PLANNING AND MANAGING VIRTUALIZED NEXT GENERATION NETWORKS

Sukant K. Mohapatra[1],Jay N. Bhuyan[2] and Hira N. Narang[2]

[1]Marlboro, NJ, USA
[2]Dept. of Comp. Science, Tuskegee, AL, USA

ABSTRACT

Service convergence, content digitization, rapid and flexible service delivery, reduction of capital and operating costs, economies of scale, changes in telecom policy and regulation, and ever increasing competition have been key factors in the evolution of virtualized Next Generation Networks (vNGN). IP-centric converged networks aim to provide a multitude of services over a single network infrastructure. Tremendous success and benefit of server virtualization in data centers is driving the adaption of network virtualization. Network virtualization is applicable to enterprise data center, and enterprise as well as wide area networks. The focus of this paper is network virtualization aspects of service providers' next generation network. The key factors for moving to virtualized network is optimal use and sharing of network infrastructure even among competitive service providers, programmability of network and rapid introduction of new service and standard based on open platform rather than proprietary implementation. Evolving Software Defined Network (SDN) and Network Function Virtualization (NFV) shall enable common network infrastructure sharing, control, and management at a higher layer thus making network devices more generic and less intelligent, thus enabling cost competitiveness and quick service delivery. Network virtualization shall enable key benefits such as lower cost, flexibility, efficiency, and security, However, the deployment of virtualized next generation networks has brought its unique challenges for network managers and planners, as the network has to be planned in a comprehensive way with effective management of virtual network elements, its correlation with physical infrastructure and monitoring of control functions and server platforms. This paper discusses generic next generation network, its virtualization, and addresses the challenges related to the planning and managing of virtualized next generation networks. This paper proposes a reference OSS model enabling effective management of vNGN, which is key contribution of this paper.

KEYWORDS

VLAN, VRF, NFV, SDN, vNGN, VNF, MANO, ONF, OpenFlow and OpenStack

1.INTRODUCTION

This paper discusses the service convergence and convergence of multiple segmented networks leading to evolution of IP-based Next Generation Networks (NGN). The paper provides an overview of NGN architecture as proposed by ITU-T [1]. The paper outlines a generic next generation network physical architecture based on transport stratum per ITU-T reference model. The architecture covers various network domains, including access, aggregation, and core network with potential technology options in each domain.

Network virtualization enables creation of virtual logical network that is decoupled from underlying physical network infrastructure and yet uses the same in supporting multiple logical networks over physical network resources. With network virtualization, one can utilize multiple physical networks into a single virtual network, or a single physical network can support multiple virtual networks. Network virtualization can also be used to create virtual networks within a

DOI : 10.5121/ijcnc.2015.7601

virtualized network construct, thus enabling support of multi-tenancy environments. Network virtualization provides tremendous benefits with respect to cost saving, rapid service introduction, scalability, and flexibility of a programmable network. This paper discusses the concepts, mechanisms, evolving standards, and architectural components based on Software Defined Network (SDN) and Network Function Virtualization (NFV) in realizing vNGN. NFV enables service providers to speed up deployment of new network services in order to foster revenue and growth.

However, network virtualization has its own challenges for network planners and managers in effective planning and managing virtualized network. Paper [7] discussed network virtualization design goals and challenges. Paper [11] describes challenges while in implementing SDN in carrier grade network. This paper discusses various challenges and issues that need to be duly considered in planning a virtualized network. Key issues for virtualized network management such as end-to-end visualization of virtual network, performance and fault monitoring of controller, configuration of virtual switches/routers (vSwitch/vRouters), monitoring and association of virtual and physical components, etc. are also addressed in this paper.

A generic Operation Support System (OSS) architectural solution is proposed in this paper. This solution enables management of virtualized next generation network (vNGN). The paper also discusses how the challenges and issues faced in managing vNGN are addressed in the proposed solution.

The paper is organized as follows: in section II, we discuss service and network convergence and describe the physical infrastructure of next generation network architecture covering various domains. Section III discusses the concept behind network virtualization, different options and evolving model based on SDN and NFV for implementing network virtualization. Section IV outlines the challenges in planning and managing vNGN. Section V provides a detailed view of solution architecture, its different components, and how it meets the challenges of managing virtualized next generation networks. Finally, we conclude the paper in section VI.

2. SERVICE AND NETWORK CONVERGENCE – NEXT GENERATION NETWORK PHYSICAL ARCHITECTURE

In this section, we discuss service and network convergence leading to unified Next Generation Network (NGN). Physical NGN architecture with different domains, from access to core supporting multiple services, is described in this paper. A reference to NGN architecture with focus on integrated planning can be found in [4].

2.1. SERVICE AND NETWORK CONVERGENCE

Although broadly Voice, Video, Data, and Messaging have typically been the predominant services used, there have been many applications under these broad categories of services that require different quality of service (QoS) and user experience. For example, as part of video service, broadcast video and video on demand need different QoS. In addition, there is service convergence in the sense that these different services can be supported by a single end user device (e.g., smart phone), rather than dedicated device to support specific service (e.g., TV for broadcast video, telephone for voice call) as in the past. For example, messaging is no longer a simple textual data, but it could be mixed of data and video. Thus, all different services are converging into rich multi-media services in which the user can access those services any time from any place using a single device, and service is no longer limited to a particular type (such as voice, video, or data). Many new innovative service types are also likely to evolve over time, thus necessitating a mixed/rich media communication service. The following Figure 1 depicts the service convergence that has already happened and is also evolving.

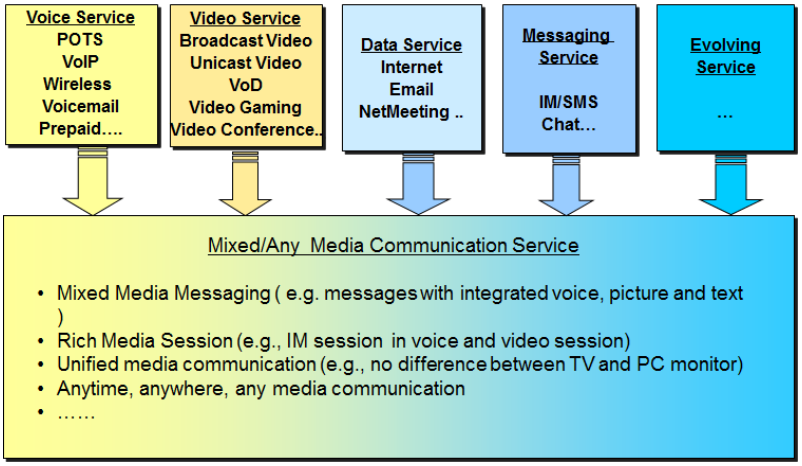

Figure 1. Service Convergence

In the past, the network had evolved and grown in a segmented manner and overlay model was standard. For example, the PSTN network was separate from the data network. SS7 network was also designed as a separate network supporting signaling for PSTN network. As new services grew and technology (e.g., ATM/FR, Optical Ethernet) evolved, new networks were deployed, but mostly in a segmented and segregated manner. It has led to complexity with high OPEX (Operational Expense) and CAPEX (Capital Expense) cost in building and managing communication network.

Service convergence, evolution of technology, Opex and Capex cost savings have led to evolution of a unified next generation architecture of packet based converged network. Different existing and emerging service/applications can be supported over a single network, rather than multiple segmented networks as in the past.

2.2. NEXT GENERATION NETWORK ARCHITECTURE

Figure 2 provides an overview of reference NGN architecture model based Y.2012 recommendation [1]. It is a two-layer model structured with service stratum and transport stratum.

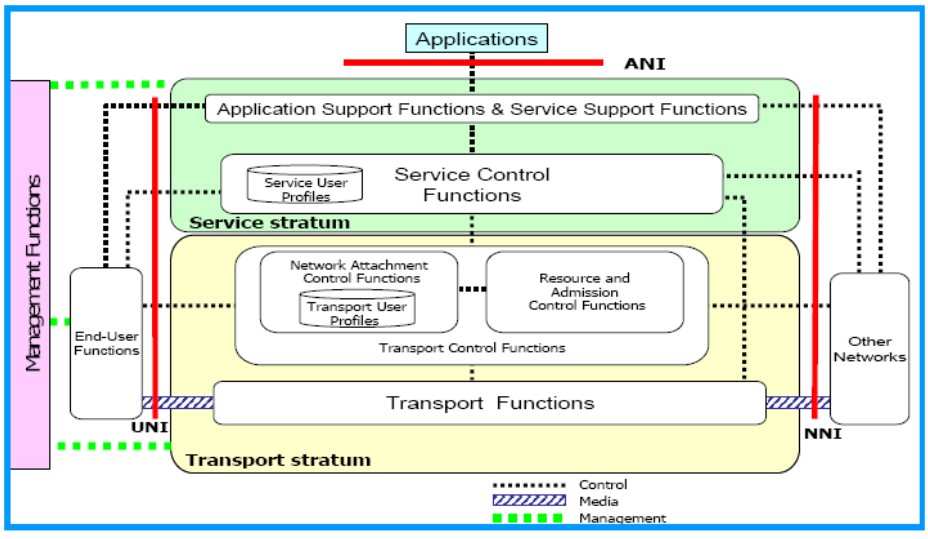

Figure 2. ITU-T Y.2012 NGN Architecture – Reference Model

The service stratum primarily covers application/service support and session control, whereas transport stratum provides flexible transport technology covering access and core network, which enable service delivery in a manner agnostic to service type and its characteristics.

Figure 3 provides an overview of a generic next generation networks architecture [4] with emphasis and extension of transport stratum of ITU-T reference architecture model based on typical deployment scenario by service providers. The Figure 3 architecture provides a physical view of various network elements that cover different domains of NGN.

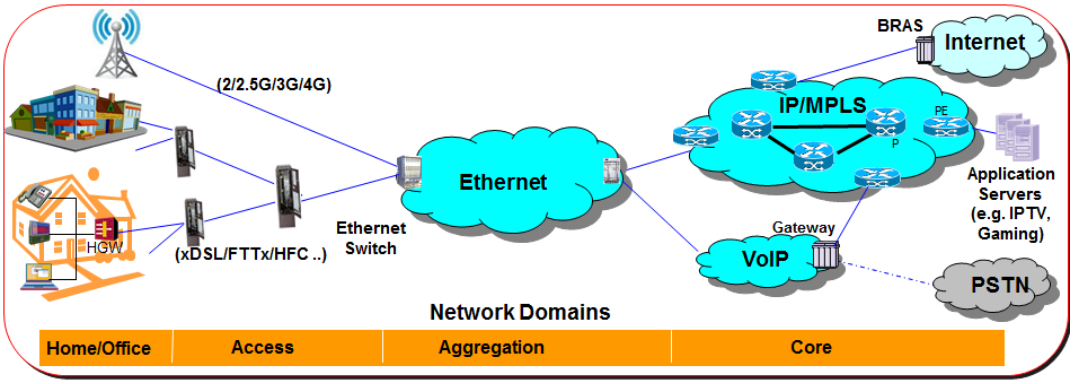

Figure 3. Next Generation Network Architecture

The next generation network is a converged network supporting various domains that span from the home/premises to the core network. The various domains of the next generation network can be organized into:

Home/Enterprise Network: This is the network used by end users such as residential homes, multi-tenant dwelling units (MDU), or business entities/enterprise. Typically, enterprise/business units use LAN internally and use Customer Premise Equipment (CPE) routers that connect to the service provider's network. The LAN could be Ethernet based, wireless based, or hybrid. The residential homes are typically connected via Home Gateway (HGW) to the provider network. Today HGW supports a variety of home networking technologies such as Home Phone Line, Cable, Ethernet, and wireless. Typically, Home/Enterprise network is not within service provider's operational network domain.

Access Network: The access network domain is part of the next generation network that provides the last mile access to home/enterprise network. The access network domain uses various technologies ranging from xDSL (Digital Subscriber Loop), FTTx (including Fiber to the Home (FTTH), Fiber to the Node (FTTN) etc.), and Hybrid Coax Fiber (HFC) to wireless technologies. Access network is part of service provides' network that interconnect private home or enterprise network.

Aggregation Network: The aggregation network domain provides traffic aggregation from the access network and routes the same to the core network of the service provider. ATM and Frame Relay network, although still deployed in this domain, are rapidly declining. Carrier Ethernet has made significant progress in this domain due to many factors such as its low cost and simplicity.

Core Network: There has been significant innovation and technological growth in IP in recent years and MPLS based IP network is primarily deployed in core network domain. The scalability, resiliency and ease of supporting new services on a single core infrastructure are very attractive. It also provides a cost-effective alternative to multiple overlay networks. In addition, IP/MPLS based core infrastructure provides easy interoperability with various existing layer 2 technologies and protocols, such as Ethernet.

3. VIRTUALIZATION OF NEXT GENERATION NETWORK (VNGN)

Network virtualization enables creation of separates logical networks abstracted from the underlying physical network infrastructure. By using network virtualization it is possible to create a single virtual network out of multiple physical networks or multiple virtual networks out of single physical network. This model is referred to as external network virtualization. External network virtualization involves actual network devices that support physical network. Network virtualization can be used within virtual servers creating networks between virtual machines. This model is called internal virtualization, which is purely based on software that can be quite complex. In this paper's reference to network virtualization, we primarily focus on external virtualization.

Network virtualization is not entirely a new concept. Traditionally, network virtualization has been in use for years using virtual Layer 2 and Layer 3 networks over a common physical network infrastructure. Virtual LAN (VLAN) is a Layer 2 construct of network virtualization in a standard carrier Ethernet Network using 801.1q trunking [2] method. Virtual Routing and Forwarding (VRF) is Layer 3 construct of network virtualization where a physical router can support multiple virtual router instances, which maintains its own forwarding table. A Virtual Private Network (VPN) [3] allows private network service over a public or shared infrastructure such as service provider backbone network. There have been various approaches to network virtualization using tunneling, encapsulation, and encryption techniques to create multiple overlay logical networks over a common physical network infrastructure.

In this paper, we discuss evolving network virtualization model using Network Function Virtualization (NFV) and Software Defined Network (SDN) with focus on typical service providers' next generation network (shown in Figure 3). It may be noted that NFV and SDN, though independent, are functionally complementary in supporting network virtualization. NFV and SDN can be deployed independently and also with or without each other. Virtualization is typically performed at the edge of the network, whereas rest of the network remains unchanged.

3.1. NETWORK FUNCTION VIRTUALIZATION (NFV)

Figure 4 depicts reference architecture model of NFV [5]. NFV implements Virtual Network Function (VNF) of Network Elements (e.g., Router, Switch, Mobile Network Nodes such as MME, SGW, PGW, GGSN, SGSN, Home Gateway, AAA server, Firewalls etc.) in software that run on industry standard server hardware and Virtual Machine (VM). A VNF can run over multiple VMs or on a single VM. Physical resource such as computing, storage and connectivity for VNF is supported through the virtualization layer (e.g. hypervisor), which primarily decouples underlying hardware resources. Element Management System (EMS) in the following reference architecture diagram provides typical element management functionality for multiple VNFs, while OSS/BSS refers to service providers' Operation and Business Management System. NFV Management and Orchestration (MANO) function includes: Orchestrator enabling orchestration and management including instantiation and service assurance of VNF. VNF Manager Support lifecycle management of VNF instances, and Virtualized Infrastructure Manager primarily manages and monitors compute, storage and network resources for VNF implementation.

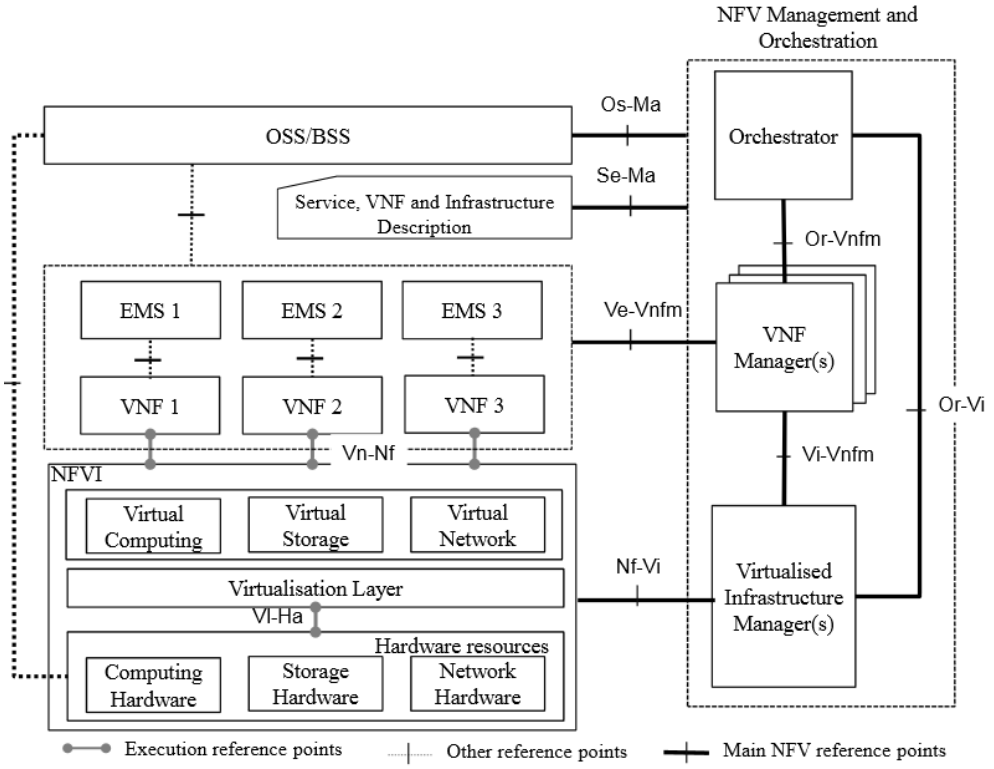

Figure 4. ETSI VNF Reference Architecture

NFV enables flexible creation of network service using VNF instances and VNF Forwarding Graph (VNF-FG) as discussed in section 3.3. NFV enables service providers, high flexibility and faster service deployment including ease of adding new services, thereby reducing Capex/Opex cost, while using industry standard off-the-shelf hardware and software.

3.2. SOFTWARE DEFINED NETWORK (SDN)

Software Defined Networking (SDN), is primarily about decoupling of control plane from the data plane, dealing mostly with the lower layers (L2-L4) function, where network intelligence and state are logically centralized and underlying network infrastructure is separated from applications. Details of SDN architecture as defined by Open Networking Foundation (ONF) can be found in [6].

Figure 5 provides an overview of SDN architecture based on ONF reference model [6]. In the application layer, business applications support various business specific applications such as service provider customer network management portal, content distribution network management, etc. In application layer orchestration system broadly provides network resource orchestration. Business applications run using northbound interface of SDN controller. In control plane, the SDN controller is the key component of SDN architecture. It is logically centralized with a global view and control of network resources as well as service demand. It enables network configuration based on abstract view of specific behavior/functional requirement to support services in vNGN. Network services module support applications like network planning, network analytics, and load balancing, etc. OpenFlow is the standard southbound interface to the data plane defined by Open Networking Foundation (ONF) [6]. The data plane is where OpenFlow enabled network elements reside. The key function of NEs in data plane is traffic forwarding based on rules executed by the SDN controller. Thus these NEs need not possess any proprietary intelligence rather than supporting packet forwarding mechanism as a standard hardware commodity.

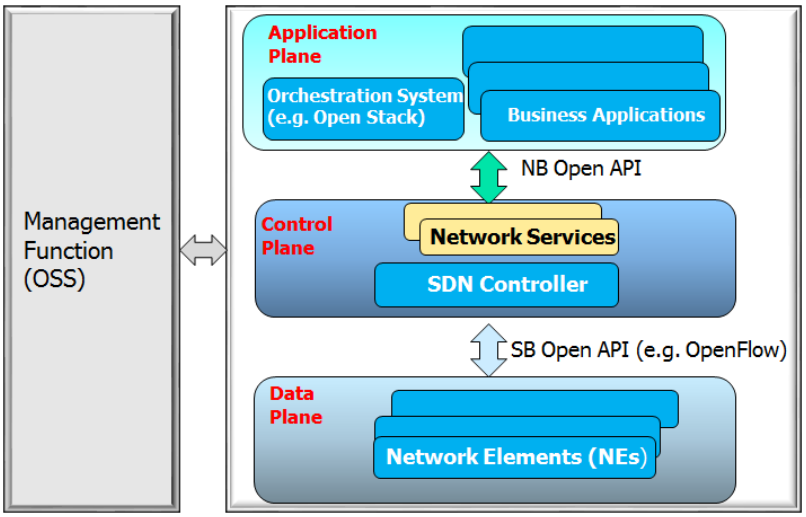

Figure 5. SDN Reference Architecture

3.3. SDN AND VNF WORKING TOGETHER

Functionally SDN and NFV are complementary and synergetic even though each can be deployed in an independent manner. SDN focuses on control and L2-L3 data forwarding, whereas virtualization, intelligent edge device, service chaining is supported by NFV. SDN can be used to interconnect many VNF end points (e.g. vCPE) in NFV platform. Figure 6 shows SDN and VNF working together in an integrated way from architectural perspective. VNF equipment can be dynamically reconfigured based on applications and traffic patterns, whereas SDN controller can steer traffic in network elements. In the scenario where orchestration and the management can be VNFs by itself, the OpenFlow protocol can be part of the Nf-Vi interface or Vn-Nf interface (as shown in Figure 6).

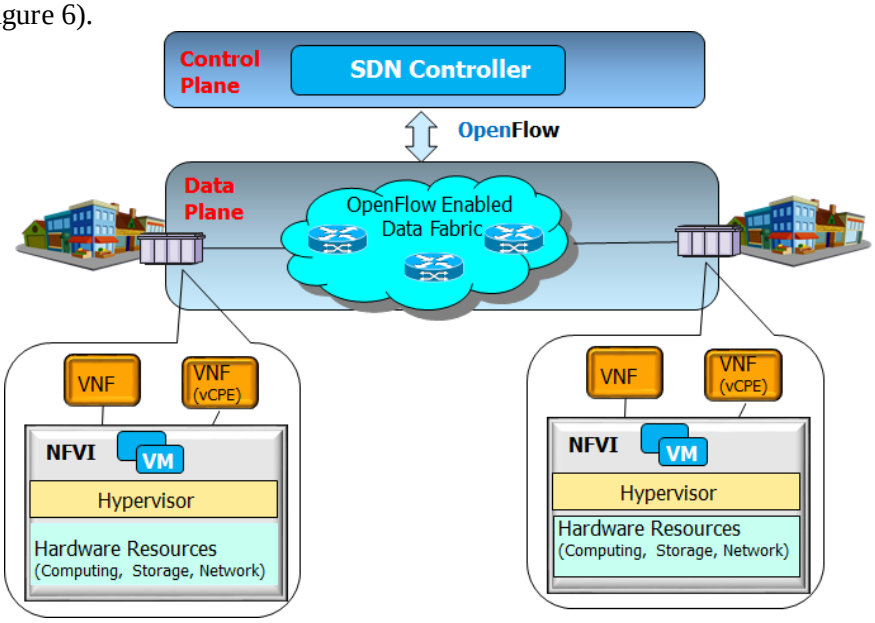

Figure 6. SDN and VNF Architectural Model

One of the key advantages of NFV based platform is the implementation of service chaining using multiple VNFs realizing network service. The Orchestration module can dynamically define set of service using network intelligence of SDN. The concept of service chaining is described in the next section.

3.4. PHYSICAL AND LOGICAL VIEW OF NETWORK & REALIZATION OF NETWORK SERVICE

In a high level, vNGN architecture can be viewed and abstracted into three layers, as depicted in Figure 7. The actual physical network infrastructure constituting network element and their inter-connection (as in Figure 3) can be viewed as physical network resource. Physical network in effect provides virtual network resources. Virtual resources can be isolated from each other unless allowed by security policies. Virtual networks can be viewed as logical constructs of the virtual resources implemented on top of physical network. Each customer of a provider network can have one or more virtual networks.

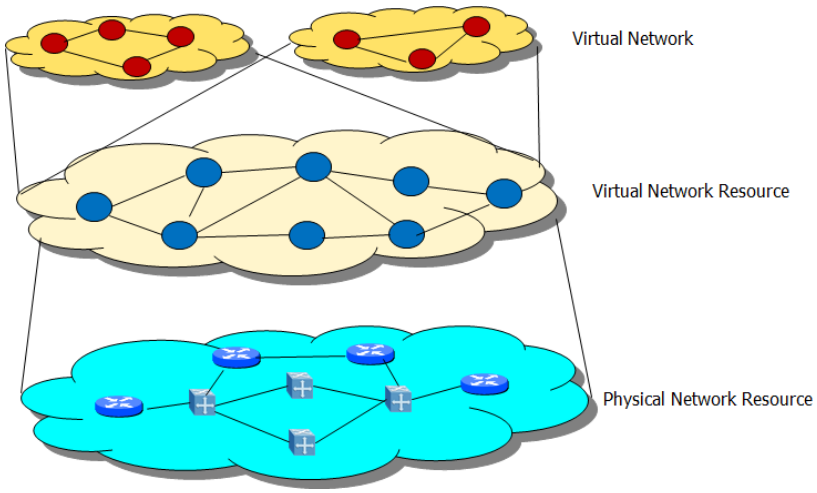

Figure 7. Multi-layer View of vNGN

NFV enables effective management of end-to-end network services utilizing group of VNFs bound together via VNF Forwarding Graph (FG), also known as service chain. Actual realization of end-to-end network service is depicted in Figure 8, as per reference model described in [5].

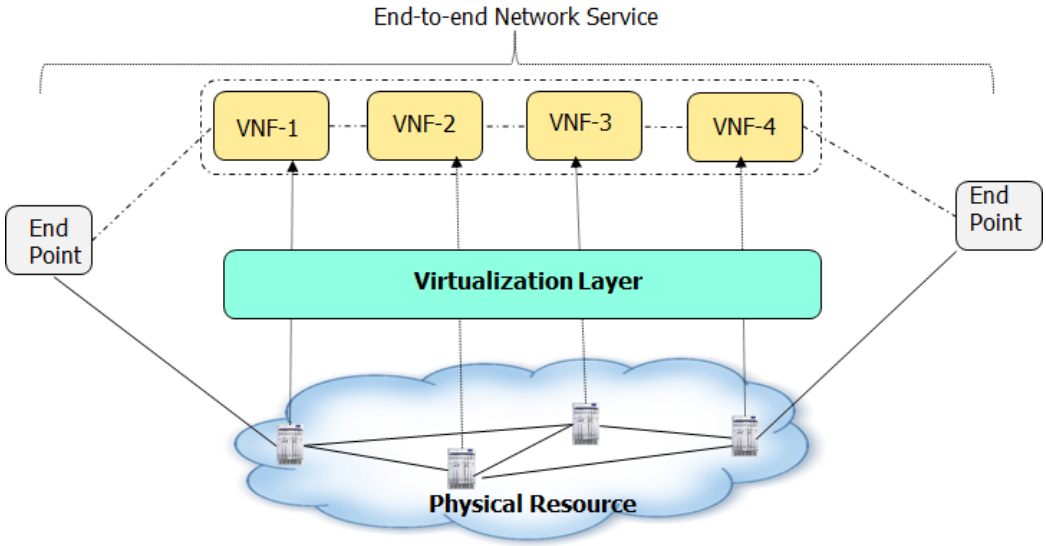

Figure 8. Realization of end-to-end Network Service using VNF and VNF-FG

4. NETWORK VIRTUALIZATION PLANNING AND MANAGEMENT CHALLENGES

There are enormous values and benefits in deploying or migrating to vNGN. Some of the key benefits includes: common infrastructure sharing even among competitors, programmability thus enabling rapid service introduction, high available infrastructure, non-proprietary NEs, and open standard platform leading to significant Capex and Opex savings. However, it has its potential issues and challenges in planning and managing vNGN. In this section we highlight some of the work related to NFV and SDN and issues. We specifically focus on key issues and challenges in planning and managing vNGN. Due considerations must be taken into account related to implementation and deployment of NFV and SDN systems/components, standard compliance, co-existence with existing network infrastructure and OSS/BSS systems, and security aspects.

4.1. RELATED WORKS

Given evolution of network virtualization and current state of ecosystems, paper [8] provides insight to practical issues and guidelines in deploying Network Virtualization and SDN. Paper [7] provides view of network virtualization challenges and describes architectural principles and design goals. Paper [9] addresses resource allocation specific issue in network virtualization. Paper [10] outlines challenges and solutions while implementing network virtualization using OpenFlow. Specific challenges with respect to network performance, scalability, security and interoperability with potential solution while deploying SDN in carrier grade network has been described in paper [11].

4.2. PLANNING VNGN – CHALLENGES

As described above, two key components to achieve network virtualization are NFV and SDN. In addition to standard activities in this area by ETSI, ONF, and IETF, many vendors provide solutions and could have some proprietary aspects in their solution. Also transitioning to vNGN will occur over a period of time along with existence of legacy network. Some key planning challenges and consideration that need to be taken in deploying network virtualization and SDN are enumerated below:

Network Function Virtualization (NFV): The orchestration and management of VNF must be carried out along with legacy network ensuring proper configuration and security. Resiliency, scalability, and performance of hardware and software components associated in implementing NFV must be ensured. Automation is the key to high scalability of NFV. Interoperability with different vendor's virtual appliance and middleware (e.g., hypervisor) needs to be duly considered.

SDN Controller: As SDN controller is the main intelligence behind programmable network, its architecture with respect to scalability, availability, and performance are of key considerations. Its compliance to standards such as ONF [6] shall ensure interoperability.

Network Elements: Service provider network is expected to support Network Elements/Switches from multiple vendors. Protocol support between control plane and data plane is a key aspect. Support of standard OpenFlow enabled Switch is another critical consideration. Hybrid OpenFlow switch or even different version of OpenFlow software support could pose interoperability challenges.

Co-existence with Existing Systems: It is expected that full migration to vNGN will be accomplished over a period of time. So co-existence with existing network infrastructure and OSS/BSS is a key aspect while planning the migration. Maximal reuse and enhancement as applicable to existing network resource and systems has to be considered in order to reduce Capex.

4.3. MANAGING VNGN – CHALLENGES

There are multiple challenges in managing vNGN from OSS/BSS point of view. We highlight below some of the key challenges that network manager faces today in migrating and managing vNGN.

Network Function Virtualization (NFV) Systems Management: NFV enables some core networking function like switching, routing, load balancing, etc. supported by software decoupled from proprietary hardware appliance. NFV is implemented using high capacity physical server, network and storage on standard industry platform in a virtualized environment. The management system needs to support lifecycle management of virtual network functions (VNFs) like initialization, modification, deletion etc. The monitoring of virtual network and its relationship with physical network is also a key management aspect. In addition, the normal service assurance related to server management in a highly scalable and reliable environment needs to be supported for server platform.

SDN System Management: SDN controller and network service functions are expected to be supported on standard open platform such as Open DayLight and protocols such as OpenFlow. As SDN is the main intelligence behind implementing vNGN, management system has to support key operational aspect in monitoring such as fault, performance, capacity of the SDN system in real-time ensuring high availability of the system. It is also expected that SDN shall perform many of the actions specifically related to network configuration and routing that is typically performed by management systems today. Traditional OSS is expected to support limited functionality with deployment of SDN controller and OpenFlow enabled network appliances.

Visualization: Complete visualization of network resource including virtual and physical components in the network is a very key requirement for network operation point of view. Visualization component (GUI) of management system must provide end-to-end visualization of virtual network, physical network resource, and drilldown to specific resource to visualize detail state of the resource.

Security Management: One of the key aspects is that platform and system implementing NFV and SDN to be fully secured for the detection and mitigation of DDoS attacks. In addition, management system shall support security aspects related to access management, authentication, data confidentiality, and secured communication at various interfaces. A good reference to telecommunication security and security for network management application can be found in [13].

Co-existence/Integration with Existing OSS/BSS System: Even though OpenFlow enabled switches are expected to be deployed in the network to take full advantage of SDN controller, the traditional network will be there for a foreseeable future. The management system must enable management of both SDN and non-SDN components of the network in an integrated fashion, simultaneously leveraging existing OSS/BSS assets in order to reduce Capex.

5. AN ARCHITECTURAL SOLUTION FOR MANAGING VNGN

Figure 9 below provides an overall architectural model with key building blocks in support of effective management of vNGN. The proposed vNGN management solution architecture uses component-based model. Various components can be added, updated and/or removed in a plug and play mechanism within the overall solution frame work. Similarly sub-components within a component can be easily added and/or removed in an independent manner without impacting functional aspects of component itself. In this paper we provide a brief context of the solution architecture, its components, and sub-components and mainly focus on details of management aspects in meeting the challenges and issues, as outlined in previous sections. The specific contribution of this paper is the solution model in managing evolving vNGN in a cost effective and efficient manner while leveraging typical OSS/BSS assets that may exist in service providers' operation center. The solution model also specifically addresses the key issue of network management challenges.

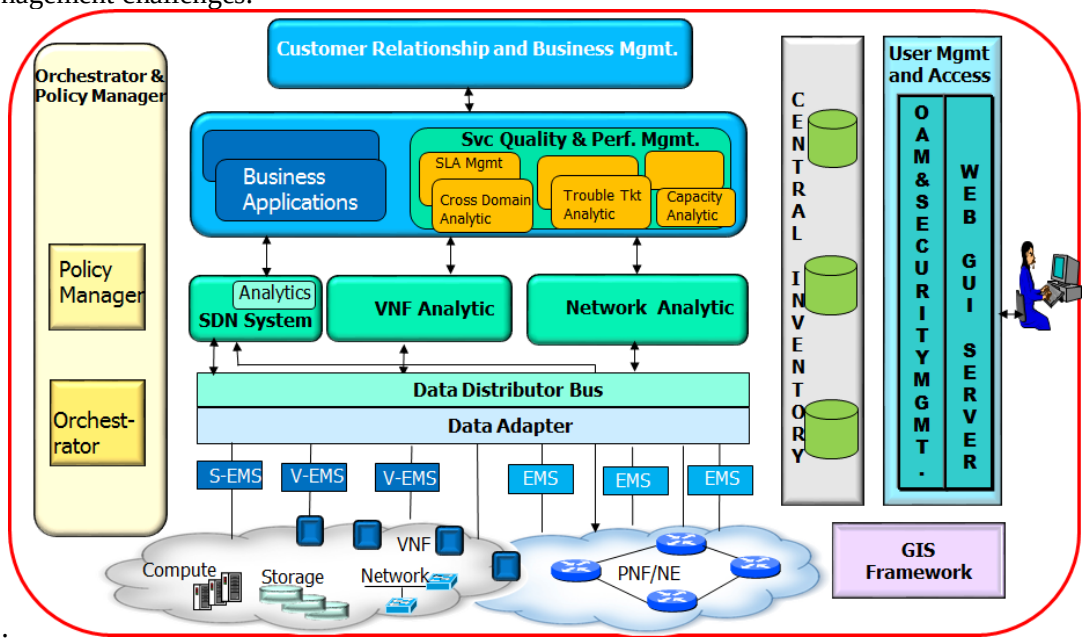

Figure 9. High Level View of Management Solution Architecture for vNGN

5.1. BRIEF OVERVIEW OF SOLUTION ARCHITECTURE COMPONENTS

In Figure 9, the infrastructure layer constitutes physical network resource/Network Elements (NE) termed as Physical Network Function (PNF), which primarily constitute data plane carrying user service traffic. The network elements could be OpenFlow enabled or non-OpenFlow enabled. The other infrastructure constitutes compute, storage and network resource along with virtualizer (e.g., hypervisor) to support NFV capability. Same server platform can also be utilized for SDN system. This paper does not focus on specific implementation aspects and inter-component communication mechanism, as the same can be realized using many existing common off-the-shelf (COTS) platform and protocols. However, we refer to standard open platform and protocols for implementation of various components, as applicable. Also, the existing system in OSS/BSS domain in service provider's operation center must be leveraged in order to reduce Capex and enable ease of use by existing personnel without significant training with new products. Various building blocks for network management systems have been discussed below:

Element Management System (EMS): The EMS layer has typical EMS functionality in supporting both legacy network elements as well as VNF. Typically, EMS supports one or more NEs of same type and have functionality for configuration and retrieval/receipt of performance metrics (e.g., trap, performance counters) of the NEs under its domain. The EMS supporting VNFs are noted as V-EMS. The functionality of V-EMS is similar to EMS modules supporting VNFs as defined in [5]. S-EMS in the architecture refers to server infrastructure management system at EMS layer.

Data Adapter and Data Distribution Bus: Data Adapter enables the receipt of various infrastructure layer configuration information and performance metrics from multiple EMS, which could be using different north-bound API/interfaces. Also Data Adapter supports standard south bound API (e.g. SNMP) for direct communication with NEs in infrastructure layer, which may not have any EMS support. Data distribution bus enables the distribution of collected virtual and physical network data to other modules in upper layer. Data distribution can be implemented using pull-push and/or subscription based mechanism, as needed.

Orchestrator and Policy Manager: Orchestrator broadly provides functionality for network resource orchestration as means for delivering business request. Orchestrator creates and tracks the process for implementation of a business request such as creation a virtual network for a tenant across the service provider network, and apply security policy to a group of VMs at the edge of tenant's virtual network. Orchestrator is typically deployed using open standard platform OpenSatck and OpenCloud.

At infrastructure layer, Orchestrator provides resource reservation and allocation for virtualized resource. It also provides virtual resource configuration information to VNF manager so that VNF can be configured appropriately to function within VNF FG in support of network service. Orchestrator supports VNF life cycle management in exchanging information related to VNF inventory, state, data, capacity, usage and accounting information with OSS/BSS [5]. Orchestrator module works in with VNF analytic component module (as describe below) in this architecture. Using event based service, virtual resource data can be synchronized between Orchestrator and Central Inventory Management (CIM) system, as described below.

Policy Manager primarily manages business, service, and network policies and initiates control or orchestration service as appropriate.

SDN System: SDN is implemented as logically centralized but on physically distributed platform in open source cloud environment. SDN is typically supported on Open DayLight - a standard open platform. The south bound interface is based on OpenFlow, which shall manage OpenFlow enabled devices in network infrastructure layer. The north-bound interface could be based on Representational State Transfer (REST) Application Programming Interface (API) [14] for interworking with business applications and orchestration system. REST API can also be used for interfacing traditional OSS/BSS components supporting integration. The physical server management for SDN can be supported by COTS server management systems and tools such as Chef and Solarwinds.

SDN controller is responsible for translating request at high level of abstraction into clear action on physical and virtual network appliances such as setup of virtual services like virtual firewall in a VM and also use underlying physical firewall service node.

Analytic sub-components of SDN system are responsible for collecting, analyzing, and presenting network managers on SDN platform fault, performance, capacity and availability aspects in near real-time. This enables management of SDN system, including testing and troubleshooting in case of failure and performance degradation of SDN system.

NFV Analytics: NFV analytics is the component supporting management of NFV infrastructure (server, storage, computing), virtualizer, VMs and VNFs resources dedicated to realization of NFV. NFV analytics receive data from V-EMS via Data Distributor. It supports collection, analysis and visualization of fault, performance, capacity, optimization and other data related to operation, management and monitoring of NFV resources and function in the network. This component also supports management of VNF life cycle such as initialization, update, termination and scaling (up/down) of VNF instances. NFV Analytics is compliant with functionality of Virtualized Infrastructure Manager and VNF Manager(s) as defined in [5].

Network Analytics: Network Analytics supports typical Network Management Systems (NMS) layer functionality for traditional network elements. It supports network resource management, configuration, and network wide path computation in support of service provisioning. It also supports collection, analysis, and collation of network testing, performance, fault, alarm correlation, capacity related data to enable effective network operation and troubleshooting. With support of SDN enabled data fabric in the network, it is expected that majority of network configuration and routing shall be managed by SDN controller.

Business Applications: Business applications support various business specific functions and requirements in supporting applications such as customer network management portals in compliant with application layer of SDN architecture as defined in [6].

Service Quality and Performance Management*:* Service Quality and Performance Management component provides service level network analytics and service quality management. It includes extensible sub-components, which can be used in plug and play model. Some of the subcomponents includes:

- **Cross Domain Analytics:** Provides customer service issues and identification of problem related to specific domain or part of the network including partner or 3rd party hosted network.
- **Trouble Ticket Analytics:** It correlates network level fault with services and identifies specific customer service impact and resolution of same.
- **SLA Management:** This sub-component provides analysis related to contracted service quality with a customer and actual service quality rendered and enforcement of Service Level Agreement (SLA).
- **Capacity Analytics:** This sub-component provides capacity constraint specific issues in support of existing customer service such as VPNs. It also supports cross-domain network capacity analysis in support of various services.

Central Inventory Management: Central Inventory Management (CIM) is a very key component in the vNGN management system architecture frame work. The CIM captures inventory data in various layers/levels which is used by other components in realizing their functions. In addition, data store in this component can be used as "Big Data" in support of different analytics and service intelligence applications.

Inventory component in infrastructure layer include physical as well as logical/virtual resources. The physical resources includes various NEs (Routers, Switches), Mobile Network Elements (HLR/HSS, SGSN/GGSN, RNC, SGW/PGW, (e)NodeB ...), NGN signaling node (e.g., SBC), and Server hardware platform. Similarly virtual network component could include VMs and software defined virtual functions for physical components such as vCPE, vSwitch, and vRouters. The CIM component at infrastructure layer contains information on all physical and virtual resources, interconnectivity, properties and states.

In network layer, CIM shall store information related to various network path provisioned in the network, network resources involved (e.g., NE/Port) and their interconnectivity. CIM also contains information of service association with provisioned network path. At business/application layer, CIM is the central repository for various product/portfolio that is supported by service provider.

The information stored in CIM can be used by multiple components. For example, Network Analytic component can use inventory information from CIM and associate a network failure information received from EMS to identify root cause of network failure. Similarly, at service layer using network path and service association, any network failure can be correlated to specific customer service impact by trouble ticket analytic component. As CIM provides a network wide view, resource, and service information; the repository could be used by various analytic applications to gain various intelligence and information for effective use of network resource, service and enabling revenue growth.

In addition, information on physical resource can be used by GIS framework component in providing physical location of network resources. Similarly Web GUI component can utilize information stored in CIM for network wide visualization functionality.

Customer Relationship and Business Management: The customer relationship and business management component shall support customer facing and business management specific functionality. Customers could include retail as well as business customers. The functionality supported in this module shall include customer profile, customer service order, service order realization and tracking, and customer billing etc.

User Management: The user management includes OAM and Security Management that supports user administration, authentication, authorization, auditing, and secured communication etc. [12, 13] for operation personnel. The Web GUI Server provides web-based access to management system from client workstation.

Geographical Information System (GIS) Framework: This component enables various modules to use geo-spatial information and provide network manager with GIS based visualization of infrastructure layer covering NEs, their interconnectivity and Server platform location.

5.2. MEETING THE KEY MANAGEMENT CHALLENGES

NFV Management: Orchestrator, NFV analytics, V-EMS components provides full support and management of NFV capability. NFV analytics support real-time monitoring and management associated with NFV resource and infrastructure. Orchestrator component along with CIM support virtual network and its relationship with physical network. Correlation functionality in Network Analytic component along with GUI provide appropriate monitoring and end-to-end visualization capability in support of NFV management.

SDN System Management: SDN system along with other components provides effective management and support of SDN functionality in overall architectural framework. The analytics in SDN system shall support real-time monitoring and management of SDN resource. Open platform and standard API supports integration of SDN system into existing OSS/BSS infrastructure of service provider.

Visualization: Web server based GUI component provides end-to-end network visualization including physical as well as virtual resources in concert with GIS framework, Central Inventory Management (CIM) and various analytic modules. Leveraging the relationship information between physical and virtual resources as stored in CIM will help GUI component in visualizing detail network service realization along with associated physical and virtual resources.

Security: OA&M and Security Management component provides secured user access and system management. The Open DayLight consortium's SDN controller contains toolset that can be used for the detection and mitigation of DDoS attacks as well.

Integration with existing OSS/BSS Systems: The architecture as proposed in section 5.1 above enables migration/enhancement of existing OSS/BSS supporting SDN & NFV while using existing assets. The Element Management, Network Layer & Service Layer model of management principle fit well with existing OSS/BSS embedded base. Well defined standard interfaces and model enables easy add-on of NFV and SDN capability into existing operation and management model.

6. CONCLUSIONS

This paper provides an overview of next generation networks architecture reference model, focused on transport stratum. Various domains of physical architecture of next generation networks have been discussed. A detail view of network virtualization, software defined network and associated key components are discussed. The evolution and deployment of vNGN poses multiple challenges for network planners and mangers, and key issues must be taken into consideration in effective planning and management of vNGN is also highlighted. This paper focuses on managing vNGN with a reference network management solution architecture for deployment of virtualized next generation networks. Future work expected to address some of the other key challenges and issue in deployment of vNGN.

REFERENCES

[1] ITU-T Y.2012, "Recommendation ITU-T Y.2012", Functional requirements and architecture of the NGN, 2006.

[2] IEEE, 802.1Q – IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks, 2014

[3] Madhulika Bhandure, Gaurang Desmukh, Saili Waichal, and Varshpriya JN, "Approach to build MPLS VPN using QoS Capabilities", International Journal of Engineering Research and Development, Vol 7, Issue 8, PP. 22-32, June 2013.

[4] Sukant K. Mohapatra, "Integrated Planning for Next Generation Network", IFIP/IEEE International Symposium on Integrated Network Management, 2009.

[5] ETSI, Network Function Virtualization Architectural Frame Work, ETSI, GS NVF, 2013, http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf

[6] ONF, "Open Network Foundation, SDN Architecture", ONF TR 502, 2014, https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf

[7] N.M Mosharaf, Kabir Choudhury and Raouf Boutaba, "Network Virtualization: State of the Art and Research Challenges", IEEE Communication Magazine, 2009

[8] Jim Metzler, Aston Metzler and Associated, "The 2013 Guide to Network Virtualization and SDN", 2013, http://www.webtorials.com/content/2014/01/2013-guide-to-network-virtualization-sdn-3.html

[9] Aun Haider, Richard Potter, and Akihiro Nakao, "Challenges in Resource Allocation in Network Virtualization", 20th ITC Specialist Seminar, 2009.

[10] Martias J, Tornero B, Mendola A, Jacob E, Toledo N, "Implementing Layer 2 Network virtualization using OpenFlow: Challenges and Solutions, 2012 European Workshop on Software Defined Networking (EWSDN), 2012.

[11] Sakir Sezer, Sandra Scott-Hayward, Puspinder Kaur Chouhan, Barbara Fraser, David Lake, Jim Finnegan, Neil Vijoen, Marc Miller, and Navneet Rao, "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks", IEEE Communications Magazine, Vol 51, No. 7, July 2013.

[12] ITU-T, "Security in Telecommunication and Information Technology - An overview of issues and deployment of existing ITU-T Recommendation for secure telecommunications", 2003, http://www.itu.int/itudoc/itu-t/85097.pdf

[13] Telcordia, "GR-815-CORE Generic requirements for Network Element/Network System (NE/NS) Security," Issue 2, March 2002.
[14] Richardson, Leonard; Mike Amundsen, "RESTful web API", O'Reilly Media, ISBN 978-1-449-35806-8 , 2013

AUTHORS

Sukant K. Mohapatra has a Ph.D in Computer Science with specialization in Telecommunications from Stevens Institute of Technology, New Jersey. His research interest includes: Next Generation Fixed and Mobile Network Architecture, Software Defined Network, Cloud Computing, Network Planning, and Network Management. He has worked over twenty five years in telecommunication industry in leadership capacity. He is recipient of DMTS award in Bell Laboratories and a senior member of IEEE. He is the founder chairman of National Institute of Science and Technology (NIST), India.

Jay N. Bhuyan is a professor in the Department of Computer Science at Tuskegee University. His research and teaching interests include Telecom Software Architecture and Development, Software and Network Security, Big Data Analytics, and Parallel & Distributed Computing. He received a PhD in Computer Science from the University of Louisiana at Lafayette. He has over 25 years of full-time and part-time teaching experience as well as over 15 years of research and development experience in the Telecom industry. He is a member of IEEE and IEEE Computer Societies.

Hira N. Narang is the department chair and a professor in the Department of Computer Science at Tuskegee University. His research and teaching interests include High Performance Computing, Information Systems Security, and Computer Networks. He received a PhD in Applied Mathematics from the Delhi University, India, Master in Computer Science from University of Kentucky, and a Master in Computer Engineering from Auburn University. He has over 30 years of teaching experience as well as over five years of research and development experience in the industry. He is a recipient of several research & infrastructure grants from NSF, NASA, Xerox, HP, etc.