment to make connection. In above Figure Three different locations of a networks like office, lab and library. If these want to connect and exchange the information with other like library want to communicate with office than LAN is not support this so we can make VLANs that connect all LANs with a single rather than multiple switch because in VLAN all ports can be configured.

The main latency problems of a router can be solved by VLANs.VLANs are essentially

Layer-2 constructs, even though implementations in different layers do exist. All frames in a VLAN bear a common VLAN ID in their MAC headers, and VLAN-enabled switches use both the destination MAC address and the VLAN ID to forward frames. Multiple VLANs on multiple switches can be connected together using trunking, which allows information from multiple VLANs to be carried over a single link between switches.

i. Why Used VLAN

It is best to use when you have to connect more devices on your LAN, like if the devises are more than 200.The main cost effective thing in VLAN is it provide the configuration of each and every port on a switch. The issue of lot of broadcast traffic is solved with the help of VLANs it also helps out to overcome the slowdown of network due to security measures implementation.VLAN are reduce the cost of physical devices, you can use a single switch rather than multiple switches.

C. Network Function Virtualization

The concept and collaborative work on NFV was born in October 2012 when a number of the world's leading TSPs jointly authored a white paper [6] calling for industrial and research action.The highly diverse and dynamic network services demanded by current and emerging applications bring in new challenges to service provisioning in future networks.Network virtualization introduces an abstraction of the underlying infrastructure upon which virtual networks with alternative architecture may be constructed to meet diverse service requirements [2].The European Telecommunications Standards Institute (ETSI) developed NFV, a network architecture concept that leverages virtualization technologies to transfer network functions from hardware appliances to software applications [3].

Diverse and fixed proprietary appliances make the service deployment and testing increasingly difficult. NFV was proposed as a key technology to benefit IT virtualization evolution [8], [20], [21] by separating the hardware network functions from the underlying hardware appliances by transferring network functions from dedicated hardware to general software running on commercial off-the-shelf (COTS) equipment's, i.e., virtual machines [22] [25]. These software applications are running on standard IT platforms like high-performance switches, service, and storage. By NFV, the different network functions can be deployed in different locations of the networks such as data-centres, network nodes, and end-node of network edge as required. Currently, the market of NFV includes switching elements, network appliances, network services and applications.

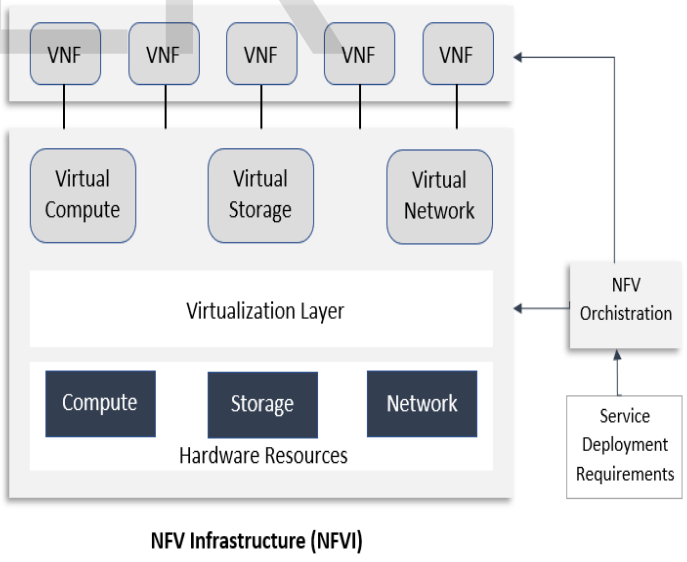


Fig.3 NFV Architecture

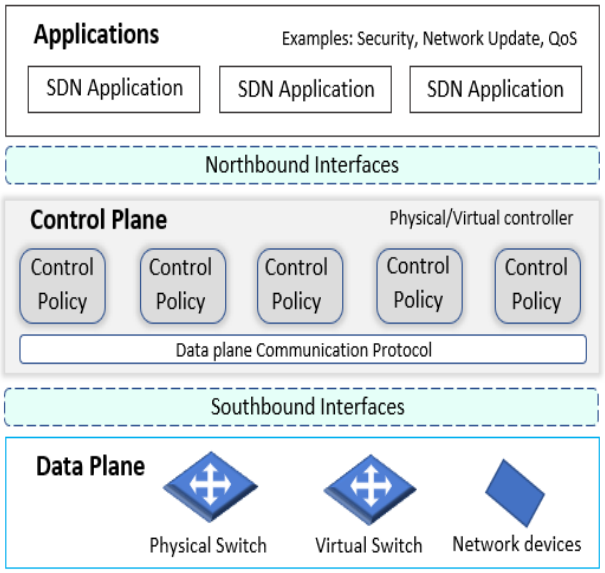
NFV is to reduce middle boxes deployed in the traditional networks to take the advantages of cost savings and bring flexibility.NFV technology

also supports the co-exists of multi-tenancy of network and service functions, through allowing the usage of one physical platform for different services, applications, and tenants.NFV grips the notion of network virtualization and provides more specific mechanisms to decouple service functions from infrastructures. Software-defined networking (SDN) and network functions virtualization (NFV) are two significant recent innovations that are expected to address these challenges.

For the research community to develop new architectures, systems and applications, and to evaluate alternatives and trade-offs in rapid advancement in networking and computing technologies has enabled a wide variety of applications with diverse requirements on network services. The major benefits introduced by NFV include simplified service development, more flexible service delivery, and reduced network capital and operational costs.

D. Software Defined Network

Software-Defined Network (SDN) is an important and recently emerging network architecture to decouple the network control from the data forwarding by directly programming [13], [15]. With its inherent decoupling of control plane from data plane, SDN offers a greater control of a network through programming [16]. This combined feature would bring potential benefits of enhanced configuration, improved performance, and encouraged innovation in network architecture and operations.SDN offers a promising alternative for traffic steering by programmatically configuring forwarding rules [11].



SDN Architecture

Fig. 4 depicts the SDN architecture [11], [17].

There are three different layers:

Application Layer:

This layer covers an array of application focusing on network services, and they are mainly software applications communicating with the control layer.

Control Layer [18] [19]:

As the core of SDN, the control layer consists of a centralized controller, which logically maintains a global and dynamic network view, takes requests from the application layer, and manages the network devices via standard protocols.

Data-plane Layer:

Infrastructure including switches, routers and network appliances. In SDN context, these devices are programmable and support standard interfaces [12].

The application layer utilizes the northbound APIs to communicate with the SDN controller, which enable different control mechanisms for the networks. The southbound APIs de ne the communication interface between the controller layer and data plane devices, which on the other hand enable the application to control the forwarding device via this flexible and programmable way.

SDN separates network control and data forwarding functionalities to enable centralized and programmable network [1].
Key components of the SDN architecture include a data plane consisting of network resources for data forwarding, a control plane comprising SDN controller(s) providing centralized control of network resources, and control/management applications that program network operations through a controller. The control-resource interface between the control and data planes is called the southbound interface, while the control-application interface is called the northbound interface.
Advantages promised by SDN include simplified and enhanced network control, flexible and efficient network management, and improved network service performance.

III. COMPARISON

Both SDN and NFV rely on software that operates on commodity servers and switches, but both technologies operate at different levels of the network. SDN is designed to offer users a way to managed network services through software that makes networks centrally programmable, which allows for faster configuration. On the other side NFV separates network functions from routers, firewalls, load balancers and other dedicated hardware devices and allows network services to be hosted on virtual machines.

Because these both are based on concept of abstraction so as comparison SDN seeks to separate network control functions from network forwarding functions, while NFV seeks to abstract network forwarding and other networking functions from the hardware on which it runs.

Issue	NFV (Telecom Networks)	Software Defined Networking
Approach	Service/Function Abstraction	Networking Abstraction
Formalization	ETSI	ONF
Advantage	Promises to bring flexibility and cost reduction	Promises to bring unified programmable control and open interfaces
Protocol	Multiple control protocols (e. g SNMP, NETCONF)	OpenFlow is de-facto standard
Applications run	Commodity servers and switches	Commodity servers for control plane and possibility for specialized hardware for data plane
Leaders	Mainly Telecom service providers	Mainly networking software and hardware vendors
Business Initiator	Telecom service providers	Born on the campus, matured in the data centre

Table.1 NFVvs. SDN

IV. CHALLENGES

One of the difficulties developing in the NFV situation is the thought of various leveled organization, as there are various viewpoints prompting this methodology. To begin with, we should consider the adaptability of the coordination procedure. The administrations will in all probability be conveyed over frameworks covering noteworthy land scopes, blending assets sent over access, collection, and center systems, and notwithstanding achieving assets overseen by outsiders.

Another test to be considered is the normal changeability of the administration over its life cycle, and in the organization procedure itself. System administrations will be worked as a blend and match of the diverse accessible system

capacities;however,this procedure will presumably be completed in various strides by various entertainers.

CHALLENGES	NFV(Network function virtualization) And SDN(Software define network)
New Technology	Difficult to stay up-to-date
Legacy infrastructure	Significant challenge to adoption and scale is legacy networks. Several older products will not be upgraded to support the technology
Security Issues	Open window for security risks. Software's are naturally less secure than hardware
Lack of Standards	Virtualized market is the need for standards for communications among components but it takes years.
Traffic	Traffic in an NFV network will be invisible using traditional monitoring strategies.
Failure Handling	It is non-trivial to detect and respond to failures in NFV. Although most failures are supposed to be handled automatically, Staff needs to know how to verify that everything went well and must re-learn how to deal with problems in the new framework.
Foundation reflection	Virtualization of physical foundations for layer-measurement reflection assumes a critical job in future systems administration with SDN-NFV combination. How it offers a promising way to deal with giving standard interfaces.
Constriction of virtual system	How to give abstract descriptions of VSF attributes, how to make VSFs available and discoverable, and how to select and compose the optimal set of VSFs are all relevant problems that need more thorough study.
Quality and administration confirmation	How can achieve the comparable level of quality and confirmation like physical hardware as compare to virtual environment
Embedding	Virtual network embedding brings in a new challenge for embedding VNs comprising virtual functions of both networking and computing into heterogeneous infrastructures networks as well as data.This requires federated control and management of network, compute, and storage resources across autonomous domains on an Internet scale.
Management of virtual systems and capacities	Discrete interfaces for controlling and overseeing physical framework assets and virtual administration capacities is a challenge.

Table.2 Virtualization Cha

V. CONCLUSION

We can conclude the Successful Reason of Virtualization of Networks in this paper some core reason which gives strongest in information technology:

Management is the one of reason because Physical devices are difficult to manage because these are hardware oriented but in virtualization management is more reliable due to the software based and uniform interface which is through standard abstraction. Virtualization feature Sharing is a old but effective in past multi-core processors are used in computer technology for the allocation of huge resources by dividing into virtual parts. This division can make it possible to run different virtual machines (VMs) for multiple users. It will same but opposite technique is used to construct a large virtual resource which is roll up by small resources. A Giant virtual resource will be help out in making reliable storage which is derived from many unusable and extra resources.

Mobility of users is readily increases due to availability of quick access Resource but the issue which it brings is reallocation. Virtual Resources is the easier way to reallocate them without any hesitation of physical requirements.Isolation is most discussing thing because Single user always be a most secure entity in networking but a network is never being a single user, multiple users are exchanging and helping multiple resources, so it is important to make a secure bridge which cannot isolate data among the users [7].

A single virtual component is not being able to monitor the activities or interfere with the activities of other users. In case, Different users belong to same organization can chose this for reliable results.

References:

[1] Chowdhury, NM MosharafKabir, and RaoufBoutaba. "A survey of network virtualization." *Computer Networks* 54.5 (2010): 862-876.

[2] Rosen, Eric, and YakovRekhter. *Bgp/mplsvpns*. No. RFC 2547. 1999.

[3] Rosen, E., and YakovRekhter. *BGP/MPLS IP virtual private networks (VPNs)*. No. RFC 4364. 2006.

[4] Chowdhury, NM MosharafKabir, and RaoufBoutaba. "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] Virtualisation, Network Functions. "An introduction, benefits, enablers, challenges & call for action." *White Paper, SDN and OpenFlow World Congress*. 2012.

[7] Jain, Raj, and Subharthi Paul. "Network virtualization and software defined networking for cloud computing: a survey." *IEEE Communications Magazine* 51.11 (2013): 24-31.

[8] Schaffrath, Gregor, et al. "Network virtualization architecture: Proposal and initial prototype." *Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures*. ACM, 2009.

[9] Fischer, Andreas, et al. "Virtual network embedding: A survey." *IEEE Communications Surveys & Tutorials* 15.4 (2013): 1888-1906.

[10] Fischer, Andreas, et al. "Virtual network embedding: A survey." *IEEE Communications Surveys & Tutorials* 15.4 (2013): 1888-1906.

[11] Duan, Qiang, Yuhong Yan, and Athanasios V. Vasilakos. "A survey on service-oriented network virtualization toward convergence of

networking and cloud computing." *IEEE Transactions on Network and Service Management* 9.4 (2012): 373-392.

[11] Rao, Sridhar KN. "SDN and its Use-Cases-NV and NFV." *Network* 2 (2014): H6.

[12] Handigol, Nikhil, et al. "Plug-n-Serve: Load-balancing web traffic using OpenFlow." *ACM Sigcomm Demo* 4.5 (2009): 6.

[13] Mendonca, Marc, et al. "A Survey of Software-Defined Networking: Past." *Present, and Future of Programmable Networks* (2013).

[14] Bakhshi, Taimur. "State of the art and recent research advances in software defined networking." *Wireless Communications and Mobile Computing* 2017 (2017).

[15] Fundation, Open Networking. "Software-defined networking: The new norm for networks." *ONF White Paper* 2 (2012): 2-6.

[16] Foster, Nate, et al. "Frenetic: A network programming language." *ACM Sigplan Notices* 46.9 (2011): 279-291.

[17] Raghavan, Barath, et al. "Software-defined internet architecture: decoupling architecture from infrastructure." *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*. ACM, 2012.

[18] Tootoonchian, Amin, et al. "On Controller Performance in Software-Defined Networks." *Hot-ICE* 12 (2012): 1-6.

[19] Monaco, Matthew, Oliver Michel, and Eric Keller. "Applying operating system principles to SDN controller design." *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*. ACM, 2013

[20] Chowdhury, NM MosharafKabir, and RaoufBoutaba. "A survey of network virtualization." *Computer Networks* 54.5 (2010): 862-876.

[21] Chowdhury, NM MosharafKabir, and RaoufBoutaba. "Network virtualization: state of the art and research challenges." *IEEE Communications magazine* 47.7 (2009): 20-26.

[22] Santos, Jose Renato, et al. "Bridging the Gap between Software and Hardware Techniques for I/O Virtualization." *USENIX Annual Technical Conference*. 2008.

[23] Egi, Norbert, et al. "Towards high performance virtual routers on commodity hardware." *Proceedings of the 2008 ACM CoNEXT Conference*. ACM, 2008.

[24] Al-Fares, Mohammad, Alexander Loukissas, and Amin Vahdat. "A scalable, commodity data center network architecture." *ACM SIGCOMM Computer Communication Review*. Vol. 38. No. 4. ACM, 2008.

[25] Greenhalgh, Adam, et al. "Flow processing and the rise of commodity network hardware." *ACM SIGCOMM Computer Communication Review* 39.2 (2009): 20-26.

[26] Sahoo, Jyotiprakash, SubasishMohapatra, and Radha Lath. "Virtualization: A survey on concepts, taxonomy and associated security issues." *2010 Second International Conference on Computer and Network Technology*. IEEE, 2010.