Evolving IP/MPLS network in order to meet 5G requirements

Irena Šeremet, Samir Čaušević
Communication Technology
Faculty for traffic and communication
Sarajevo, Bosna I Hercegovina
Irena.seremet.1@gmail.com , Samir.causevic@gmail.com

Abstract—**5G will bring many new services and demands enabling advances in Internet of Things, Smart Cities, Artificial Intelligence, Virtual Reality, Self-driving cars etc. To enable all these use cases, several changes in RAN, network IP core and user end devices will be applied. This paper is focused on IP packet data networking in core and directions of development in order to meet 5G requirements. IP/MPLS network, as a core network in ISP networks, will have to adapt and adopt new technologies. This paper presents a short overview of 5G networks and how new technologies such as SDN, NFV, SD-WAN and Network Slicing will impact and change IP/MPLS network.**

Key words: 5G, IP/MPLS, SDN, NFV, SD-WAN, Network Slicing

I. INTRODUCTION

Fifth generation of cellular mobile networks will introduce many services, technologies and implementations. Cisco VNI Global Mobile Data Forecast, 2016–2021 [1] predicts that by the 2021, global mobile data traffic will reach 49 exabytes per month, or a run rate of 587 exabytes annually. Ericsson [2] predicts total mobile data traffic forecast to rise at a compound annual growth rate of 39 percent, reaching 107 exabytes (EB) per month by the end of 2023. Also, [2] states that it is expected that 20 percent of mobile data traffic worldwide will be carried by 5G networks. 5G will enable crucial advances in Internet of Things, Artificial Intelligence, Virtual Reality, Self-driving cars etc. By the [3], aim of 5G system is responding to the widest spectrum of services and applications in the history of mobile and wireless communications categorized in (i) enhanced mobile broadband (eMBB), (ii) ultra-reliable and low-latency communications (URLLC) and (iii) massive machine-type communications (mMTC). Also, 5G system aims to provide an efficient platform enabling new business cases and models integrating vertical industries, such as automotive, manufacturing, energy, eHealth, and entertainment. In [4] are presented key challenges for the 5G Infrastructure PPP such as providing 1000 times higher wireless area capacity and more varied service capabilities compared to 2010, saving up to 90% of energy per service provided, reducing the average service creation time cycle from 90 hours to 90 minutes, creating a secure, reliable and dependable Internet with a "zero perceived" downtime for services provision, facilitating very dense deployments of wireless communication links to connect over 7 trillion wireless devices serving over 7 billion people and ensuring for everyone and everywhere the access to a wider panel of services and applications at lower cost. Authors in [5] state three basic engineering requirements for 5G: a) *Data rate*; b) *Latency*; c) *Energy and Cost:* As we move to 5G, costs and energy consumption will, ideally, decrease, but at least they should not increase on a per-link basis. 5G-PPP document [6] provides an overview of the use cases and models that were developed for an early evaluation of different 5G radio access network concepts and can be classified into six families: Dense urban, Broadband (50+ Mbps) everywhere, Connected vehicles, Future smart offices, Low bandwidth IoT, Tactile internet/automation. To enable all these use cases, several changes in radio access network - RAN and core will be applied. In [3] it is defined new 5G architecture. Also, new types of frequency bands like micro and millimeter waves are expected to be used. These will make small cells even smaller and denser than in current setups. [3] But how will IP/MPLS backbone network have to change in order to serve all these 5G changes and requirements? In this paper it will be explored how 5G will impact IP/MPLS network. In section II, we will present an overview of IP/MPLS networks and in section III main features that IP/MPLS should support for 5G. In section IV we will present framework of the new IP/MPLS network with new technologies and services enabling 5G requirements. We will conclude our paper in section V.

II. IP/MPLS NETWORK

Multiprotocol Label Switching is a protocol-agnostic technique designed to direct data from source to destination based on labels rather than IP prefixes. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made on the contents of assigned label, without the need to open and examine the packet. Routers in an MPLS network exchange using label distribution protocol (LDP) and standardized procedures in order to build a complete picture of the network. When an unlabeled packet enters IP/MPLS network, the ingress router inserts one or more labels in the packet's newly created MPLS header. The packet is then passed on to the next hop router. When a labeled packet is received by an MPLS router, the top label is examined. Based on the contents of the label a swap, push or pop operation is performed. [7] Transit routers typically need only to examine the topmost label on the stack. At the egress router, when the last label has been popped, only the payload remains.[7] One of the key features that MPLS support

are traffic engineering, Virtual Routing and Forwarding - VRFs and L2/L3 VPNs. Traffic engineering enables ISPs to route network traffic to offer the best service to their users in terms of throughput and delay. By making the service provider more efficient, traffic engineering reduces the cost of the network. MPLS traffic engineering, using Resource Reservation Protocol RSVP, automatically establishes and maintains Label-switched Paths -LSPs across the backbone. The path used by a given LSP at any point in time is determined based on the LSP resource requirements and network resources, such as bandwidth. [8] MPLS VPN is a family of methods for using multiprotocol label switching (MPLS) to create virtual private networks (VPNs) which can be (i) point-to-point (ii) Layer 2 (iii) Layer 3. [9] A VRF instance consists of one or more routing tables, a derived forwarding table, the interfaces that use the forwarding table, and the policies and routing protocols that determine what goes into the forwarding table. Because each instance is configured for a particular VPN, each VPN has separate tables, rules, and policies that control its operation. [10] MPLS as a technique is very flexible, adaptive and scales very quickly. With IP/MPLS, the paths between end-points are dynamic and extremely resilient to failures; IP/MPLS will find a path as long as one exists, regardless of the number and locations of failures in the network. [11] LSPs from source to destination are pre-determined so devices in LSP don't have to make decision on every hop. This allows faster data transfer and less load for routers. MPLS allows ability to control and manage QoS on the label level. In spite of the many advantages of MPLS, the development of new technologies results in different needs and requirements of end users. New technologies introduce more services which will call for significant changes in IP/MPLS networks to meet low latency, reliability and connectivity requirements. Networks of fifth generation will have many new services with many different new requirements. IP/MPLS network will have to go in the direction of virtualization, network programmability, cloud-native principles and granular slicing of network on a per-tenant and per-service level. Below we will discuss the new directions of the development of the IP/MPLS network in order to meet the requirements of 5G networks.

III NEW DIRECTIONS OF THE IP/MPLS NETWORK DEVELOPMENT IN ORDER TO MEET 5G REQUIREMENTS

As mentioned before, 5G will introduce new flexible platform enabling new business cases, models and services such as autonomous vehicles, Internet of Things (IoT), Virtual Reality etc. In this chapter a new direction for the development of the IP/MPLS network will be presented to meet the requirements of 5G. IP/MPLS will have to develop in the direction of virtualization, programmability, cloud networking, and network slicing. Some key discussed technologies and are: Network Programmability, Software Defined Network-SDN, Network Function Virtualization-NFV, Software Defined Wide Area Network-SD-WAN, Segment Routing-SR and Network Slicing-NS.

A. Network Programmability

Cisco [12] defined programmability-enabled network as a network driven by intelligent software that can deal with a single node or a group of nodes using programming interfaces-APIs, which serve as the interface to the device or controller in order to gather data or intelligently build configurations. The idea of programing the networks has been created back in 1988 with SOFTNET [13], where network nodes have been reprogrammed to provide new user services during normal operation. In 1990s OpenSignaling [14], Active Networking [15], GSMP [16] were introduced. As explained in [17], core of these proposal was to provide access to the network hardware via open, programmable network interface which would allow the deployment of new services through a distributed programming environment. In 2006 NETCONF [18], protocol for installing, manipulating and deleting the configuration of network devices was introduced. Introducing NETCONF was the beginning of modern and more intelligent network programming. In 2006, project Ethane [19] set the foundation for what would become SDN. Also, in 2006 SANE [20] presented logical server that performed all routing and access control decisions. More detailed historical overview of network programmability was presented in [17] and [21].

B. Software Defined Network-SDN

Software Defined Networking (SDN) is an architecture which decouples control plane and data plane achieving flexible and intelligent networks. The SDN provides programmability of a control plane and automation of configurations through a centralized controller and open APIs. Network operators can implement their own protocols, rules and policies with common programming languages achieving flexible control over network services such as routing, traffic engineering, QOS and security. [21] SDN architecture consists of 3 layers: (i) infrastructure layer which represents physical routers and switches; (ii) control layer which is centralized controller responsible for managing devices in infrastructure layer and (iii) application layer with applications interacting with lower layers. Applications communicate with controller through northbound interfaces or APIs and controller communicates with infrastructure devices through southbound interfaces such as OpenFlow, Netflow, Netconf, BGP-LS/PCEP etc. Authors in [22] mentioned many SDN network designs [23], [19], [24], [25], on the security area [26], [27], [28], optimizations for the transmission medium [29] [30], traffic engineering [31], multicasting [32]. Moving from IP/MPLS to SDN should be gradual and well thought out. Before migration, organizations should educate themselves, understand how SDN can help or damage their network, determine which functionalities are needed from an SDN controller and consider impact on existing network. Also it is needed to determine how big is the gap between current IP/MPLS network and new SDN solution. Authors in [33], [34], [35] researched Hybrid SDN. Authors in [36] presented scheme called Zeppelin which builds upon MPLS using MPLS for packet tagging and a centralized control plane with OpenFlow as the SDN control protocol for setting up flow state on the switches. IP/MPLS network is a good foundation network for implementing SDN solutions.

C. Software Defined Wide Area Network SD-WAN

SD-WAN is a concept of implementing SDN to WAN connections such as broadband internet, 4G, LTE, or MPLS. SD-WAN is managed by a centralized controller and uses SDN to automatically determine the best route between two sites. Also it has the ability to monitor links and if needed, dynamically route traffic to links with enough bandwidth for each application's demand. In [37] authors highlighted main challenges in designing SD-WAN system which concerns placing controllers, failure resiliency and scale-out behavior in decentralized controller architecture and updating data plane in large networks. In the security area, authors in [38] presented main threats in SD-WAN which related to NFV, management, orchestration, cryptography threats etc. Authors in [39] and [40] presented B4, Google's private cross-planet WAN connecting Google's data centers. There are many advantages of using SDN in wide area networks considering higher flexibility, security, speed, network visibility and reducing costs.

D. Network Function Virtualization-NFV

The concept of NFV [41] allows creating logical segments of network functions stored on servers and virtual machines instead of physical purpose-built hardware. Network virtualization treats all network's logical components and services as a single pool of resources that can be accessed without regard for its physical location providing flexible provisioning, deployment, and centralized management of virtual network functions. [42] There are three basic components of virtualized platforms with NFV: (i) physical server (ii) hypervisor which provides the virtual environment (iii) guest virtual machine which emulates the physical network functionalities. Authors in [42] explain how through NFV, SDN is able to create a virtual service environment dynamically for a specific type of service chain. Virtualized network functions are basic element which compose the service chain. A lot of different network elements and functions can be running in virtual environment: firewalls, load-balancers, routers, NAT, IDS/IPS, HLR, RNC, IPsec/SSL virtual private network gateways etc. A lot of research has been done in the field of virtualizing network functions [43], [44], [45], [46].

E. Segment Routing – SR

Segment Routing is a new concept of routing where routing paths are divided into segments in order to enable better network utilization. IETF in [47] describes segment routing as a source based routing where node steers a packet through a controlled set of instructions, called segments, by prepending the packet with an SR header. The headend node steers a flow into a Segment Routing Policy which is detailed in [48]. Segments in SR can be topological or service instruction. For example, one segment can instruct a node to forward traffic through a certain outgoing port, or segment can be associated with a specific QoS or security policy. SR architecture [49] supports three types of control plane: (i) distributed, where segments are allocated and signaled by routing protocols like OSPF or BGP; (ii) centralized, where SR controller decides which nodes need to steer which packet on which source-routed policies; (iii) hybrid where distributed control plane is combined with a centralized controller. Segment routing architecture can be directly applied to the MPLS data plane with no change in MPLS forwarding plane [50] [51]. When SR is used over MPLS architecture, segment IDs are an MPLS label and traditional push, pop and swap actions are applied by the routers on the path. In [49] behaviors associated with SR over MPLS data plane are explained. Authors in [52] reviewed mapping of the SR operations to MPLS label operation, which is presented in Table I.

Some experimental demonstrations of SDN segment routing are presented in [53] and [54]. Also, authors in [53] demonstrated IP/MPLS network and SR controller as a new extended version of a Path Computation Element - PCE solution.

Table I SR OPERATIONS MAPPING TO MPLS LABEL OPERATIONS [52]

Segment Routing	**MPLS**
SR Header	Label Stack
Active Segment	Topmost Label
PUSH Operation	Label Push
NEXT Operation	Label Pop
CONTINUE Operation	Label Swap

F. Network Slicing – NS

Network slicing allows multiple virtual networks with different network demands to share a single physical infrastructure. Network slicing will enable many new use cases in the future such as AR/VR, smart cities, vehicle-to-everything V2X etc. 3GPP [55] has defined a network slice to be a logical network that provides specific network capabilities and network characteristics. Network slicing enables the operator to create networks customized to provide optimized solutions for different market scenarios which demands diverse requirements, e.g. in the areas of functionality, performance and isolation. NGMN [56] has defined network slicing instance as a set of network functions, a resources to run these network functions, forming a complete instantiated logical network to meet certain network characteristics required by the Service Instance. 5G network slicing can be implemented in different parts of the network including slicing the 5G radio access network (RAN), packet core network, and end-user devices. There are many papers on 5G RAN network slicing [57] [58] [59] [60] [61] [62]. In the core network, IP/MPLS network can be the bearer of network slices. In order to be bearer of slices, IP/MPLS network needs to provide basic mechanisms of virtualization, isolation of slices, security, QoS etc. Authors in [63] analyze requirements of network slicing on IP/MPLS networks and identify the potential gaps between the existing mechanisms and the network slicing requirements. As a way to provide virtualization in IP/MPLS networks, [64] suggests reusing existing VPN technologies with some enhancements from the newly developed technologies such as SDN, NFV to meet the network

slicing requirements. Each network slice presents particular service requirement with necessary QoS parameters such as bandwidth, latency, jitter, packet loss etc. and certain level of security. Between these slices there has to be different degree of isolation. Isolation is required in control and data plane for each slice. In current IP/MPLS networks, VPNs are competing for the same resources so the isolation is only partial. In order to support more demanding service requirements in 5G, IP/MPLS network has to provide higher level of isolation using new, enhanced technologies such as SDN and NFV.

IV EVOLVED IP/MPLS FRAMEWORK

In this section will be presented framework of service provider IP/MPLS network which is extended with new required technologies in order to meet 5G service demands. Framework is presented in the Fig1. This framework contains IP/MPLS routers connected with 10 or 100 Gigabit links, SDN controller and data center with certain virtual network elements. Most service provider IP/MPLS networks consist of devices from different vendors, so only vendor agnostic solutions are acceptable. Current IP/MPLS devices do not support the OpenFlow protocol, so as a southbound protocol between devices and controller NETCONF is used. The controller is located on a virtual machine and manages the entire network. The controller, as well as other devices in the network, supports Segment Routing. Services provided by a service provider can be internal, services provided to resident users, and services provided to business users. Each of these services can be divided into special network slices based on the type of traffic, required level of availability, delay, security etc. Various network slices are associated with certain segments and can be routed differently with Segment Routing. ISPs can offer Network Slicing as a service to customers. Datacenters contain virtual machines where network elements such as Network Address Translation (NAT), Firewall, Broadband Remote Access Server (BRAS), Broadband Network Gateway (BNG), Access and Mobility Management Function (AMF) and User Plane Function (UPF) are mounted. The ISP connects with its remote locations over SD-WAN. Also ISP offers business users the service of SD-WAN. This set-up of network link enable virtualization, network programmability, end-to-end optimized traffic engineering, high bandwidth, low latency etc.

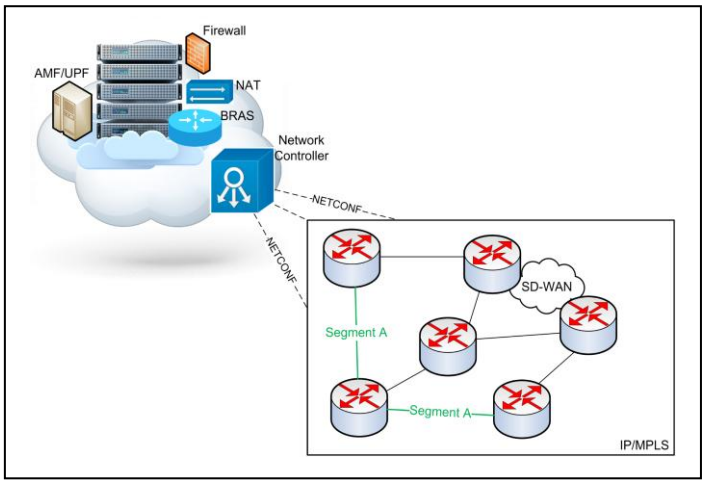

Figure 1 Framework

V CONCLUSION

The arrival of the fifth generation networks will bring a number of improvements in everyday life. 5G-era applications will require increasing speeds, lowering delays and better coverage which will result in developing new smart technologies. In order to accommodate these requirements, operators will have to introduce changes and improvements in different parts of network. Beside RAN part, IP packet data networking plays an important role in providing new 5G services. MPLS is good starting point for providing these improvements. MPLS is an established protocol that provides end-to-end network architecture, using layer 2 and layer 3 VPNs, traffic engineering, QoS etc. However, it does not provide end-to-end traffic engineering, virtualization, service function chaining, nor network slicing. In order to meet new demands which 5G brings, IP/MPLS network needs to evolve and apply new technologies enabling seamless connectivity for all distributed virtual network functions in datacenters and ISP clouds. Implementing SDN controllers, NFV, SD-WAN and Segment Routing in IP/MPLS network is a basis for providing new 5G services. Evolved IP/MPLS will enable virtualized, programmable, intelligent and rapid network which will interconnect all mobile and cloud elements dynamically.

REFERENCES

[1] C. corp and CISCO corp, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update,” pp. 2016–2021, 2013.

[2] Ericsson Corporation, “Mobile data traffic growth outlook.” [Online]. Available: https://www.ericsson.com/en/mobility-report/reports/june-2018/mobile-data-traffic-growth-outlook.

[3] 5GPPP, “View on 5G Architecture (Version 2 . 0),” no. July, 2017.

[4] 5GPPP, “The 5G Infrastructure Public Private Partnership.” [Online]. Available: https://5g-ppp.eu/.

[5] J. G. Andrews *et al.*, “What Will 5G Be?,” vol. 32, no. 6, pp. 1065–1082, 11AD.

[6] M. Maternia and S. El Ayoubi, “5G PPP use cases and performance evaluation models,” *5G-PPP Initiat.*, 2016.

[7] “Multiprotocol Label Switching.” [Online]. Available: https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching.

[8] Cisco, “MPLS Traffic Engineering.” [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/TE_1208S.html#wp37345.

[9] “MPLS VPNs.” [Online]. Available: https://en.wikipedia.org/wiki/MPLS_VPN.

[10] Juniper, “MPLS VPN Overview.” [Online]. Available: https://www.juniper.net/documentation/en_US/junos/topics/concept/mpls-security-vpn-overview.html.

[11] Packet Design, “Understanding and Managing IP / MPLS Mobile Backbone and Backhaul Networks.” 2015.

[12] T. Ryan, *Programming and Automating Cisco Networks*. Cisco Press, 2017.

[13] J. Zander and R. Forchheimer, “The SOFTNET Project: A Retrospect,” *Ieee Eurocon.*, pp. 343–345, 1988.

[14] A. T. Campbell, I. Katzela, K. Miki, and J. Vicente, “Open signaling for ATM, internet and mobile networks (OPENSIG’98),” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 29, no. 1, p. 97, 1999.

[15] G. J. M. David L. Tennenhouse, Jonathan M. Smith, W. David Sincoskie, David J, Wetherall, “A Survey of Active Network Research,” *IEEE Commun. Mag.*, pp. 80–86, 1997.

[16] IETF, “General Switch Management Protocol (GSMP) V3.” .

[17] B. Astuto, M. Mendonca, X. Nguyen, K. Obraczka, and T. Turletti, “A Survey of Software-Defined Networking : Past , Present , and Future of Programmable Networks,” vol. 16, no. 3, pp. 1617–1634, 2014.

[18] IETF, “Network Configuration Protocol (NETCONF).” .

[19] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, “Ethane,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, p. 1, 2007.

[20] S. S. Martin Casado, Tal Garfinkel, Aditya Akella, Michael Freedman, Dan Boneh, Nick McKeown, “SANE: A Protection Architecture for Enterprise Networks,” in *15th USENIX Security Symposium*, 2006.

[21] S. Rowshanrad, S. Namvarasl, V. Abdi, M. Hajizadeh, and M. Keshtgary, “A survey on SDN, the future of networking,” *J. Adv. Comput. Sci. Technol.*, vol. 3, no. 2, p. 232, 2014.

[22] M. Casado, T. Koponen, S. Shenker, and A. Tootoonchian, “Fabric: A Retrospective on Evolving SDN,” *Proc. first Work. Hot Top. Softw. Defin. networks - HotSDN ’12*, p. 85, 2012.

[23] C. D. Caesar Matthew and R. J. Feamster Nick, “Design and Implementation of a Routing Control Platform,” in *2nd Symposium on Networked Systems Design & Implementation*, 2005, no. 02, pp. 15–28.

[24] J. Kempf *et al.*, “OpenFlow MPLS and the open source label switched router,” *2011 23rd Int. Teletraffic Congr.*, pp. 8–14, 2011.

[25] N. Gude, J. Pettit, and S. Shenker, “Nox: Os for Networks.”

[26] Scott-Hayward, S., O'Callaghan, G., & Sezer, S, “SDN Security : A Survey", Queen ’ s University Belfast - Research Portal, pp. 1–7, 2013.

[27] L. Dolberg *et al*., “Network Security through Software Defined Networking : a Survey” 2014.

[28] S. . A. Scott-Hayward, S.a , Natarajan, S.b , Sezer, “Survey of Security in Software Defined Networks,” *Surv. Tutorials*, vol. 18, no. 1, pp. 623–654, 2016.

[29] N. A. Jagadeesan and B. Krishnamachari, “Software-Defined Networking Paradigms in Wireless Networks: A Survey,” *ACM Comput. Surv.*, vol. 47, no. 2, pp. 1–11, 2014.

[30] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Vasilakos, “Software-Defined and Virtualized Future Mobile and Wireless Networks: A Survey,” *Mob. Networks Appl.*, vol. 20, no. 1, pp. 4–18, 2015.

[31] I. F. Akyildiz, A. Lee, P. Wang, M. Luo, and W. Chou, “A roadmap for traffic engineering in software defined networks,” *Comput. Networks*, vol. 71, pp. 1–30, 2014.

[32] S. Computer and S. Network, “A Survey of Multicast in Software-Defined Networking Weidong Gu 1,2 , Xinchang Zhang 2,” no. Icimm, pp. 1096–1100, 2015.

[33] Y. Sinha, S. Bhatia, V. S. Shekhawat, and G. S. S. Chalapathi, “MPLS based hybridization in SDN,” *2017 4th Int. Conf. Softw. Defin. Syst. SDS 2017*, pp. 156–161, 2017.

[34] D. K. Hong, Y. Ma, S. Banerjee, and Z. M. Mao, “Incremental Deployment of SDN in Hybrid Enterprise and ISP Networks,” *Proc. Symp. SDN Res. - SOSR ’16*, pp. 1–7, 2016.

[35] S. Vissicchio, L. Vanbever, and O. Bonaventure, “Opportunities and research challenges of hybrid software defined networks,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 2, pp. 70–75, 2014.

[36] J. Kempf, Y. Zhang, R. Mishra, and N. Beheshti, “Zeppelin - A third generation data center network virtualization technology based on SDN and MPLS,” *Proc. 2013 IEEE 2nd Int. Conf. Cloud Networking, CloudNet 2013*, pp. 1–9, 2013.

[37] O. Michel and E. Keller, “SDN in Wide-Area Networks : A Survey,” pp. 37–42, 2017.

[38] S. Gordeychik and D. Kolegov, “SD-WAN Threat Landscape.”

[39] S. Jain *et al.*, “B4: Experience with a Globally-Deployed Software Defined WAN,” pp. 3–14.

[40] C.-Y. Hong *et al.*, “B4 and After: Managing Hierarchy, Partitioning, and Asymmetry for Availability and Scale in Google’s Software-Defined WAN,” *Acm Sigcomm*, pp. 74–87, 2018.

[41] A. Introduction *et al.*, “NFV-White-Paper 2,” *Citeseer*, no. 1, pp. 1–16, 2012.

[42] Yong Li and Min Chen, “Software-Defined Network Function Virtualization: A Survey,” *IEEE Access*, vol. 3, pp. 2542–2553, 2015.

[43] W. Yang and C. Fung, “Fisheries research vessel handed over by Welsh builder,” *Sh. Boat Int.*, vol. 2, no. 9, pp. 6–7, 2002.

[44] D. Cotroneo *et al.*, “Network function virtualization: Challenges and directions for reliability assurance,” *Proc. - IEEE 25th Int. Symp. Softw. Reliab. Eng. Work. ISSREW 2014*, pp. 37–42, 2014.

[45] J. Gil Herrera and J. F. Botero, “Resource Allocation in NFV: A Comprehensive Survey,” *IEEE Trans. Netw. Serv. Manag.*, vol. 13, no. 3, pp. 518–532, 2016.

[46] S. R. Bansal, Bharti, “Security Issues in Network Function Virtualization,” vol. 7, no. 5, pp. 134–141, 2017.

[47] IETF, “Segment Routing Centralized BGP Egress Peer Engineering.” .

[48] IETF, “Segment Routing Policy Architecture.” .

[49] IETF, “Segment Routing Architecture.” .

[50] IETF, “Segment Routing interworking with LDP.” .

[51] IETF, “Segment Routing with MPLS data plane.” .

[52] C. Filsfils, N. K. Nainar, C. Pignataro, J. C. Cardona, and P. Francois, “The segment routing architecture,” *2015 IEEE Glob. Commun. Conf. GLOBECOM 2015*, 2015.

[53] A. Sgambelluri, F. Paolucci, A. Giorgetti, F. Cugini, and P. Castoldi, “Experimental demonstration of segment routing,” *J. Light. Technol.*, vol. 34, no. 1, pp. 205–212, 2016.

[54] A. Sgambelluri, A. Giorgetti, F. Cugini, G. Bruno, F. Lazzeri, and P. Castoldi, “First Demonstration of SDN-based Segment Routing in Multi-layer Networks,” *Opt. Fiber Commun. Conf.*, p. Th1A.5, 2015.

[55] ETSI, “System Architecture for the 5G system.” .

[56] N. Alliance, “5G White Paper,” By NGMN Alliance 1.0.” 2015.

[57] N. N. Adlen Ksentini, “Toward Enforcing Network Slicing on RAN: Flexibility and Resources Abstraction,” *IEEE Commun. Mag.*, 2017.

[58] H. Zhang, N. Liu, X. Chu, … K. L.-I., and undefined 2017, “Network slicing based 5G and future mobile networks: mobility, resource management, and challenges,” *Ieeexplore.Ieee.Org*, no. August, pp. 138–145, 2017.

[59] J. Ordonez-Lucena, P. Ameigeiras, Di. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, “Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges,” *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, 2017.

[60] and M. K. M. Xenofon Foukas, Georgios Patounas, Ahmed Elmokashfi, “Network Slicing in 5G: Survey and Challenges,” *IEEE Commun. Mag.*, 2017.

[61] A. Nakao *et al.*, “End-to-end Network Slicing for 5G Mobile

Networks," *J. Inf. Process.*, vol. 25, no. 0, pp. 153–163, 2017.

[62] I. Da Silva *et al.*, "Impact of network slicing on 5G Radio Access Networks," *EUCNC 2016 - Eur. Conf. Networks Commun.*, pp. 153–157, 2016.

[63] IETF, "Problem Statement of Network Slicing in IP/MPLS Networks." .

[64] Q. Chen and C. Liu, "A Survey of Network Slicing in 5G," no. Csma, pp. 27–35, 2017.