VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

Digital Assignment, OCTOBER 2020

B.Tech., Fall-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	ITE3001
COURSE NAME	DATA COMMUNICATION AND COMPUTER NETWORKS
SLOT	B2+TB2
FACULTY	Prof. DINAKARAN M.
SURVEY TITLE	SOFTWARE-DEFINED NETWORK FUNCTION AND VIRTUALIZATION

What is SDN?

Enterprise networks are vital in keeping a business connected but they are struggling to keep up with the demands of digital business like more data, video and voice, more mobile users, devices and cloud services and more online threats. A network is made up of lots of different boxes called routers and switches. It functions a bit like an old toy train set where each piece of track controls how traffic is managed and forwarded. It needs to be set up by hand which takes time, is costly and is prone to human error and each piece of track is not smart enough to know what the rest of the track looks like or how its performing. Adding more capacity or capabilities such as to support more traffic means adding more of those routers and switches which means more time cost and complexity.

The software-defined network (SDN) is different. It works by virtualizing the network giving new levels of visibility and control. Simply put, it moves control of the network away from all the individual pieces to a centralized dashboard where you are always in the know. So instead of that old train set it is more like a computer game where you can build and adapt the perfect transport network in real time. You get a real-time bird's-eye view of what is happening instead of manually updating each piece of track. You can program it to adapt dynamically.

The rules you set helped your network become more intelligent and responsive so you can allocate bandwidth automatically making sure the most important traffic takes priority. By pooling your network capacity, you can make the efficient use of all your resources so that staff and customers get the best possible experience and because your network knows what is going on it can detect and block security threats before they can derail your business. In short, the network works out for itself what each part needs to do saving time and cost and reducing risk.

What is NFV?

Network function virtualization NFV decouples hardware from software in network functions. Network function virtualization is a subset of software-defined networking, this huge trend right now in networking called SDN. So, it moves network functions from specialized appliances right. To have specialized hardware and embedded software that runs on them, to applications that simply run on common off-the-shelf equipment just standard server appliances switches and storage the basic structure here.

Traditionally you had specialized appliances for firewalls, load balancers, deep packet inspection routers, all these things were basically appliances. Your appliances that have specialized hardware designed by the manufacturer right in case of firewall may be right makes a specialized firewall or load balancers from function that have specialized rack mountable appliances with their own hardware and their own embedded software running on that hardware. So, each time you want to add a load balancer to your data centre, you are

basically ordering a piece of equipment sending a technician out to the data centre to install and set that up. But with software-based functions these same network functions are performed now on off-the-shelf servers.

There is a virtualization layer so the hypervisor and then you are running a firewall virtualized network function or load balancer virtualized network function or router and virtualized network function. On top of this basically off-the-shelf hardware and what manages all this there is an orchestration and management layer that manages all these network functions. So, the advantages are pretty obvious. It is much more flexible to have SEP to have separation of hardware and software. It is much more scalable and elastic so you can scale or down your load balancing or your firewall capacity by simply pushing a button on a control panel from anywhere.

If you need to add a new firewall you do not order a piece of equipment and have a technician install it which would sometimes take weeks. You basically press a button on your control panel and new firewall is instantly configured and set up within minutes in your data centre. So, it is much more scalable and much more elastic. Depending on whether your need for capacity is going up or down in your data centre you can localize these network functions. Now you can move to exactly where the workload is within the data centre not just wherever you have space.

Cost reduction: You reduce your capital expenditure and your operating expenditure. You are not pouring out money upfront for a new piece of equipment and operating expenses should be lower using virtualized network functions time to market. You no longer have to wait for a new equipment cycle typically as two to three years for networking equipment now you are basically just waiting for a new software cycle and a release cycle for new features in the virtualized network function. In innovation now, all of a sudden are a whole new batch of start-up companies and small companies that do not have the high barriers to entry or to compete in this space. You also have contribution and innovation coming from the academic side so potentially there is a lot of new innovation.

You can come in to virtualise network functions so some of the challenges and requirements can be addressed. Virtualized Network functions have to be as fast, secure, reliable, easy to operate and instantiate. They have to be every bit as good in every respect as the custom-made appliances that they are replacing. There is a basic framework defined by the European telecom standards Institute. It is a pretty loosely defined framework that virtualized network functions run on and it is intentionally defined loosely so that there is room for innovation, room for a lot of different solutions depending on what works best for different customers.

But the basic framework is that there is a hardware layer, you have storage, network and compute resources down here and on top of that there is a virtualization layer, basically a

hypervisor. And then there is a virtualization layer on top of that and then you have applications running on top of this virtualized Hardware and then on the right here we have basically orchestration and management. So, there is a module that runs the that basically does all the orchestration and management.

Network function virtualization with software-defined networking basically sits on the northbound API between the application layer and the control layer. So, in a fee management and orchestration is a pretty important piece of NFV. So, again there is a framework basically defined by ETSI for what functions have to be carried out by the management and orchestration layers. So, orchestration is managing the life cycle of network services instantiation and elastic scaling for the network services. It is doing onboarding for new network services and it is doing performance measurements. It basically needs to gather statistics on the performance of each virtualized Network function and look for ones that are overworked and ones that are under worked and make adjustments as needed.

In access control right we have security so we have to control validation and authorization for each all the network resources in the management module is going to manage the configuration life cycle management and element management for the virtualized Network function instances. So you may have many instances of a firewall for instance a NFV virtualized firewall and the management module is going to have to keep track of all those which ones are running on which server it basically is going to build up new ones tear other ones down it manages a scale up and scale down dynamically on an as-needed basis. So, it is taking these statistics the performance measurements provided by the orchestration layer and saying hey we need to increase our firewall capacity over here on this section of the data centre.

Some of the promised benefits of Network Virtualization are more rapid innovation since innovation can proceed at the rate at which software evolves. Rather on hardware development cycles, allowing for new forms of network control, and potentially simplifying programming. It is important to make a distinction between Network Virtualization and Software-Defined Networking. Network Virtualization is arguably one of the first killer applications for SDN. And in some sense, SDN is a tool for implementing Network virtualization. But the two are not one in the same. Remember the defining tenant of SDN is the separation of the data and control plant, whereas the defining tenant of Network virtualization. Is to separate the underlying physical network from the logical networks that lie on top of it. So SDN can be used to simplify many aspects of Network virtualization. But it does not inherently obstruct the details of the underlying physical network.

Network Functions Virtualization (NFV) and Software Defined Networking (SDN) improve network abilities by empowering the sending and control of network capacities utilizing programming rather than equipment explicit middleboxes. This programmability empowers the advancement of new programming administrations intended to meet a developing

rundown of organization necessities. By and by, this equivalent adaptability and programmability can encourage malignant conduct by assailants with incomplete access to the SDN and NFV the board foundation.

Challenges?

SDN and NFV together provide a synergy which opens many new opportunities in network architecture and management. The key to success with SDN and NFV is to develop long-term plans and carry them out one step at a time replacing network devices with software required hardware changes at the beginning. Vendor compatibility is not standardized yet meaning VNFs from different vendors may not be working together at an optimal level. Network management may present unique challenges in the case of service interventions. In system, configurations will vary as customers gain control. With a new virtual infrastructure that can start up in minutes the provider needs to keep up with the rapid growth that short-term spurts do not overwhelm. At any network security is essential with SDN since it entails sending network control data over the internet. The SDN controller needs to be highly reliable to prevent any malware or DDo attack. Keep your telecom services up-to-date with the latest technological development.

NFV is excessively intricate. While NFV gives a chance to diminish opex and improve client experience, it presents extra layers of operational unpredictability that "put more onus on the administrator to coordinate innovations that were generally incorporated by a seller."

This rings with the aftereffects of a review that as of late attempted that got some information about the hugest boundaries to actualizing open source NFV (rather than sourcing a turnkey arrangement from one provider). Development/soundness (35%) was the main concern, which is nothing unexpected given that a large number of the open source NFV ventures are very new.

As communication service providers or CSP move from physical to hybrid networks, incorporating SDN an NFV continue to offer service and regulatory edicts will play a very important role. When we talk about continuity of service we are talking about two aspect the security of the virtualized environment as well as the continuity's of service in the same environment. Today's network are primarily built on infrastructures that are closed platforms just as they have been for decades. The new paradigm shift to SDN and NFV means that the infrastructure becomes more software based, more open and more IT.

The unavoidable uptick sought after for new process, organization and capacity in programming characterized foundation represents a danger to checking stages. These arrangements must have the option to add observing ability to oblige the fast development

of the foundation. On the off chance that they can't include extra limit request, they can immediately become over-bought in, making execution perceivability holes.

Not at all like inheritance framework in the SDN world we can have various overlay geographies running on head of the physical organization. At whatever point another help begins, it conveys the fundamental virtual framework, and along these lines the quantity of observed components can develop quickly with expanded interest – overwhelming customary limit the executives.

The arrangement is to send execution checking inside both physical and virtual machines. At the point when additional exhibition the executives limit is required, turning up extra virtual apparatuses on request empowers execution checking to flex with the requests of a SDN climate and still give answers in short order.

The unavoidable uptick sought after for new process, organization and capacity in programming characterized foundation represents a danger to checking stages. These arrangements must have the option to add observing ability to oblige the fast development of the foundation. On the off chance that they can't include extra limit request, they can immediately become over-bought in, making execution holes.

Not at all like inheritance framework in the SDN world we can have various overlay geographies running on head of the physical organization. At whatever point another help begins, it conveys the fundamental virtual framework, and along these lines the quantity of observed components can develop quickly with expanded interest – overwhelming customary limit the executives.

The arrangement is to send execution checking inside both physical and virtual machines. At the point when additional exhibition the executives limit is required, turning up extra virtual apparatuses on request empowers execution checking to flex with the requests of a SDN climate and still give answers in short order.

Life open protocols like OpenSwitch, Linux, Oopenstack along with white box hardware or the foundation of this paradigm change. Several vendors are proposing open source orchestration solutions and CSPs are working on customer service provisioning portals. This opens up the network to even more vulnerabilities and challenges from security perspective as well as introducing some new network assurance requirements handle CSPs prevent against denial of service attacks.

SV is moved to SDN and NFV components become a couple so again. The question is how are regulatory services enforced in a virtualized environment when the function residency can change throughout the virtual environment IE function fluidity local regulations can be used

for address local infrastructure issues whereas network service provision like Internet services may require more of a global regulation and governance network processing analysis and management are being shifted to the cloud often referred to a poco cloud enabling services over multiple infrastructures which in turn will require a thorough revision of the current regulatory framework.

The capacity to mechanize the provisioning of new combined frameworks in minutes and effect different gadgets simultaneously is a distinct advantage, particularly thinking about that the present relative static conditions depend on manual setups. With SDN, new register, organization and capacity gadgets and highlights are promptly accessible for use. At the point when just running day by day minds what's happening in your current circumstance, these dynamic, continuous changes mean noteworthy holes in perceivability.

Click on the links below to view referenced research papers.

Reference 1	Reference 2	Reference 3	Reference 4
Reference 5	Reference 6	Reference 7	Reference 8
Reference 9	Reference 10	Reference 11	Reference 12
Reference 13	Reference 14	Reference 15	Reference 16

****