Software Defined VPLS Architectures: Opportunities and Challenges

Madhusanka Liyanage[1], Mika Ylianttila[2], Andrei Gurtov[3]
[1,2] Centre for Wireless Communications (CWC), University of Oulu, Finland
[3] Department of Computer and Information Science, Linköping University, Sweden
Email: [1]madhusanka.liyanage@oulu.fi, [2]mika.ylianttila@oulu.fi, [3]gurtov@acm.org

***Abstract*—Virtual Private LAN Services (VPLS) is an Ethernet based VPN (Virtual Private Network) service which provides protocol independent and high speed multipoint-to-multipoint connectivity. In this article, we discuss the possibility to use emerging networks concepts such as Software Defined Networking (SDN) and Network Function Virtualization (NFV) to improve the performance, flexibility and adaptability of VPLS networks. SDN and NFV based VPLS (SoftVPLS) architectures offer new features such as centralized control, network programmability and abstraction to improve the performance, flexibility and automation of traffic, security and network management functions for future VPLS networks.**

I. Introduction

Virtual Private LAN Services (VPLS) have gained the immense popularity among industrial enterprises as an ideal networking solution to interconnect legacy SCADA (Supervisory Control and Data Acquisition) and process control devices over a shared network. Due to the protocol independent, high speed and low cost operation compared to other VPN networks, VPLS networks are used in many application domains. Today, VPLS applications range from industrial networks to mobile backhaul networks. Recently Data Center Interconnect (DCI) has become one of the leading applications of VPLS networks [1].

New VPLS applications demand additional operational requirements such as enhanced security, simplified provisioning of services, optimized network resource utilization, enhanced scalability and automatic network management support[1]. However, existing legacy VPLS architectures are complex, inflexible and static to provide such features for new applications.

On these grounds, SDN and NFV concepts are identified as promising technologies to design dynamic, flexible, secure and scalable of VPLS networks. In this article, we highlight how SDN and NFV concepts can be used to improve the performance of VPLS networks. Initially, we explain the Software Defined VPLS Architecture and it's components. Then, We discuss the expected performance advantages of SDN and NFV based VPLS architectures and how they can solve the issues in the legacy VPLS architectures. We also present the key challenges and limitations of those architectures. Moreover, the performance of a Software Defined VPLS architecture is analyzed with existing legacy VPLS architectures by using both simulation and testbed experiments.

The rest of the paper is organized as follows. The background of existing VPLS architectures and SDN/NFV technologies are presented in Section II. Section III presents SDN and NFV based VPLS (SoftVPLS) architecture and their key features. Expected advantages of SoftVPLS architecture are presented in Section IV. Section V contains a performance evaluation of different VPLS architectures. In Section VI, we highlight the limitations of SoftVPLS architectures. Finally, Section VII concludes the article.

II. Background

A. Virtual Private LAN Services (VPLS)

VPLS provides Ethernet based multipoint-to-multipoint communication over a provider network. It can extend the Ethernet broadcast domain to multiple sites which are geographically dispersed across the globe.

A VPLS network has four key elements 1) customer sites, 2) Customer Edge devices (CEs), 3) Provider Edge devices (PEs), 4) the provider network (Figure 1). Customer sites are L2 private networks which are dispersed across the globe. VPLS networks interconnects customer sites by using the provider network. CEs are the interface devices between the customer and provider networks. PEs have all VPLS intelligence and support VPLS functions. The provider network can be a public Wide Area Network (WAN) such as mobile networks and the Internet. A full mesh of VPN tunnels/PWs(Pseudo Wires) are established between PEs over the provider network. Different types of tunnels such as IPSec (IP Security), L2TPv3 (Layer 2 Tunneling Protocol Version 3) and MPLS (Multiprotocol Label Switching) are used to establish the mesh network tunnels[2]. The key benefits of VPLS networks are summarized in Table I [3], [4], [5].

IETF standardizes two basic VPLS frameworks by using BGP [6] and LDP [7]. Later, several other MPLS

TABLE I: Key Benefits of VPLS Networks

Benefit	Description
Multipoint-to-multipoint connectivity	Transparent, protocol-independent, multipoint connectivity solution for remote customer sites.
COTS (commercial off-the-shelf) solution	COTS connectivity services for customers which out modifying their own private network segments.
Interoperability	Eliminates L2 (Layer 2) protocol conversion between LAN and WAN. Removes the IP ?issues,? namely, trust, security and outsourcing.
Low Cost Operation	Customer network segments can be implemented with low cost L2 switches than expensive L3 (Layer 3) routers.
Support of Service Level Agreements (SLAs)	Upgrading and downgrading of service levels (e.g. Bandwidth, QoS level) is possible without changing the customer site equipment.
VPLS auto-discovery and service provisioning	Addition of new sites is possible without reconfiguring existing sites due to VPLS auto-discovery and service provisioning features.
Full control of Customer sites	Customer has full control of network management and routing of their own network segment. They can modify, add or remove network devices without informing the VPLS operator or their help.

based VPLS architectures had been proposed to improve the performance of VPLS networks[3]. HIP (Host Identity Protocol) enabled virtual private LAN service (HIPLS)[8] is proposed to increase the security of VPLS networks. Thereafter, several HIP based VPLS architectures are proposed to further enhance the security and scalability of HIPLS[9], [2], [10], [11]. However, these legacy VPLS architectures are still suffering from several limitations. Table II explains the key limitations of legacy VPLS networks [3], [12], [13], [14], [15], [16], [17].

A survey on SDN and MPLS integration is presented in [12]. Furthermore, the possibility to implement SDN based VPNs as a Service on MPLS-free provider networks is presented in [13]. The evolution of carrier ethernet architecture by using SDN technologies is discussed in [14]. A utilization of SDN to improve the tunnel management performance of secure VPLS architectures is presented in [16]. Hu et. al present SDN based VPLS system which realized the VPLS service on-demand by leveraging on OpenVirteX network virtualization platform[15]. An SDN based framework to automates the Ethernet VPN deployment and management inside SDN-based DCs using OpenStack and OpenDaylight platform is presented in [17].

B. Software Defined Networking (SDN) and Network Function Virtualization (NFV)

In common terms, SDN is considering as ?the new norm of networking?[18]. SDN concepts proposed to decouple the control and data planes of a network. A logically centralized software program called network controller is used to control the operation of the entire network. NFV allows the implementation of network control functions as software applications which run on top of the control plane[19].

SDN offers three key attributes namely, logically centralized intelligence, programmability and abstraction[18], [19]. The controller sees the global view of the network from a single pane of glass. Thus, the centralized decision-making procedure will be more efficient than present autonomous and distributed procedures. Programmability enables the ability to use advanced software programming techniques to modify the network behavior and its functions. The complex network infrastructure and protocols are hidden behind the NOS (Network Operation System). Furthermore, business applications can get the abstract information of the underlying network via the SDN controller[18].

III. Software Defined VPLS (SoftVPLS) Architecture

An SDN and NFV based SoftVPLS architecture is illustrated in Figure 1[14], [15], [16]. This SoftVPLS architecture proposes three main changes to legacy VPLS networks. First, it decouples the control plane from the data plane and implements the control plane functions in a logically centralized controller. Second, VPLS management functions will implement as software applications of service provider owned data center or cloud. Third, data path PEs are replaced with SDN switches (e.g. Openflow switches)[14], [15], [16].

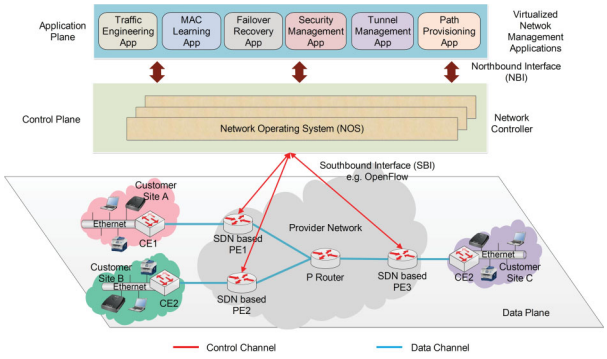


Fig. 1: The SoftVPLS Architecture

Therefore, SoftVPLS architecture consists of three planes, namely, Data Plane(DP), Control Plane (CP) and Application Plane (AP). DP is formed by PEs, P-routers

and physical links to interconnect them. In SoftVPLS networks, PEs are now SDN switches. CP contains a logically centralized controller which controls DP devices by using a control protocol such as OpenFlow[18]. Legacy VPLS management functions are implemented in AP as software applications. The SDN controller for SoftVPLS is modified to support legacy VPLS management functions such MAC (Media Access Control) learning, tunnel management and path provisioning functions. Moreover, SoftVPLS also supports additional functions such as traffic engineering, security management and failover recovery, to improve the performance of VPLS networks.

In contrast to the existing SDN networks, an extended SDN southbound API (Application Programmable Interface) should be utilized in SoftVPLS architecture. Existing southbound APIs such as OpenFlow support only basic flow base routing function. The extended SDN southbound interface should support additional functions such as IPSec tunnel management. Table III contains a comparison of SoftVPLS with existing VPLS architectures.

IV. Expected Benefits of SoftVPLS architecture

The adaptation of SDN and NFV concepts offers new features such as centralized intelligence, network programmability, abstraction, common device standards and flow based traffic management which are useful to implement dynamic, flexible, secure and scalable VPLS networks [12], [13], [14], [15], [16]. On the one hand, the added features in SoftVPLS can also be used to overcome the limitations in legacy VPLS networks. Table II presents how these SoftVPLS features can be used to overcome the issues in legacy VPLS networks. On the other hand, SDN features add extra benefits to VPLS networks.

A. Enhanced Security

The SoftVPLS architecture offers network-wide real time security monitoring. The controller can monitor network activities and detect anomalous behaviors by analyzing historical and real-time network status and performance data. Moreover, the controller can take real-time proactive decisions of mitigating such attacks with a greater degree of accuracy. For instance, security actions such as reduction of resource limits, fine tuning of firewalls and ingress filters can be dynamically performed in malicious network segments to prevent and propagation of DoS (Denial of Service) attacks[20]. Moreover, holistic network informatics are useful for efficient forensic analysis as well as designing reactive security mechanisms.

The SoftVPLS architecture supports centralized security control and orchestration of security mechanisms. The synchronization of various security policies will be efficient with the centralized intelligence. It removes overlapping and redundant security policies in the VPLS networks[20].

B. Scalability

The SoftVPLS architecture can dynamically estimate and adjust the tunnel parameters based on real time traffic session characteristics. As a result, it can significantly reduce the average number of tunnels per PE and the total number of tunnels in the network compared to legacy secure VPLS architectures by disconnecting inactive tunnels. It improves the control and forwarding plane scalability of VPLS networks[16]. In addition, the SoftVPLS architecture supports virtualized resources which can be allocated dynamically to match the real-time traffic load. It also eliminates the unnecessary requirement to reserve physical resources to match with busy hour traffic. It drastically reduces the network implementation cost and increases the scalability.

C. Extra Features

Due to the network wide visibility and centralized controlling, the SoftVPLS architecture can support many new features such as TE (Traffic Engineering), load sharing, OAM (Operations,Administration and Management), fast failover, rate limiting of VPN traffic and rate limiting of BUM (Broadcast, Unicast,and Multicast) traffic [12], [16]. Such added features improve the scalability, security and service quality of VPLS networks.

D. High rate innovation

The SoftVPLS architecture enables the network programmability and support software based virtualized network functions. The software based VPLS functions can be deployed and modified very quickly compared to legacy hardware based VPLS functions[13]. Therefore, the deployment of new network functions and business applications is quite fast in SoftVPLS networks.

E. Low cost operation

In the SoftVPLS architecture, VPLS functions can be dynamically deployed on already existing SDN based network infrastructures. It helps reassign and share the infrastructure resources with other network services. Moreover, the common device standards allow to mix-and-match different vendor equipment. These factors reduce CAPEX cost of the VPLS deployments[13].

With the help of centralized controlling and abstraction, the SoftVPLS architecture supports flexible management schemes, such as dynamic configuration, automation and reduced signaling traffic. This features lead to a reduction in OPEX costs[16]. In traditional VPLS systems, these features are difficult to implement and would come at much higher costs.

TABLE II: Limitations in legacy VPLS architectures and mitigating mechanisms in SoftVPLS architecture

Limitations in Legacy VPLS architecture	**Description**	**Mitigating mechanisms in SoftVPLS architecture**	**Enabling feature in SoftVPLS architecture**
Complexity of network management	Current VPLS architectures need the support of many control protocols for VPLS management[3], [6], [7].	Simplifies the network management by using centralized network management and eliminate the use of complex control protocols by using single standard control protocol [12].	Centralized controller, common device standard and standard control protocol.
Limited Scalability	Due to the N-Square scalability problem and complex control protocols, current VPLS architectures support only 3 to 30 sites[8], [2], [11], [16].	Enhanced the scalability by terminating unused VPN tunnels and globally optimizing the utilization of network resources[16].	Global visibility and network programmability
Limited granularity on flow control	Flow classification is only based on MAC addresses[3], [6], [7].	The flow-based control model in SDN architecture allows to apply the flow control policies at a very granular level such as the session, user, device, and application levels [13].	Flow based traffic routing
Static VPN tunnel establishment	Tunnel parameters are pre-defined and unable to fine tune the tunnel parameters dynamically[16].	VPLS operator can dynamically change the tunnel parameters based on real-time network status[16].	Global visibility and network programmability
Lack of attack mitigation	Dynamic mechanisms are not available to prevent attacks and attack propagation[11], [16].	The controller takes proactive and reactive decision-making by blending historical and real-time network status and communication data.	Centralized controller and network programmability
Expensive, complex and vendor specific devices	VPLS routers should support many protocols. Operators need VPLS enabled expensive devices. Moreover, vendor specific devices cannot be ?mixed-and-matched? for cost effective deployments[12].	Simplify DP devices by integrating their control functionality within the SDN network controller. A common control protocols (e.g. OpenFlow) is used to control all the data plane PEs by eliminating vendor specific and proprietary protocols and devices[13].	Common device standard and standard control protocol
Lack of resource optimizations	No mechanism to optimize the resource utilization of VPLS networks[16].	The controller has the global visibility of the network as well as the historical and real-time network information. Therefore, it can take informed decisions to optimize the network resources[12], [16].	Centralized controller and global visibility
Lack of traffic engineering features	No architecture supports traffic engineering features to provide load balancing, optimal routing or to minimize the traffic transport delay)[12], [16].	The controller has access to the real-time network information. Based on that, the controller can take change the network parameters dynamically [12], [16].	Centralized controller, global visibility and network programmability

V. Performance Evaluation

The performance of SoftVPLS architecture analyzed with HIP and MPLS based VPLS architectures by using simulation and testbed experiments.

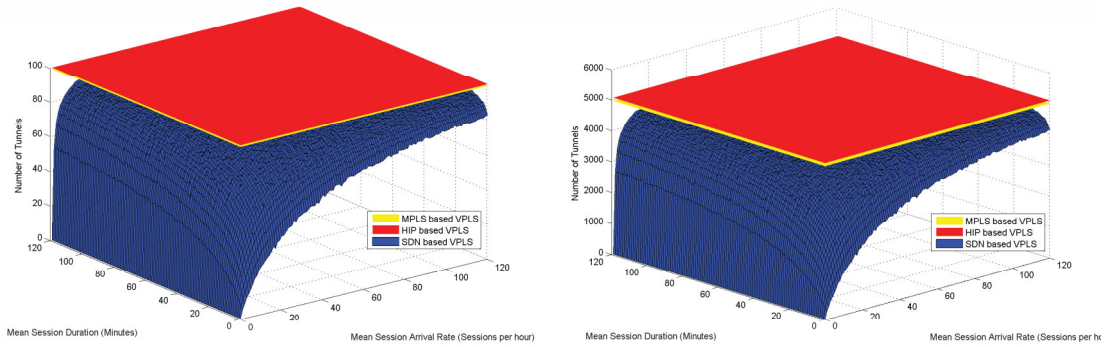
A. Simulations

The scalability performance of different VPLS architecture categories is analyzed by using OMNET++ simulation environment. We analyzed all three types of VPLS architectures, i.e. 1) MPLS based VPLS (LDP [7]) 2) HIP based VPLS [2] and 3) SDN based VPLS [14], [15], [16]. We used a provider network consist of 100 PEs and 100 R-routers. The model network is generated by using stochastic Kronecker graphs. The simulation model establishes tunnels according to the tunnel management mechanism of each architecture. In the experiments, we changed the session duration and the session arrival rate of each tunnel and compared the total number of tunnels in the networks and average number of tunnels per PE. The session arrival process is modeled as a Poisson process and the session duration is modeled as an exponential distribution. Figure 2 illustrates the simulation results.

According to the simulation results (Figure 2), both the total number of tunnels in the network and the number of tunnels per PE are lower in SDN based VPLS architecture than other VPLS architectures. SDN controller dynamically change the tunnel durations to terminate the underutilized tunnels. Moreover, the expected advantage of SDN based VPLS is higher for the networks with low session duration and low arrival rate. The reduction of the number of active tunnels verifies the enhanced control and data plane scalability than legacy VPLS architectures.

B. Testbed

The feasibility of SoftVPLS architecture is analyzed in a Testbed. We used two SDN enabled OpenVswitch (OVS) version 1.10.0 switches as PEs. Then, we attached a CE for each PE. Here, laptops with Intel i5-3210M



(a) Average number of tunnels per PE

(b) Total number of tunnels in the network

Fig. 2: Scalability Analysis

TABLE III: Comparison of difference VPLS architectures

Property	**MPLS VPLS [6], [7]**	**HIP VPLS[8], [2], [11]**	**SoftVPLS**
Path provisioning	LDP/BGP	HIP	Centralized
Tunnel establishment	MPLS	IPSec	MPLS/IPSec
Traffic rate limiting	No	No	Dynamic
OAM	LSP Ping	HIP updates	Centralized
MAC table	Per PE	Per PE	Centralized
Tunnel establishment topology	Meshed	Meshed	Based on STP
Tunnel duration	Static	Static	Dynamic
BUM (Broadcast, Unicast,and Multicast) traffic handling	Flooding	Flooding	Centralized
Dynamic BUM limiting	No	No	Yes

CPU is used as CEs. The POX controller is used as the SDN controller and it uses OpenFlow version 1.1.0 to control PEs. We established a communication section between two CEs and measure the data plane throughput and tunnel establishment delay performance by using the IPERF network measurement tool and Internet Control Message Protocol (ICMP) messages. Figure 3 presents the experiment results.

The data plane performance (TCP throughput and Jitter) of proposed architecture is similar to existing HIP based VPLS architectures[2]. The utilization of SDN has no impact on IPsec encryption process. As a results, it cannot reduces the encryption delay at switches to improve the data plane performance. However, the SDN based VPLS architecture supports advanced traffic engineering features. E.g. Tunnel Resumption Procedure (TRP)[16]. By using the TRP, the SDN based VPLS architecture is significantly reduced (about 45% reduction) the tunnel establishment delay of subsequent tunnel establishments between authorized PEs.

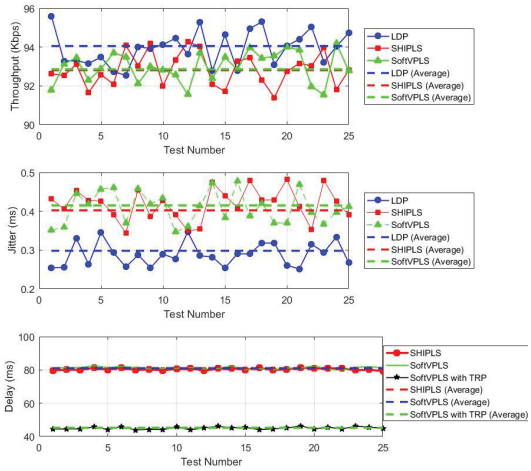


Fig. 3: Testbed Experiments

VI. Limitations in SoftVPLS architecture

The SoftVPLS architecture introduces a new generation of VPLS networks which provide cost-effective, flexible, robust and efficient network services tailored to individual customer needs. Despite above advantages, the SoftVPLS architecture must overcome several challenges not only to fully realize the expected benefits but also to fuel the larger scale deployment. The following are four common categories of challenges in the SoftVPLS architecture.

A. Interoperability

The deployment of SoftVPLS architecture in new provider networks is fairly straightforward. New networks can be deployed with all SDN-ready devices and equipment. However, transitioning a legacy provider network to an SDN based provider network is challenging as the provider network is likely supporting other active business and network services[21], [18]. On the one hand, most of such network services are not yet SDN friendly. On the other hand, network service providers are reluctant to invest in new SDN infrastructure as they have already invested huge amount of money in current network infrastructure. Therefore, VPLS providers require a period of interoperability with a hybrid legacy-SDN infrastructure to facilitate the smooth transition.

Both, SDN and legacy network nodes have to operate together with the help of an appropriate protocol that supports SDN communications while providing backward compatibility with existing IP and MPLS control plane technologies. Such, architecture should reduce the cost, risk, and disruption of services while transitioning to a complete SoftVPLS architecture. The development of such a hybrid legacy-SDN infrastructure is challenging.

B. Security

Although SDN and NFV concepts help to overcome the security limitations of legacy VPLS networks, the SoftVPLS architecture is now vulnerable to a new set of security threats. These new threats can be divided into four threat vectors as security issues related to data plane, control plane, application plane and communication channels.

1) Security issues related to data plane: The SoftVPLS data plane is now vulnerable to a new type of attacks. For instance, flow poisoning attack injects invalid traffic flows not only to exhaust TCAM (Ternary Content-Addressable Memory) of data plane switches but also the controller resources[22]. Moreover, SoftVPLS networks now share the data plane devices with other network services. An attack on other network services might be able to cease the operation of SoftVPLS networks.

2) Security issues related to control plane: The network controller is considered as the single point of failure or bottleneck of all SDN based systems including SoftVPLS architecture. The newly introduced controller is the default target of DoS attackers. Moreover, the controller itself is a software application which runs on operating system. Such operating system might have its own vulnerabilities such as the use of insecure protocols such as HTTP, telnet, or outdated security patches and firmware[20].

3) Security issues related to application plane: In contrast to the hardware based VPLS network, the SoftVPLS architecture proposes software based controlling and network services. On one hand, the manipulation of a software application is comparably easier than black-box type hardware devices. Moreover, software applications are vulnerable to programming issues such as buffer overflow and null pointers issue. The lack of strong authentication at the application plane will allows malicious third party applications to jeopardize the smooth operation of VPLS network. On the other hand, the introduction of new elements such as hypervisors creates new attack surfaces on SoftVPLS networks. It is also a critical security requirement to ensure the trust between new elements such as virtual machines, virtual switches, hypervisors, controllers and management modules.

4) Security issues related to communication channels: SoftVPLS architecture uses two communication channels. 1) Data channel: To deliver user traffic and 2) Control channel: To transport signaling and control data. IP based VPLS communication channels should contain required security measure to avoid common security attacks such as eavesdropping, DoS, reset and Man-in-the-Middle (MitM) attacks. Moreover, the SoftVPLS communication channels are now vulnerable new type of eavesdropping attack called "SDN Scanner" attacks. The attacker can use "SDN Scanner" mechanism to collect flow information on the data channel to attack the control channel[22].

The existing SDN control protocols (e.g. OpenFlow) use TLS (Transport Layer Security) based communication. However, TLS sessions are vulnerable to classical IP based attacks such as TCP Syn DoS, reset and IP spoofing attacks[20].

C. Performance

The separation of control and data planes can introduce extra latency into SDN based VPLS architecture. Since every data plane devices have to frequently contact the SDN controller, controller response time and throughput can contribute to overall poor performance of the VPLS network.

As a solution for this issue, SDN based networks push more intelligence to the edge of the data plane. Although this approach can improve the performance, final architecture is moving away from the intent of original SDN concepts. It is somewhat closing to replication of legacy VPLS networks built on fully distributed intelligent devices. A proper balance of control function delegation has to be sought where virtualization and centralized control are maintained without degrading network performance.

D. Scalability

Since the SoftVPLS architecture consists of a centralized controller, the proper deployment of the controller is important to achieve scalability in SDN based VPLS networks. In many cases, it is not possible to use single

controller for large scale VPLS networks due to the latency in the control channel. As a result, multiple or distributed controller architectures are used in many SDN networks [23]. Such solutions can introduce new obstacles such as convergence and countless control instances to configure and manage. Moreover, it is also challenging to find the optimum number of controllers and the best location for each controller. The SoftVPLS architecture should have a method to solve the conflicts when multiple controllers are available for a single data plane device.

VII. Conclusion

The immense popularity of Virtual Private LAN Services (VPLS) in new application domains is creating new operational requirements such as enhanced security, simplified provisioning of services, optimized resource utilization and enhanced scalability. However, legacy VPLS architectures are not adequate enough to support such services due to complex, inflexible and static control and management functions.

The introduction of emerging Software Defined Networking (SDN) and Network Function Virtualization (NFV) concepts is improving the performance, flexibility and adaptability of VPLS networks. SDN and NFV based SoftVPLS architecture offers new features such as centralized control, network programmability and abstraction to solve the limitations in legacy VPLS networks.

Despite the expected advantages, the SoftVPLS architecture also faces several challenges in terms of interoperability, security, performance and scalability. The SoftVPLS architecture must overcome the challenges to fully realize the expected benefits in the large scale deployment.

Acknowledgment

This work has been performed under the framework of the SECUREConnect (Secure Connectivity of Future Cyber-Physical Systems) and Towards Digital Paradise projects. This research is funded by Academy of Finland and TEKES, Finland.

References

[1] N. Chen, Y. Fan, X. He, Y. Liu, and Q. Li, "Research on Cloud Datacenter Interconnect Technology," in *Web Technologies and Applications*. Springer, 2015, pp. 79–86.

[2] M. Liyanage and A. Gurtov, "Securing Virtual Private LAN Service by Efficient Key Management," *Security and Communication Networks*, vol. 7, no. 1, pp. 1–13, 2014.

[3] V. Joseph and S. Mulugu, *Deploying Next Generation Multicast-enabled Applications: Label Switched Multicast for MPLS VPNs, VPLS, and Wholesale Ethernet*. Elsevier, 2011.

[4] X. Dong and S. Yu, "VPLS: An Effective Technology for Building Scalable Transparent LAN Services," in *Asia-Pacific Optical Communications*. International Society for Optics and Photonics, 2005, pp. 137–147.

[5] H. Awadalla, "Wide Area Ethernet, VPNs, VPLS - Current Trends and Future developments," in *Telecoms Networks-The Next Generation, 2005. The IEE Annual Course on (Ref. No. 2005/11047)*. IET, 2005, pp. 0_21–5.

[6] K. Kompella and Y. Rekhter, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling," RFC 4761, IETF, January 2007.

[7] M. Lasserre and V. Kompella, "Virtual Private LAN Service (VPLS) using Label Distribution Protocol (LDP) Signaling," RFC 4762, IETF, January 2007.

[8] T. Henderson, S. Venema, and D. Mattes, "HIP-based Virtual Private LAN Service (HIPLS)," *Internet Draft*, IETF, December 2013.

[9] M. Liyanage and A. Gurtov, "A Scalable and Secure VPLS Architecture for Provider Provisioned Networks," in *IEEE Wireless Communication and Networking Conference: WCNC 2013*. IEEE, 2013.

[10] M. Liyanage, M. Ylianttila, and A. Gurtov, "Secure Hierarchical Virtual Private LAN Services for Provider Provisioned Networks," in *Communications and Network Security (CNS), 2013 IEEE Conference on*. IEEE, 2013, pp. 233–241.

[11] M. Liyanage, A. Gurtov, and M. Ylianttila, "Secure Hierarchical VPLS Architecture for Provider Provisioned Networks," *Access, IEEE*, vol. 3, pp. 967–984, 2015.

[12] M. Casado, T. Koponen, S. Shenker, and A. Tootoonchian, "Fabric: A Retrospective on Evolving SDN," in *Proceedings of the first workshop on Hot topics in software defined networks*. ACM, 2012, pp. 85–90.

[13] S. Konstantaras and G. Thessalonikefs, "Software Defined VPNs," Master's thesis, University of Amsterdam, 2014.

[14] D. Cai, A. Wielosz, and S. Wei, "Evolve carrier Ethernet Architecture with SDN and Segment Routing," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on a*. IEEE, 2014, pp. 1–6.

[15] J.-W. Hu, C.-S. Yang, and T.-L. Liu, "L2OVX: An On-demand VPLS Service with Software-Defined Networks," in *Advanced Information Networking and Applications Workshops (WAINA), 2016 30th International Conference on*. IEEE, 2016, pp. 861–866.

[16] M. Liyanage, A. Gurtov, and M. Ylianttila, "Improving the Tunnel Management Performance of Secure VPLS Architectures with SDN," in *Proc. of IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA. IEEE*. IEEE, 2016.

[17] K. A. Noghani, C. H. Benet, A. Kassler, A. Marotta, P. Jestin, and V. V. Srivastava, "Automating Ethernet VPN Deployment in SDN-based Data Centers," in *Software Defined Systems (SDS), 2017 Fourth International Conference on*. IEEE, 2017, pp. 61–66.

[18] B. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 3, pp. 1617–1634, 2014.

[19] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network Function Virtualization: Challenges and Opportunities for Innovations," *Communications Magazine, IEEE*, vol. 53, no. 2, pp. 90–97, 2015.

[20] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in Software Defined Networks: A Survey," *Communications Surveys & Tutorials, IEEE*, vol. 17, no. 4, pp. 2317–2346, 2015.

[21] S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 36–43, 2013.

[22] M. Liyanage, A. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security Perspective," *IEEE Security and Privacy Magazine*, 2016.

[23] S. H. Yeganeh, A. Tootoonchian, and Y. Ganjali, "On Scalability of Software-Defined Networking," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 136–141, 2013.