A survey of Virtual Private LAN Services (VPLS): Past, present and future

Article *in* Computer Networks · June 2021

DOI: 10.1016/j.comnet.2021.108245

CITATIONS
2

READS
983

6 authors, including:

Kuntal Gaur
Manipal University Jaipur
4 PUBLICATIONS **13** CITATIONS
SEE PROFILE

Anshuman Kalla
Uka Tarsadia University
33 PUBLICATIONS **489** CITATIONS
SEE PROFILE

Jyoti Grover
Malaviya National Institute of Technology Jaipur
42 PUBLICATIONS **456** CITATIONS
SEE PROFILE

Mohammad Borhani
Linköping University
4 PUBLICATIONS **32** CITATIONS
SEE PROFILE

A Survey of Virtual Private LAN Services (VPLS): Past, Present and Future

Kuntal Gaur, Anshuman Kalla*, Jyoti Grover, Mohammad Borhani, Andrei Gurtov, Madhusanka Liyanage

***Abstract*—Virtual Private LAN services (VPLS) is a Layer 2 Virtual Private Network (L2VPN) service that has gained immense popularity due to a number of its features, such as protocol independence, multipoint-to-multipoint mesh connectivity, robust security, low operational cost (in terms of optimal resource utilization), and high scalability. In addition to the traditional VPLS architectures, novel VPLS solutions have been designed leveraging new emerging paradigms, such as Software Defined Networking (SDN) and Network Function Virtualization (NFV), to keep up with the increasing demand. These emerging solutions help in enhancing scalability, strengthening security, and optimizing resource utilization. This paper aims to conduct an in-depth survey of various VPLS architectures and highlight different characteristics through insightful comparisons. Moreover, the article discusses numerous technical aspects such as security, scalability, compatibility, tunnel management, operational issues, and complexity, along with the lessons learned. Finally, the paper outlines future research directions related to VPLS. To the best of our knowledge, this paper is the first to furnish a detailed survey of VPLS.**

***Index Terms*—VPLS, SDN, MPLS, BGP, LDP, HIPLS.**

I. Introduction

The globalisation and expansion of enterprises and organisations have led to an indispensable need to securely connect various sites and offices that are geographically distributed worldwide. Virtual Private Networks (VPNs) have emerged as a cost-effective solution to realise this goal. VPNs are a way to logically divide shared networking infrastructure to create a closed virtual network that allows secure access to private services and resources that are geographically distributed [1]. Previously, the use of VPNs was confined to big organisations, as only they could afford the required infrastructure. Recently, VPN services have gained momentum and are now being used both by individuals and organisations of all sizes and nature for secure dissemination of data and sharing of resources over public networks. Thus, VPNs enable multi-location enterprises to communicate securely via the public internet. A typical VPN network is shown in Figure 1.

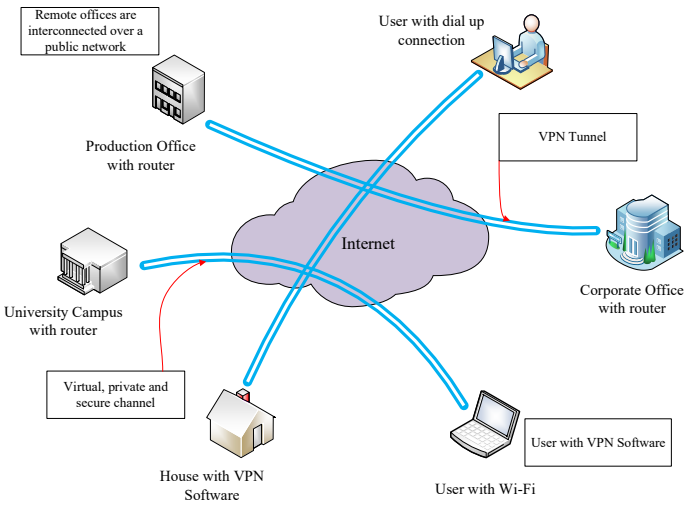

Fig. 1: Network schematic diagram for VPN connections

There are Layer 1 (L1), Layer 2 (L2), and Layer 3 (L3) VPN networks based on the layer of the Open Systems Interconnection (OSI) model at which they are implemented. In L2VPN, frames at the data link layer are transmitted between locations connected via Ethernet. Multi-Protocol Label Switching (MPLS) is used for transporting data in L2VPN [2]. Communication occurs between routers known as Provider Edge (PE) routers. Layer 3 VPNs (L3VPN) use MPLS and IP technology for data transportation [3]. As opposed to L2VPN, in which only L2 is virtualized, in L3VPN, the whole network is virtualized for communication. Additionally, L1 VPN has also been introduced to meet growing traffic demands. It leverages the control and management capabilities of L2 and L3 networks [4]. The auto-discovery requirements of L1VPN are similar to those of L3VPN. Generalized Multiprotocol Label Switching (GMPLS) is employed by L1VPN for routing and signalling [5]. GMPLS supports both Lambda Switch Capable (LSC) devices and Time-Division Multiplexing. Lambda Switching is used in optical networks for routing. Therefore, L1VPN can be applied to SONET (TDM) and Optical Transport Networks (OTN). To support L1 functioning, few services were identified: maintenance of information related to membership and routing, route computation, and connection control and management.

* Corresponding author

Kuntal Gaur is with Department of Computer Applications, Manipal University Jaipur, India. e-mail: kuntal.gaur@jaipur.manipal.edu

Anshuman Kalla is with Centre for Wireless Communications, University of Oulu, Finland. email: anshuman.kalla@ieee.org and anshuman.kalla@oulu.fi

Jyoti Grover is with Department of Computer Science and Engineering, Malaviya National Institute of Technology Jaipur, India. e-mail: jgrover.cse@mnit.ac.in

Mohammad Borhani is with the Department of Computer and Information Science, Linköping University, Sweden. e-mail: mohammad.borhani@liu.se

Andrei Gurtov is with the Department of Computer and Information Science, Linköping University, Sweden. e-mail: andrei.gurtov@liu.se

Madhusanka Liyanage is with the School of Computer Science, University College Dublin, Ireland and the Center for Wireless Communications, University of Oulu, Finland. e-mail: madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi

TABLE I: The List of Important Acronyms

Acronym	Definition.	Acronym	Definition
AC	Attachment Circuit	ACL	Access Control List
AFI	Address Family Identifier	AGI	Attachment Group Identifier
AH	Authentication Header	API	Application Program Interface
ARP	Address Resolution Protocol	ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol	BYOD	Buy Your Own Device
CA	Certification Authority	CE	Customer Edge device
CPVPN	Customer Provisioned Virtual Private Network	DBE	Domain Border Edge
DCI	Data Centre Interconnect	DE	Domain Edge
DoS	Denial of Service	DDoS	Distributed Denial of Service
DSL	Digital Subscriber Line	EID	Ecological Interface Design
ESP	Encapsulating Security Payload	EVPN	Ethernet Virtual Private Network
FIB	Forward Information Base	GRE	Generic Routing Encapsulation
HIP	Host Identity Protocol	HIPLS	HIP based Virtual Private LAN Service
H-VPLS	Hierarchical Virtual Private LAN Service	H-HIPLS	Hierarchical HIP based Virtual Private LAN Service
I-BGP	Internal Border Gateway Protocol	ICMP	Internet Control Message Protocol
IDN	Identity Defined Networking	IE	Island Edge
IETF	Internet Engineering Task Force	IKE	Internet Key Exchange
IoT	Internet of Things	IP	Internet Protocol
IPLS	IP only LAN services	IPsec	Internet Protocol security
L2	Layer two	L3	Layer three
L2TP	Layer two Tunneling Protocol	L3TP	Layer three Tunneling Protocol
LDP	Label Distribution Protocol	LSP	Label Switched Path
LSR	Label Switching Routers	MAC	Media Access Control
MD-5	Message Digest five	MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit	n-PE	Network facing Provider Edge
NFV	Network Function Virtualization	NLRI	Network Layer Reachability Information
OS	Operating System	PBB	Provider Backbone Bridging
OAM	Operation, Administration, and Maintenance	PE	Provider Edge
PPTP	Point to Point Tunneling Protocol	PPVPN	Provider Provisioned Virtual Private Network
PW	Pseudo-Wire	QKD	Quantum Key Distribution
QoS	Quality of Service	RARP	Reverse Address Resolution Protocol
RR	Route Reflector	RT	Route Target
RTF	Route Target Filtering	SA	Security Association
SAFI	Subsequent Address Family Identifier	S-BGP	Secure Border Gateway Protocol
SCADA	Supervisory Control and Data Acquisition	SDN	Software Defined Networking
SD-VPLS	Software Defined Virtual Private LAN Service	SPI	Security Parameter Index
SSL	Secure Socket Layer	STA	Spanning Tree Algorithm
STP	Spanning Tree Protocol	TCP	Transmission Control Protocol
TLS	Transport Layer Security	u-PE	User facing Provider Edge
VC	Virtual Circuit	VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol	VPLS	Virtual Private LAN Service
VPN	Virtual Private Network	VPWS	Virtual Private Wire Service
VRF	VPN Routing and Forwarding table	VXLAN	Virtual eXtensible Local Area Network
WAN	Wireless Area Network	WLAN	Wireless Local Area Network

Nowadays, L2VPNs like VPLS are becoming popular among service providers, as are the widely used L3VPNs, because they support multipoint communication and have robust security features. Usually, L2VPNs offer lower operational cost and higher compatibility than L3VPNs, as tunneled L2VPNs are conceptually simpler than L3VPNs [6]. The lower provisioning cost of VPLS can be attributed to its optimal resource utilization. In Hierarchical-HIPLS, where the number of PEs is higher compared to flat VPLS, provisioning cost can be reduced by deploying low-cost u-PEs and medium-cost n-PEs. This is achievable because of the service distribution pattern used by H-HIPLS.

VPLS is an easy way of provisioning an L2VPN. Moreover, VPLS is preferred because of some of its features, like protocol independence and cost-effective operational properties [7] [8]. The primary motive behind VPLS is to connect companies that operate at a global scale as if they are networked on the same Local Area Network (LAN). VPLS offers multipoint-to-multipoint Ethernet connectivity over a Multi-Protocol Label Switching/ Internet Protocol (MPLS/ IP) network [9]. In other words, VPLS merges MPLS and IP technology with Ethernet components, which rectifies the issues of Ethernet technology. In multipoint services, a Customer Edge (CE) device can communicate directly with other CE devices associated with the multipoint service. MPLS Pseudo-Wires (PWs) are used for linking virtual Ethernet bridges.

Initially, VPLS architecture was proposed as a flat architecture, which worked well for small to medium scale networks [9]. But for more extensive networks, flat architectures faced major scalability issues in both data and control planes because of the requirement of a full mesh of PWs. To resolve this issue, a Hierarchical VPLS (H-VPLS) architecture was proposed. The H-VPLS architecture provides a viable solution to the scalability issue by decreasing the number of PWs [7].

Initially, MPLS was used to implement VPLS since it had issues like the discovery of neighbours, scalability, and security. Thereafter, two standard implementations were proposed: (i) Border Gateway Protocol (BGP) for auto-discovery and signaling [10], and (ii) Label Distribution Protocol (LDP) for signaling [11]. These two architectures provided automatic neighbour discovery and signaling solutions, but security remained one of the biggest bottlenecks for VPLS [12]. Subsequently, many other architectures had been proposed to enhance the operational features of these frameworks.

Security is one of the most important areas of VPLS that is open for research. Attacks on VPLS are broadly classified into two categories: (a) attacks on the control plane and (b) attacks on the data plane. Individual solutions have been proposed for mitigating attacks on the control and data planes separately. However, no unified solution for mitigating attacks on both planes currently exists. Henderson *et al.* proposed a Host Identity Protocol (HIP) based architecture [13] for VPLS. For the first time, this architecture introduced security as a separate plane for VPLS, along with the data plane and control plane. The introduction of SDN in VPLS is a recent evolution in this series of advancements [14], [15]. Software-Defined VPLS (SD-VPLS) offers improved tunnel management, enhanced security, and better scalability. Terms used in the context of VPLS, their acronyms, and definitions are listed in Table I.

With the increase in popularity of Ethernet-based packet networks, the community needed a set of standards and tools for Operation, Administration, and Maintenance (OAM). For Ethernet service, OAM defines an area of availability, fault tolerance, and repair [16], [17].

VPLS, unlike VPN, provides multipoint-to-multipoint connectivity. However, current VPLS architectures do not support multihoming (a host device connected to more than one network) [18]. In general, an end-user device or computer network is typically connected to a single network. However, to increase reliability and performance, host devices are connected to multiple networks. This is achieved by providing the option to route the packet through another link in case of link failures. In multihoming, performance is enhanced by offering alternate shorter paths to a destination. In more recent work, all active multihoming is achieved in VPLS by using EVPN [19]. However, the use of multihoming leads to the creation of loops which degrades the network's performance. Initially, a scheme based on Split Horizon was suggested as a solution for loop prevention in VPLS [10]. In this mechanism, a VPLS Provider Edge router (PE) does not forward traffic through pseudo-wire within the same VPLS because all the routers are directly connected. Spanning Tree Protocol (STP) was suggested as an evolved solution for loop prevention [9]. STP uses an algorithm called Spanning Tree Algorithm (STA), which creates a topology database and finds the redundant links. Thanks to STP, Layer 2 switching loops are automatically removed by blocking redundant links.

STP actively monitors all the links in the network to find the redundant links. Whenever there is a change in topology, i.e., if a new link is added or an existing link is removed, STP needs to run STA to create a new database [7]. This may result in higher reconfiguration time. STP allows multiple links, but it does not balance traffic between them. In [18], [20], the authors have proposed novel solutions for implementing multihoming in VPLS.

Historically, VPLS was used only in industrial networks [21]–[24]. At present, VPLS networks are used by enterprises with applications like Data Centre Interconnect (DCI), video conferencing, Voice over Internet Protocol (VoIP), and Internet Protocol Television (IPTV). It is also being used for personal VPN services like Office Network and Home Network. In the mobile backhaul network, it is used along with IP to provide security and Quality of Service (QoS). Grid Computing is another applications of VPLS. Features of VPLS like support for IP, transparent L2 connectivity, strong security features, and efficient connection between two devices help to provide better implementations of Grid Computing [25].

The popularity of VPLS can be understood from the fact that giants like Cisco, Juniper, Samsung, Nokia, and Vodafone are working and providing training on VPLS and related technologies [26]–[30]. LAN services are being promoted by the factors like the growing use of internet technologies, industrial expansion, and innovations in cellular data. It is estimated that the VPLS global market will reach *$2,420 million by 2025*, growing at a *Compound Annual Growth Rate (CAGR) of 19.5%* between 2020 and 2025 [31].

A. Motivation

VPLS is a driving technology for communication in many industries. Nonetheless, it seems that not many survey papers are available discussing the technology in detail. Table II summarizes several survey papers related to VPLS. MPLS is the backbone of VPNs, and its importance is highlighted in [32]. This paper thoroughly discusses the protocol, operation, and application of MPLS in VPNs. Since MPLS uses tunnels for secure communication in VPNs, a survey of the use of IP tunnels is presented in [35]. Various tunneling protocols are discussed in [33] since tunneling is vital to VPLS, as it provides secure connectivity over public networks. VPLS provides Ethernet connectivity between distant areas. In [34], the authors suggested various approaches to extend Ethernet services, such as Metro Ethernet Customer Virtual LAN. The authors in [9] discuss VPLS and its architecture in detail. It describes features of VPLS like MAC addressing, packet encapsulation, loop prevention, auto-discovery, and signaling in depth. It also briefly discusses the advantages of H-VPLS over flat architectures. With an increase in the number of users, scalability and security have become major issues in VPLS. Architecture and applications of SDN are discussed in [37]. In [14], new avenues have been explored, such as Software Defined Networking (SDN), to increase scalability and enhance the security of VPLS. The authors in [36] inferred that the scalability issue of VPLS could be resolved using SDN. In-depth discussion of the security of SDN is presented [38]. In [39], taxonomy and vectors of Distributed Denial of Service (DDoS) attacks in SDN are described. Moreover, techniques to mitigate DDoS attacks are also proposed.

TABLE II: Summary of existing survey papers

Focus Area	Ref. No.	Year	What it talks about	As compared to our survey
MPLS	[32]	2000	A comprehensive literature on MPLS, its working and applications.	Brief discussion on VPN but no focus on VPLS.
Tunneling Protocols	[33]	2000	A short survey on various tunneling protocols used in VPN and their comparison.	No implicit focus on tunnel management in VPLS.
Ethernet	[34]	2004	Discusses several issues and approaches for extending Ethernet services.	No explicit focus on VPLS.
MPLS	[35]	2005	Describes use of IP tunnels in MPLS based VPNs.	No explicit focus on VPLS.
VPLS	[9]	2005	Describes VPLS and its architecture in detail. Explains address learning, loop prevention, hierarchical.	Does not talk about security of VPLS, advance architectures like HIPLS, SD-VPLS.
SD-VPLS	[36]	2014	Discusses use of SDN to provide enhanced efficiency, scalability in VPLS.	No explicit focus on security issues of SD-VPLS.
SDN	[37]	2014	Describes in depth architecture of SDN and functioning of each of its planes.	Does not discuss SD-VPLS.
SDN Security	[38]	2015	Discusses in detail various security attacks and proposed solutions for SDN.	No explicit focus on VPLS.
SDN	[14]	2016	Describes use of SDN in making VPN services easy to use which was developed under CoCo project.	No explicit focus on VPLS.
SDN	[39]	2018	A survey on DDoS attacks on SDN.	No explicit focus on VPLS.

VPLS is one of the popular technologies for multipoint-to-multipoint Ethernet services. However, there is no comprehensive survey paper that provides an in-depth survey of VPLS and its various technical aspects to the best of our knowledge. Thus, the motivation behind this paper is to present an exhaustive survey on VPLS and its current state. We intend to provide readers with a holistic view of VPLS, its various architectures, different technical aspects, evolution, numerous projects in this realm, and lessons learned along with possible future research directions. To emphasize the popularity and progress of VPLS, we have plotted the references used in this work with respect to time (i.e., year of publication) in Figure 2, which shows a continuous increase in interest by industry and researchers in VPLS. It is evident from the histogram that there has been significant work done in VPLS in the last five years. Networking giants like Cisco, Juniper Networks, and Samsung are taking a very keen interest in developing technologies related to VPLS.

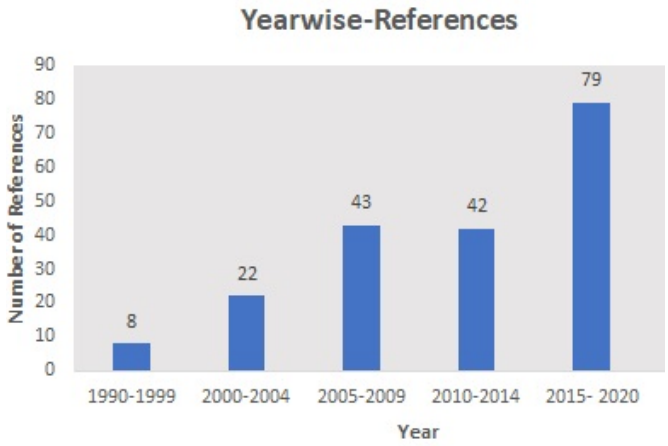

Fig. 2: References Year wise

B. Our Contribution

This paper aims to present an overview of all VPLS architectures (BGP, LDP, HIPLS, and SD-VPLS). The contributions of our paper are listed below:

*1) **Comprehensive Background Study of VPLS**:* The history of VPN networks, along with an associated taxonomy, is presented. A brief outline of various types of VPN is also presented with a major focus on VPLS.

*2) **Discussion of Various VPLS Architectures**:* Current VPLS architecture is discussed, along with an explanation of each of its components. Two categories of VPLS (Flat and Hierarchical) are also explained. Further categorization of flat and hierarchical VPLS (BGP, LDP, HIPLS) and the latest proposed architecture of SD-VPLS are also discussed.

*3) **Identify Key Technical Aspects of VPLS**:* This paper discusses various technical aspects of VPLS like security, compatibility, scalability, operational aspects, tunnel management, and complexity. We have also outlined the related work for each aspect.

*4) **Highlight the Security Challenges in VPLS**:* Identify and discuss various security challenges in each architecture of VPLS. We have also suggested multiple solutions to handle these security threats.

*5) **Discuss Various Evolved VPLS Solutions**:* With an increase in demand and advancement in technology, various enhancements have been added to VPLS as per its application. This paper presents an overview of such solutions (IDN, EVPN, and VXLAN).

*6) **Overview of Research Projects on VPLS**:* This paper discusses completed and ongoing projects related to VPLS and its technologies.

*7) **Future Research Directions**:* Based on our observations, we have underlined existing and significant challenges in VPLS, which must be addressed for further improvement of VPLS. We have also discussed state-of-art for each technical

aspect of VPLS, research gaps, and future directions, which may help researchers contribute to this field.

C. Organization

The remaining paper is organized as follows. Section II presents the history of VPNs and their classifications based on various parameters. This section also discusses current VPLS architecture and its components. Section III focuses on different types of existing Flat VPLS architectures. It also covers the standard implementation of the latest VPLS architecture, which is SD-VPLS. Section IV reviews different types of Hierarchical VPLS architectures. Section V considers the various technical aspects of VPLS and discusses the related work for each of them. The operational aspects of VPLS and related work are presented in section VI. Section VII skims through the evolved VPLS solutions that are designed to mitigate the challenges that have come up lately. Section VIII summarizes some of the interesting VPLS projects (both completed and ongoing). Applications of VPLS are also highlighted in this section. Section IX describes lessons learned and provides the landscape of future work. Finally, Section X concludes the paper. Figure 3 summarizes the outline of this paper.

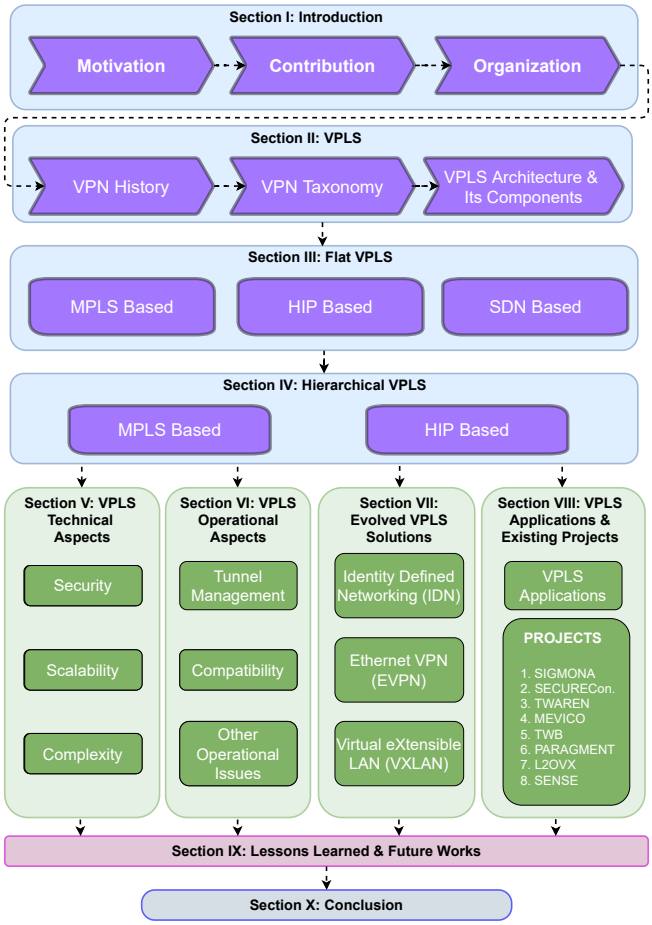

Fig. 3: Outline of this paper

II. Background of Virtual Private LAN Services

This section begins with a discussion of the evolution and taxonomy of VPN services. It also explains the general VPLS architecture and its components.

A. VPN History

A VPN is placed above a packet switched network and comprises of defined parts of packet switched network resources. In a packet switched network, the original data (to be sent) is broken down into smaller units. Each unit is called 'packet', which traverses the network. Moreover, every packet contains a destination address based on which it gets routed through the network. Due to the small size of packets, data paths can be shared among multiple users. A VPN is an assembly of logical nodes and virtual pathways. A virtual path is a logical connection between discrete parts of the network. A VPN also includes a Virtual Circuit (VC), which is a logical connection between network equipment and CE devices [40]. Nodes in the VC communicate as if they are directly connected, but communicate using switches.

In the early '90s, a customer had to either subscribe to some network (public or private) or had to own a private network before availing networking services of a packet switched network. Both subscribing to a network and owning a network had significant disadvantages [41].

In the case of network subscriptions, the user was entirely dependent on the service provider for customized equipment and features. The subscriber had no control over network capabilities like security and accounting services. Scaling was also a big concern with this model. Conversely, in a customer owned network, all of the responsibilities related to operating, managing, and engineering the network were on the network owner. The network owners had significant flexibility, but the flexibility came with considerable responsibilities as well. Furthermore, owning a network was not cost efficient.

VPNs offered an intermediate solution to these problems, i.e., it was neither entirely owned by the service provider nor by the customer. Network operators began to sell bandwidth and connectivity to customers. There was no distinction made for the VPN entity since it worked as an underlay network, meaning there were no major additional requirements for using VPN services. VPNs provided the same quality of service as that of an underlying network. The IETF has set many standards for various categories of VPNs. Some of the RFCs related to VPN are summarised in Table III.

Industries and companies are the major contributors to the growth of VPN technology. In this sector, VPNs are used to control machines operating in remote locations. Industries also use VPNs to share data and disseminate information among offices operating across the globe. Security and privacy are the significant areas of concern when working online. VPNs made it convenient for corporations to communicate securely over a public network.

In their early days, VPNs deployed conventional leased line technologies like T1 and T3 carrier lines. VPNs have evolved significantly with the advent of technology and covered a wider geographical area. Nowadays, VPNs can run

TABLE III: Selected RFCs of VPN

VPN Area	Focus	RFC #	Description
PPVPN	PPVPN	RFC 3809 [42]	Describes generic requirements for PPVPN.
	PPVPN	RFC 4026 [43]	Explains terminologies for PPVPN.
Layer 1	Layer 1	RFC 4847 [44]	Describes framework for Layer 1 Virtual Private Networks (L1VPNs).
	Layer 1	RFC 5251 [5]	Illustrates working of L1VPN in Basic mode.
	Layer 1	RFC 5252 [45]	Delineates an Open Shortest Path First (OSPF) based Layer1 Virtual Private Network (L1VPN) auto-discovery mechanism.
	Layer 1	RFC 5253 [46]	Describes an applicability statement on the use of Generalized Multiprotocol Label Switching (GMPLS) protocols and mechanisms to support Basic Mode Layer 1 Virtual Private Networks (L1VPNs).
Layer 2	Layer 2	RFC 4664 [2]	Describes framework for Layer 2 Virtual Private Networks (L2VPNs)
	Layer 2	RFC 6136 [17]	Explains Operations, Administration, and Maintenance (OAM) requirements and framework for Layer 2 Virtual Private Network (L2VPN)
	Layer 2	RFC 8466 [47]	Presents a YANG data model for Layer 2 Virtual Private Network (L2VPN) Service Delivery
	VPWS	RFC 4667 [48]	Describes L2VPN extension for Layer 2 Tunneling Protocol (L2TP)
	VPWS	RFC 6718 [49]	Illustrates scenarios and associated requirements for pseudo-wire redundancy.
	VPLS	RFC 4761 [10]	Describe functions needed to offer VPLS, and specifies mechanism for the auto-discovery and signaling using BGP.
	VPLS	RFC 4762 [11]	Explains the control plane functions of signaling pseudo-wire labels using Label Distribution Protocol (LDP).
	VPLS	RFC 7117 [50]	Illustrates procedures for VPLS multicast that utilize multicast trees in the service provider (SP) network.
	VPLS	RFC 8220 [51]	Delineate the procedures and recommendations for Virtual Private LAN Service (VPLS) PEs) to facilitate replication of multicast traffic to only certain ports using Protocol Independent Multicast (PIM) snooping and proxying.
	VPLS	RFC 8614 [52]	Explains updated processing of control flags for BGP based VPLS
	IPLS	RFC 7436 [53]	Describes the protocol extensions and procedures for support of the IPLS service.
Layer 3	Layer 3	RFC 4031 [3]	Describes requirements specific to Layer 3 Virtual Private Networks (L3VPN).
	Layer 3	RFC 4110 [54]	Presents framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs) and also provides a reference model for layer 3 PPVPNs.
	Layer 3	RFC 7359 [55]	Illustrates some scenarios in which VPN tunnel traffic leakages may occur because of use of IPv6-unaware VPN and also suggests possible solution.
	BGP/MPLS IP VPN	RFC 4364 [56]	Explains a method by which a service provider may use an IP backbone to provide IP VPNs for its customers.
	BGP/MPLS IP VPN	RFC 4684 [57]	Presents Multi-Protocol BGP (MP-BGP) procedures that allow BGP speakers to exchange Route Target reach ability information.
	BGP/MPLS IP VPN	RFC 4797 [58]	Describes an implementation of BGP/MPLS IP VPNs in which the outermost MPLS label is replaced with GRE.
	BGP/MPLS IP VPN	RFC 7814 [59]	Explains "Virtual Subnet" which is a BGP/MPLS IP VPN-based subnet extension and which can be used for building Layer 3 network virtualization overlays within and/or between data centres.
	IPsec	RFC 2709 [60]	Presents a security model by which tunnel-mode IPsec security can be architected on NAT devices.
	IPsec	RFC 3193 [61]	Explains how L2TP may use IPsec to provide for tunnel authentication, privacy protection, integrity checking and replay protection.
	IPsec	RFC 5282 [62]	Illustrates the use of authenticated encryption algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) protocol.
Evolved VPLS	EVPN	RFC 8317 [63]	Presents the method of fulfilling the functional requirements for E-Tree service with a solution based on Ethernet VPN (EVPN) and Provider Backbone Bridge Ethernet VPN (PBB-EVPN) with few extensions to their procedures and BGP attributes.
	EVPN	RFC 8584 [64]	Describes inefficiencies in the default Designated Forwarder (DF) election algorithm by defining a new DF election algorithm and an ability to influence the DF election result for a VLAN, based on the state of the associated Attachment Circuit (AC).
	EVPN	RFC 8560 [65]	Explains mechanisms for backward compatibility of Ethernet VPN (EVPN) and Provider Backbone Bridge Ethernet VPN (PBB-EVPN) solutions with VPLS and Provider Backbone Bridge VPLS (PBB-VPLS) solutions.
	VXLAN	RFC 7348 [66]	Describes Virtual eXtensible Local Area Network (VXLAN), employed for addressing the requirements for overlay networks within virtualized data centres accommodating multiple tenants.
	VXLAN	RFC 8365 [67]	Illustrates use of Ethernet VPN (EVPN) as a Network Virtualization Overlay (NVO) solution and inspects the various tunnel encapsulation options over IP and their effect on the EVPN control plane and procedures.

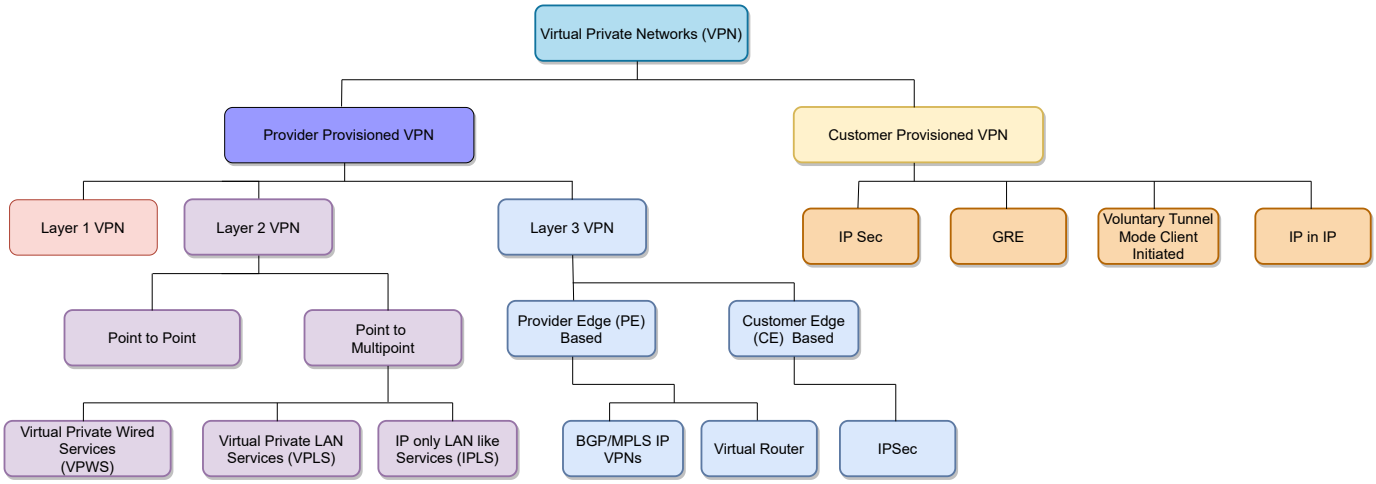

Fig. 4: Classification of VPNs

on almost any Internet connection, such as Digital Subscriber Line (DSL), wireless, and satellite [68].

Earlier VPN services were limited to big corporations and government offices. However, with evolving technologies requiring a higher level of security in data transfer over the Internet, VPN technology has also evolved. With the introduction of technologies like the Internet of Things (IoT) and Buy Your Own Device (BYOD), the use of VPNs tends to rise further. The key benefits of using VPNs are enhanced security and privacy. With ever-increasing demand for privacy in business and professional setup, VPNs are on the road to being omnipresent [41].

B. VPN Taxonomy

In the past, dial-up modems or leased line connections using X.25, frame relay, and Asynchronous Transfer Mode (ATM) were used to provide VPN connections. The network was owned and managed by telecommunication carriers. State-of-the-art technologies like DSL and Fibre optic networks resulted in a significant decrease in cost and increase in bandwidth. Cost reduction and bandwidth availability helped IP-based VPNs to replace earlier VPNs [9]. Moreover, tunnels are established for providing isolation between traffic belonging to different customers. Tunnelling technologies that are usually used in IP-based networks are Internet Protocol Security (IPSec), MPLS, Layer 2 Tunneling Protocol (L2TP), and Generic Routing Encapsulation (GRE) [42], and they are all discussed in section IV.

If a VPN connection is between sites belonging to the same organization, it is called an Intranet. If a VPN is shared by different organizations with a common interest, it is called an Extranet. For instance, an organization's network that is shared with its partner organizations is an Extranet.

VPNs can be classified into different categories. Figure 4 illustrates broader classification of VPNs [42], [43]. The provisioning agent (the party responsible for providing communication services) was considered the most important basis for classification by [69]. Based on this classification, VPNs can be broadly categorized into Provider Provisioned VPNs (PPVPN), and Customer Provisioned VPNs (CPVPN).

PPVPN is the category that is most trusted by industry for secure data transfer over public networks. In this case, a network service provider is accountable for the configuration and management of core VPN services. The objective set for the service provider is secure delivery of data and extended connectivity over shared networks with pre-determined service level assurance. Based on protocols and VPN architecture, once configured, no special software is required for a PPVPN.

Tunnels are established across the Internet by a PPVPN, enabling private traffic to traverse the public Internet without compromising connection or data. A VPN connecting a single user to a corporate network through dial-in, DSL router, or wireless LAN for remote access, will generally use Point to Point Tunneling Protocol (PPTP) or L2TP. If two or more sites are connected using a VPN, then GRE, IPsec, or MPLS protocols are usually used. Thus, PPVPNs are enterprise-level VPNs and can operate on either layer 2 or layer 3. PPVPNs favour ease of implementation and operation. Table IV presents a comparative chart of PPVPNs and CPVPNs based on cost, operation, and other features.

In a *CPVPN*, the customer can configure a VPN independent of the network service provider by deploying CE devices configured with VPN software. CE devices are routers placed near the customer end of the network. One of the most general approaches for establishing a CE based VPN is by creating IPsec tunnels through a communication network.

Since PPVPNs are the most popular type of VPN, our primary focus is on PPVPNs. Based on the layer at which a PPVPN is implemented, it can be subdivided into two categories, i.e., L2VPN and L3VPN. Some of the significant differences between L2VPN and L3VPN in terms of implementation are highlighted in Table V.

Apart from these two popular PPVPNs, there is another category of PPVPN called a Layer 1 VPN (L1VPN). Core layer1 network provides layer1 connectivity between two or more customer sites. Put simply, the data plane in L1VPN operates at layer1. In L1VPN, the customer has some control over the

TABLE IV: Comparison of PPVPNs and CPVPNs

Characteristics	**PPVPNs**	**CPVPNs**	**Remarks**
Configuration and Management of Core VPN services	By Service Provider	By Customer	Customer has a bigger role in CPVPN.
Additional Software requirement	No	Yes	CE devices configured with VPN are installed in CPVPN.
Opex and Capex	Low	High	Due to additional software requirements, the cost is higher in CPVPN.
Flexibility	More	Less	PPVPN supports a larger set of services.
Customization of Services	Limited	High	Customer can choose services according to one's requirements in CPVPN.
Intelligent Devices	PEs	CEs	PEs are under the service provider's control, and CEs are under the customer's control.
Tunnels	IPsec, GRE or MPLS	IPsec(mostly)	IPsec is becoming popular in both.
Scalability of data plane	High	low	Limited connectivity for CE devices in CPVPN.
Operating Layers	L2 or L3	L3 or L4	Layer 2 and Layer 3 communication are preferred by industries.
Security	Highly secure	Low security	PPVPN can support cryptographic algorithms for data encryption.
QoS Support	Low	High	Due to limited services, QoS is high in CPVPN.
Neighbour Discovery	Automatic	Manual Configuration	Automatic neighbour discovery is crucial for effective communication.

TABLE V: Comparison of L2VPN and L3VPN

Features	**L2VPN**	**L3VPN**	**Remarks**
Approach	Martini Approach	Private Routed Network Approach	Martini Approach is taken from chemistry and is also responsible for Transparent LAN.
Communication	Using MPLS based labels	Using BGP based Peer to Peer model	For multipoint to multipoint connectivity, MPLS labels are preferred.
Virtualization	Layer 2 is virtualized	The whole network is virtualized	In layer 2, data packets are not examined for layer 3; hence packet transfer is faster.
Scalability	Less	More	Switches in layer 3 bypass problems related with flat bridged or switched design and thus are more scalable.
Security	Less	More	Layer 3 can provide multiple level of security.
Complex	Less	More	Since layer 3 network cover a larger geographical area as compared to layer 2, variety of devices and protocols make it more complex
Customer Traffic Forwarding	Based on layer 2 information	Based on layer 3 information	Layer 3 switch can perform the function of both layer 2 and layer 3.
IP Routing	Service Provider is not involved in Customer Subnet IP Routing	Service Provider is involved in Customer Subnet IP Routing	Layer 2 can communicate within the network whereas layer 3 can communicate with an outside network as well.
Application	Used by Transport Oriented carriers	Used by carriers serving large VPNs	Layer 2 network is preferred for low to medium traffic rate. In contrast, for a higher traffic rate, layer 3 networks are preferred.

creation and type of connection. A Layer1 network consists of Time Division Multiplexing (TDM) switches, Optical Cross Connects (OXCs) or Photonic Cross Connects (PXCs). One or more links interconnect CE and PE devices. A Layer1 connection is established between a pair of CEs.

In L1VPN, data plane connectivity does not imply control plane connectivity, and the reverse is also true. This indicates the fundamental difference between L1VPNs and L2 & L3 VPNs. In an L1VPN, management of the layer1 network can be outsourced by the customer to a third party. By doing so, the customer is free from the configuration and management of participating CEs. Providers in an L1VPN can make extensive use of spare network resources if a flexible structure is used for layer1. On the other hand, the lack of popularity of L1VPNs is due to the absence of clear instructions for the confinement of connectivity among CEs, the possibility of overlapping customer addressing, and the lack of parameters to support VPNs without some extra addition.

L2VPNs are based on switched link layer technology. A well-designed L2VPN helps in the proper separation of CE and PE devices. It also supports a versatile and rich set of functionalities. Based on the services provided, L2VPNs can be sub categorized as- *Virtual Private Wire Service (VPWS), VPLS* and *IP only LAN like Service (IPLS)* [70].

VPWS is a point to point VPN service in which a CE device is present on each side of the virtual circuit. In this service, frames sent by a CE device on one side of the VC are received by the CE device on the other side. The forwarding of frames from one CE device to another is dictated by the VC on which it is transmitted, and not by the content of the frame [71], so a PE router works as a virtual circuit switch. The PE provides logical interconnection so that a pair of CE devices on each side of the PE appears to be roped by one logical layer 2 circuit. This circuit is further mapped onto tunnels in the service provider network. Tunnels can be either dedicated to a particular VPWS or can be shared amongst

various services. VPWS is available over Ethernet, ATM, and frame relay backbones [2].

VPLS is also sometimes referred to as Transparent LAN Service or Virtual Private Switched Network Service. VPLS, unlike VPWS, is a multipoint layer 2 VPN. VPLS only allows communication between CEs that belong to the same VPLS service category by providing bridged LAN services. VPLS has recently gained popularity as a practical, scalable, and economical alternative for creating metro Ethernet services. The advent of MPLS technology has made VPLS possible. MPLS eliminated the requirement of frame relay and ATM infrastructure by shifting services to an IP network, resulting in a reduction in the network's overall capital and operational cost. MPLS VCs are known as Label Switched Paths (LSPs). In IP/MPLS-based infrastructure, there is no requirement for Ethernet switches to support VPLS. A defined set of standard-based protocols that support all services makes the management of the network simple. To provide the desired service to a customer, the provider installs and configures the correct interface. High-speed connectivity over the layer 3 provider network and advanced auto discovery features are also provided by VPLS.

The primary intent behind IPLS was to provide an alternative to VPLS, for cases where the PE routers are not capable of learning Media Access Control (MAC) addresses through the data plane. IPLS is similar to VPLS except that it only supports L2 packets that contain IP. CE devices in IPLS work as hosts or routers in place of switches. IPLS supports service that carries IP and its supporting packets like Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and Neighbour Discovery. Despite being a functional subset of VPLS, IPLS is treated discretely because different mechanisms may be provided to implement IPLS service, which may, in turn, allow it to execute on a platform that may not support full VPLS functionality. For multipoint connectivity of unicast/ multicast traffic, PE devices avail either Pseudo-wire or discovery [53]. If discovery is implemented, each PE device for each IPLS instance discovers attached CE devices over IP/ MAC address association. In the case of pseudo-wire, each PE device sets up Virtual Circuit Label Switched Paths (VC-LSPs) to all other PEs that support the same IPLS instance [68], [72]. For multicasting, every PE will additionally set up a special pseudo-wire to every other PE in that IPLS instance.

C. Virtual Private LAN Services (VPLS)

Virtual Private LAN Services (VPLS) is a shared packet switched network that provides multiple PW connections. VPLS delivers layer 2 services across a WAN that emulates an Ethernet LAN in all aspects. All sites connected through VPLS appear to be on the same LAN, irrespective of the locations of the sites. This network establishes a private connection, as only CE devices belonging to the same VPLS can participate in the connection. The functioning of VPLS is similar to that of a LAN. CE devices that are members of same VPLS instance can interact and communicate with each other, as if they were communicating over a LAN, using the Service Provider's network [10].

D. VPLS Architecture and Its components

In VPLS, the service provider emulates a layer 2 switch that interconnects different LAN segments of customers. VPLS creates an illusion of CE devices being directly connected, sharing common VPLS instances, when they are actually geographically distant. VPLS built on an MPLS core network is generally preferred by SPs.

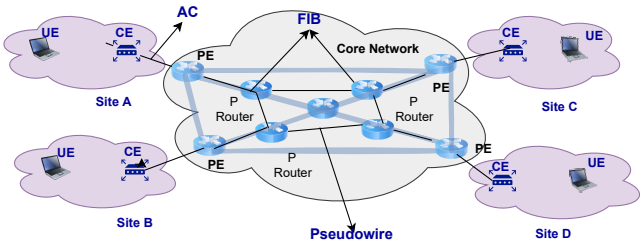

Fig. 5: VPLS components

The main components of VPLS architecture as illustrated in Figure 5 are as following:

- **Customer Edge (CE)** devices act as an interface between customer and provider network. A CE connects to the provider's network for LAN services. Minimal configuration is required from the client side, as CE devices are VPLS unaware. A CE device can be a router or Ethernet Switch.
- **Provider Edge (PE)** devices play a key role in VPLS implementation. PE routers have all VPLS intelligence and functionality embedded.
- **Attachment Circuit (AC)** is used to describe the physical or logical circuit between PE and CE devices. A logical circuit can be a tunnel or a sub-interface. If there are two links between the CE and PE devices, these two ACs can be bundled together, and are referred to as a Link Aggregation Group (LAG). To VPLS, the AC is irrelevant and can form any connection.
- **Pseudo-Wire (PW)** provides end-to-end services across an MPLS network. The PW acts as a basic building block in providing multipoint services. VPLS is a mesh of PWs that are used for creating the bridged domain across which the packet flows.
- **Forward Information Base (FIB)** guarantees traffic isolation. Association of MAC addresses to the logical ports on which they arrive is accomplished by the FIB. It is conceptually equivalent to a routing table. When there is a change in the routing of the network, the routing table is updated and these changes are reflected in the FIB as well. The FIB also stores next-hop information.

III. Flat VPLS

Two possible structures for VPLS architecture are flat and hierarchical. This section discusses various flat VPLS architectures. Additionally, SD-VPLS is also covered briefly in this section. VPLS architecture was initially proposed as a simple or flat architecture. This architecture was proposed for small to medium scale networks. For larger networks, flat architecture

faced scalability issues. Flat VPLS architecture establishes an end-to-end connection between the PE routers to provide multipoint Ethernet services. There is no differentiation between a user facing router (u-PE) and network facing router (n-PE) in flat VPLS. There is only n-PE connected directly to a user device, which increases the load on n-PE in flat VPLS.

All of the VPLS intelligence resides in PE devices, which can provide both VPLS and IP VPN services simultaneously. These are both independent services. The information shared for each type of service must be maintained separately, as different *Address Family Identifiers (AFIs)* and *Subsequent Address Family Identifiers (SAFIs)* are used for this exchange by *Network Layer Reachability Information (NLRI)*. Also, separate routing storage for each of these services must be maintained [10], [56].

In VPLS, PEs communicate with each other to discover all the other participating PEs in the same VPLS instance. A *demultiplexer*, which is placed in a data packet and is used for identifying the VPLS instance and ingress PE, is also exchanged among PEs [10]. Generally, the demultiplexer is an MPLS label. Discovery and demultiplexer exchange are control driven interactions. PEs that are part of the same VPLS instance learn about each other either by manual configuration of identities of all other PEs at each PE or by using some discovery protocol. The latter is called *Auto Discovery*. Since the PEs participating in the same VPLS instance are required to be fully meshed, the former approach is configuration intensive. Also, any change in VPLS topology (addition or removal of a PE) will require an update in the configuration of all of the PEs in that VPLS instance. Each implementation of VPLS has its own benefits and drawbacks. A comparative chart of different VPLS architectures is shown in Table VI.

PE configuration in auto discovery consists only of the identity of the VPLS established on that PE. Auto discovery is used to identify every other PE in that instance. So, a change in VPLS topology affects only the PE where the change has occurred, and other PEs remain unaffected [10]. Functionally, a PE that is part of a given VPLS instance V, must be able to communicate with other PEs in V. A PE must also be able to declare if it no longer participates in V. To perform the above functions, a PE must have means of identifying the VPLS and a way to communicate with all other PEs. The evolution of VPLS over the years is depicted in Figure 6.

1) ***MPLS based VPLS****:* MPLS technology is an amalgamation of connection-oriented forwarding techniques and Internet routing protocol [32]. It leverages the high-speed switching capabilities of an Asynchronous Transfer Mode (ATM) switch along with the IP routing protocol. MPLS is the core network in most of the VPLS architectures. A virtual bridge is simulated by the core to connect numerous attachment circuits on each of the PE devices together and form a single broadcast domain [73] , [74]. There are various MPLS based VPLS architectures like *BGP, LDP and HIPLS*, which are described in the following section.

BGP based VPLS: In general, BGP consists of four basic components which are (i) speakers, (ii) peers, (iii) links and (iv) border routers. A BGP speaker is a host that is responsible for executing the BGP protocol in the network [75]. Two

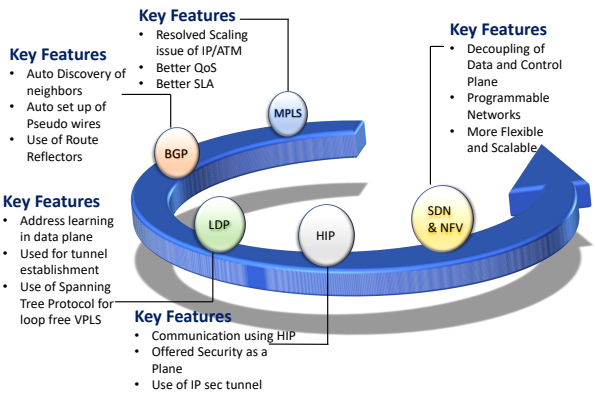

Fig. 6: The evolution of VPLS

BGP speakers that form a connection and are involved in a dialogue are referred to as BGP peers. An internal BGP peer is in the same autonomous system as that of the reference BGP speaker, while an external BGP peer lies in different autonomous systems. The connection between BGP peers is called a link. TCP is used to form reliable BGP links. A border router has an interface to a physical network that is shared with a border router in other autonomous systems [76].

A *Route Target Community* is an extended community that identifies one or more routers that may receive a set of routes (which carry this community) carried by BGP. To avoid overlapping of addresses resulting from the use of private IP addressing by a user network, MPLS VPNs introduced the concept of a separate routing table per VPN in every PE. Each VPN has its own *VPN Routing and Forwarding Table (VRF)*. Each VRF has one or more Route Target (RT) attributes attached to it, which are communicated as an attribute of a route [56].

Signaling is the process of exchanging demultiplexers (involving the establishment and tear down of PWs). Apart from this, signalling also transmits certain features of the PWs that a PE defines for a given VPLS. Signalling starts once auto discovery is completed. A demultiplexer can be exchanged with a PE by sending an update message to all other PEs in that instance. However, this process will create extra load on the PE and the control plane. To reduce this load, the concept of *Label Blocks* was introduced.

LDP based VPLS: A fundamental principle on which MPLS works is that two Label Switching Routers (LSRs) must have consensus on the interpretation of the labels. This concept is used for forwarding traffic between and through LSRs. The Label Distribution Protocol (LDP), which is a set of procedures, is used for achieving this. Information is shared between LSRs regarding the binding each LSR has made [11].

A PE in LDP is ordinarily an edge router that is qualified for executing the LDP signalling and/or routing protocols to establish PWs. Establishing tunnels for communication with other PEs and forwarding traffic via PWs, is also accomplished by a PE [77].

In large networks, flooding is a technique for distributing routing information updates quickly to every node. All unknown frames (unicast, broadcast, multicast) are ran over

TABLE VI: Comparative chart of different VPLS architectures

Property	*LDP*	*BGP*	*HIP Based VPLS*	*SDN Based VPLS*
Path Provisioning	LDP	BGP	HIP	Centralized Control
MAC Table Maintained	At each PE	At each PE	At each PE	Maintained centrally at the controller
Tunnel establishment	Using MPLS	Using MPLS	Using IPSec	Using MPLS or IPSec
Tunnel Parameter Updating	Predefined, Static	Predefined, Static	Predefined, Static	Predefined but can be updated Dynamically
Network Management	Complex	Complex	Complex	Comparatively Simple
Traffic Handling (Broadcast, Multicast and Unicast)	Flooding	Flooding	Flooding	Centrally Controlled
Traffic Engineering	Not Supported	Not Supported	Not Supported	Supported

corresponding PWs to all PE nodes that are part of that VPLS, and are also sent to ACs. It is not feasible to statically configure a PE with every possible association of each destination MAC address and its PW. So, PEs in VPLS should be able to effectively comprehend the MAC addresses of both ACs and PWs and to replicate and forward the packet across both ACs and PWs. In LDP, reachability is learned by a standard learning bridge function in the data plane. In BGP, this is done via the control plane. If a packet with an unknown source MAC address arrives on a PW, then in order to dispatch outgoing packets over a PW to the destination MAC address, each packet needs to be connected with a PW. The case is similar when a packet with an unknown MAC address arrives on an AC.

The overall operation can be better explained with the help of an example, such as the one given in [11]. Suppose we have configured a set up between PE-I, PE-II and PE-III. There are 3 sites S-I, S-II and S-III that are connected through C1, C2 and C3 respectively as depicted in Figure 7. VPLS is initially set up so that P-I, P-II and P-III have a full mesh of Ethernet PWs. The VPLS instance is assigned a unique identifier called an Attachment Group Identifier (AGI), which identifies the type of name of the VPLS. Consider that PE-I signals PW label 102 to PE-II and 103 to PE-III. Similarly, PE-II signals PW label 201 to PE-I and 203 to PE-III. Assume that a packet from C1 is moving towards C2. When the packet departs C1, assume that it has a source MAC address M1 and destination MAC of M2. If PE-I does not know where M2 is, it will flood the packet to PE-II and PE-III. Upon receiving the packet, PE-II will have PW label 201. So PE-II can conclude that the source MAC address M1 belongs to PE-I. It can therefore associate MAC address M1 with PW label 102.

*2) **HIP based VPLS**:* The main idea behind Host Identity protocol enabled VPLS (HIP-VPLS) was to provide secure VPLS architecture. In the HIP, hosts use public keys to authenticate each other over IP and use Encapsulating Security Payload (ESP) to establish secure data channels. HIP decouples the endpoint identifier and locator roles of the IP address. Based on public key security infrastructure, HIP introduces Host Identity name space [68], [78]. A cryptographic host identifier replaces all instances of IP addresses in an application. It provides secure methods for IP multi-homing and mobile computing. There are certain limitations of current IP addressing, mentioned below, which can be overcome using

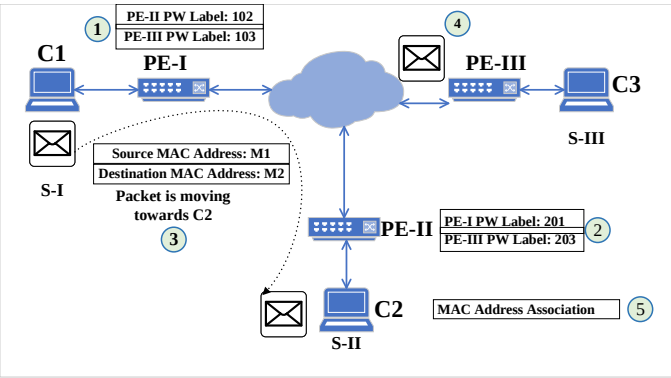

Fig. 7: LDP address learning [11]

HIP: (i) In IP, it is not possible to change a host address without hindering the transport layer connection. By separating the end point identifier and locator roles of the IP address, this can be resolved. (ii) IP networks are vulnerable to spoofing attacks as machines have no consistent and verifiable identity. HIP provides a way of authenticating machines. (iii) The lack of bilateral authentication and authorization of machine communication leaves machines exposed to north-south and east-west attacks. Using HIP, machines authenticate each other and set up a secure tunnel for communication [7].

PWs in HIP-VPLS consist of HIP enabled ESP tunnels. PE devices are interconnected using IP networks (IPv4 or IPv6 or hybrid). PEs in HIP-VPLS are responsible for:-

1) Providing a secure tunnel over which layer 2 frames may travel between CEs, which are interconnected by the VPN.
2) Authentication of the peer PE devices belonging to the same overlay.
3) Maintaining Access Control Lists (ACLs) that define which CEs are permitted to communicate with other CEs.

At the protocol level, PE devices know each other by a name, HIT, which is the hash of the host identity public key. The operational name of the PE device is bound to the HIT using certificates. A common set of Certification Authorities (CAs) must be shared amongst all the PE devices in an overlay. A network operator must at least define a unique overlay name and must authorize the PEs that belong to that overlay.

*3) **SDN based VPLS**:* VPLS has found its application from industrial networks to mobile backhauls. Increased demand for VPLS is accompanied by additional operational requirements, like enhanced scalability and security, optimal use of network resources, ease of provisioning and traffic engineering. Existing VPLS architectures fail to provide these features, due to their complex, static and inflexible nature. SDN-based VPLS addresses three major issues faced by traditional MPLS-based VPN and VPLS architectures:

1) *Complexity in Service Provisioning:* In traditional VPN services, a Service Provider (SP) must learn the complicated VPN configuration for provisioning and maintaining VPN services. This is a time consuming process. The complexity further increases in a multi-vendor environment, where each device has its own specific set of instructions.
2) *Expensive Devices:* A considerable number of control plane functionalities are implemented in PE devices due to the vertical integration of the control plane and the data plane in current architectures. To achieve this, a network must use expensive and high performance routers. Considering the growing number of users, it is not cost effective for SP to use many such devices.
3) *Scalability:* This is one of the most serious concerns for VPLS services. PE devices come under heavy load as the number of devices is increased to meet growing demand. Tunnel establishment time also increases with the increase in the size of the network.

SDN and NFV can be used to provide flexibility, security and scalability to the dynamic design of a VPLS architecture. In principle, SDN is a centralized routing approach. It decouples the data plane from the control plane. An SDN network consists of three planes: Data plane, Control plane and Application plane. The devices in the data plane are responsible only for the forwarding of traffic, whereas all the intelligence lies in a controller, which is the main component of a control plane.The controller dictates the overall behaviour of the network. The channel via which the data plane and the control plane communicate is referred to as the control channel. This control channel is established using SDN control protocols. In the application plane, network control functions and services are implemented as software applications [79].

The data plane devices receive a set of rules from the controller, known as flow entries. These entries are stored in local flow tables to determine the forwarding behaviour of the data plane devices. When a packet is received by a data plane device whose matching conditions are specified in the flow entry, the specified actions are taken accordingly. If there is no matching entry for the packet, it is forwarded to the controller for the required action.

On the one hand, globalization requires networks to be more secure, scalable and agile. These requirements have led to the advent of SDN, which is a new paradigm that allows software networks [37]. On the other hand, VPLS is one of the leading technologies for connecting business enterprises. Thus the use of SDN in the realm of VPLS is expected to enhance the capabilities of VPLS. More specifically, SDN can be applied in VPLS to enhance security, scalability and make the network more programmable, which increases flexibility and agility. So, one of the recent technological advancements in the field of VPLS is SD-VPLS.

An SD-VPLS architecture is defined in [36], comprised of six components- Island controller, Domain Controller, DE device, D device, DBE device and IE device. An island represents each LAN in the architecture. The Island Controller is situated inside the client's site and is responsible for managing the OpenFlow switch. It also manages the acceptance and forwarding of the packets to the provider's network. The Domain Controller manages traffic between islands of the same or other provider networks. It is responsible for managing several OpenFlow switches in the core network. DE is an acronym for Domain Edge device, which is an OpenFlow switch connecting Island(s) to a Domain. In the Domain network, an OpenFlow switch is referred to as a domain device or D device. A Domain Border Edge (DBE) device is an OpenFlow switch interconnecting various domains. An Island Edge (IE) device, which is also an OpenFlow switch, interconnects Islands to Domains. Figure 8 illustrates its architecture.

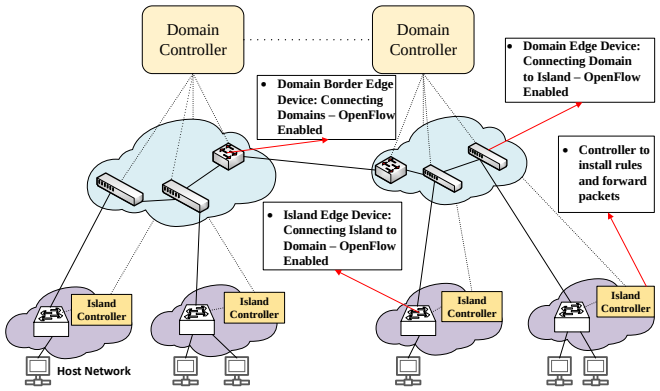

Fig. 8: SD-VPLS components

IV. Hierarchical VPLS

Due to scalability issues in flat VPLS architecture, it cannot be deployed in large-scale networks. The hierarchical architecture of VPLS provides a feasible solution to address scalability issues. A flat VPLS architecture requires a full mesh of PWs between each pair of PEs. So, if there are N PEs in the VPLS network, $O\ (N * (N-1)/2)$ PWs are required for each VPLS [80]. This is referred to as the N Square Scalability Problem. A flat VPLS architecture faces the following scalability issues due to the requirement of a high number of PWs:

- Because of the establishment and maintenance of such high numbers of PWs, there is huge signalling overhead.
- Each PE has limited support for hardware ingress replication and simultaneous tunnels. A PE failing of N hardware ingress replication will result in re-sending of broadcast frames N times in the same network, which in turn will exhaust N times the allocated bandwidth, thereby reducing the scalability of the forwarding plane.

- To forward the frame through a network, a PE must have complete knowledge of the network. Thus, PEs are required to maintain huge forwarding tables. As a result of massive forwarding tables, PEs need to conduct extensive searching to locate the correct destination address.
- Addition and deletion of new PE are tedious, and hence service provisioning is difficult.

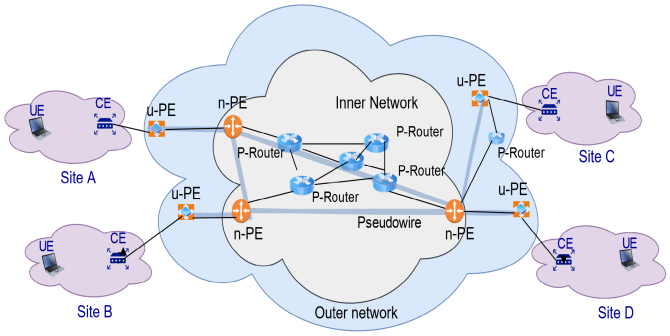

Fig. 9: H-VPLS components

H-VPLS addresses the issue of scalability by reducing the number of PEs that are connected to full mesh topology. Hence, it requires a lower number of PWs than flat VPLS. Just like flat VPLS, H-VPLS can be implemented using BGP, LDP and HIP. Table VII presents a feature comparison of different H-VPLS architectures. In general, H-VPLS has two types of PEs. User facing PEs are called u-PEs, and network-facing PEs are called n-PEs. A u-PE works as the aggregation point and forwards all the packets to the next n-PE. All of the brainpower of VPLS architecture lies in the n-PEs. These are responsible for learning addresses, forwarding packets and auto discovery. Figure 9 illustrates the H-VPLS architecture.

*1) **MPLS based VPLS**:* The popularity of MPLS in VPNs can be attributed to the ability of MPLS to forward packets over random non-shortest paths and emulation of high-speed tunnels. This combines the advantages of both layer 3 routing (connection-less) and layer 2 forwarding (connection-oriented).

BGP based H-VPLS: Hierarchical BGP is one of the solutions for the scaling problem of VPLS at the control plane. In VPLS, control plane scaling is required to alleviate the full mesh connection among VPLS BGP speaker. It passes message only to the interested speaker rather than all the BGP speakers and simplifies the addition and deletion of BGP speakers in the network.

In hierarchical BGP, Route Reflectors (RR) [81] are used. An RR is a BGP speaker that can re-advertise or reflect external route information sent by other BGP speakers to Internal-BGP (IBGP) peers, which is otherwise not the case in IBGP. As RRs are fully meshed, a BGP session is established between each BGP speaker and one or more RRs. This eliminates the need for direct full mesh connectivity among all BGP speakers. This technique can be applied recursively if a large number of RRs is required by the provider for scaling.

In contrast to the definition of hierarchical VPLS, the use of RRs is a control plane technique, and it does not in any way change the forwarding path of VPLS traffic. Multiple sets of RRs can be defined, and a particular RR does not need to handle all messages from a given PE. To limit the VPLS message passing to interested speakers only, Route Target Filtering (RTF) [57] is used. RTF limits the distribution of routes only to those systems for which it is necessary. Although the use of RTF is orthogonal to the use of RR, they work well in conjunction.

LDP based H-VPLS: Extending the VPLS tunneling technique into the access switch domain is often beneficial. This can be achieved by treating the access device as a PE and establishing PWs between it and other edge devices. VPLS core PWs are referred to as the hub, and access PWs as spokes. Hubs are augmented with spokes for 2-tier hierarchical VPLS. A spoke PW terminates on a virtual switch instance on the Maximum Transmission Unit (MTU-s) and the PE-rs, unlike traditional PWs, which terminates on a physical port. For hierarchical connectivity the following elements are used:

- **MTU-s**- This is a device supporting layer 2 switching functionality. It performs general bridging tasks(learning/replicating) on all of its ports. Spokes are also included as they are treated as Virtual ports. As MTUs can bridge, a single PW per VPLS instance is sufficient for any number of access connections in the same VPLS instance. This further reduces signaling overhead between MTU-s and PE-rs.
- **PE-rs**- VPLS bridging functions, routing and encapsulation (MPLS) are performed by PE-rs. This device's operations are independent of the device present on the other side of the spoke. PE-rs switch traffic between spokes, hubs and ACs once the MAC address has been learnt.
- **PE-r**- This is a device capable of routing but not bridging. It is also capable of provisioning PWs between itself and other PWs.

*2) **HIP based H-VPLS**:* Liyanage *et al.* [80] proposed a hierarchical architecture using the HIP protocol. The main aim of Hierarchical-HIPLS (H-HIPLS) is to help in the implementation of hierarchical architecture, support dynamic address learning mechanisms and provide added security functionalities to traditional VPLS architecture. These security functionalities include authentication, integrity and confidentiality. H-HIPLS is a modification to the HIP-based session key mechanism. Security features of the HIP are used to establish a secure connection over a VPN. In this architecture, the scalability of the security plane remains the same but scalability for the control and forwarding planes is increased.

The complete overview of VPLS - architecture, implementation and usage is presented in Figure 10.

V. VPLS Technical Aspects

In this section, technical aspects affecting the implementation and operation of VPLS are discussed. There can be various factors affecting the functioning of VPLS, but in this section, a broad discussion is presented.

A. Security

Security refers to maintaining integrity, confidentiality and accessibility of the network and data. Security measures act as

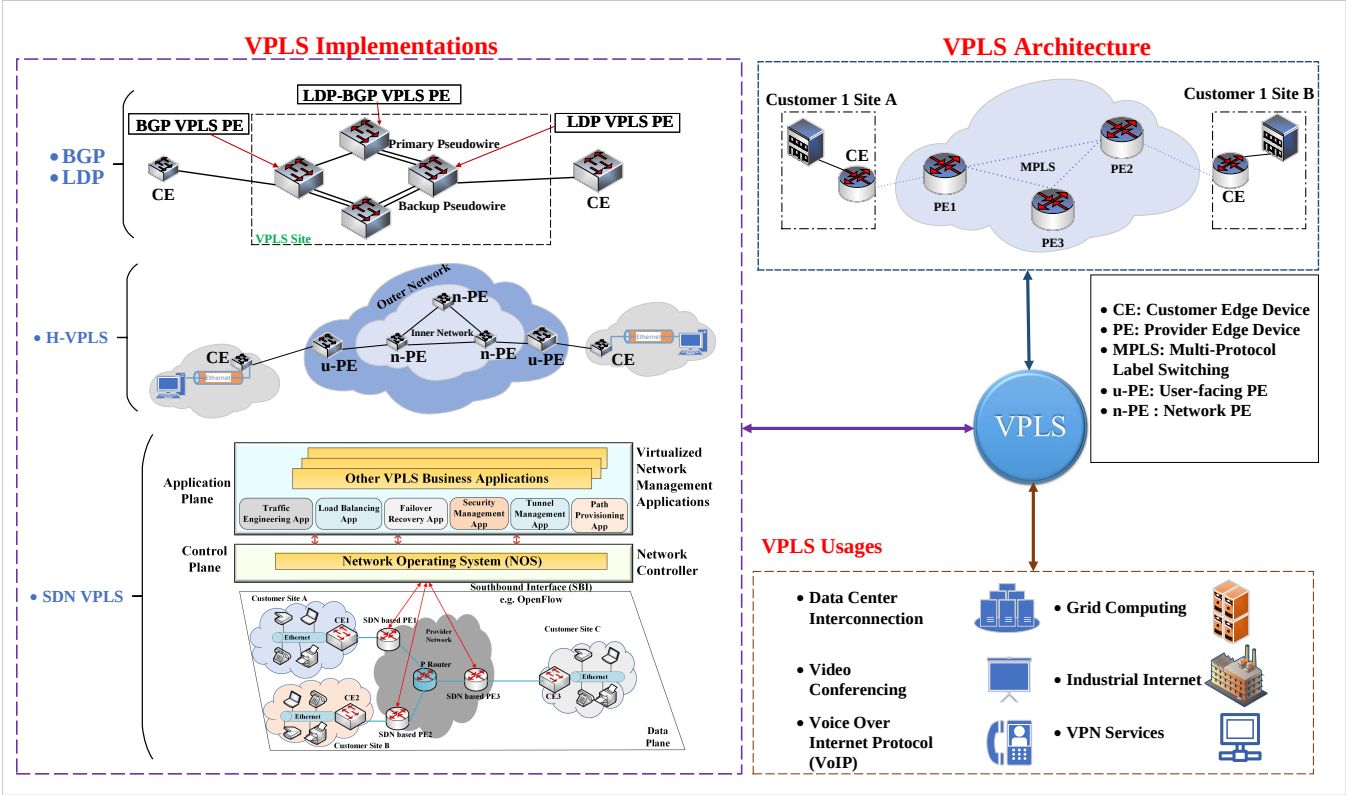

Fig. 10: Panoramic view of VPLS architecture, implementations and applications

TABLE VII: Comparison of different hierarchical architectures

	Hierarchical LDP	Hierarchical BGP	Hierarchical HIPLS
Control Plane Scalability	✓	✓	✓
Data Plane Scalability	✓	✓	✓
Security Plane Scalability	×	×	✓
Data Traffic Encryption	×	×	✓
Multiple Protocol Support	✓	✓	✓
IP Attack Protection	×	×	✓
Control Protocol Protection	×	×	✓

a defence mechanism against external as well as internal malicious users and mitigate security attacks. A security breach in a PPVPN may result in a replay, observation, modification or deletion of user data, injection of malicious data into the network, traffic pattern analysis, degradation of Quality of Service (QoS) of PPVPN or disruption of service [82].

VPLS aims to provide secure data flow over a public network. The PPVPN core and each PPVPN is defined as a trusted zone, each of which is a separate entity, hence trusted zones are distinct. However, sometimes the PPVPN core network provides Internet access. In such a case, a transit point is defined for security purposes [82]. The PPVPN allows restricted and controlled communication between trusted zones through precisely defined transit points.

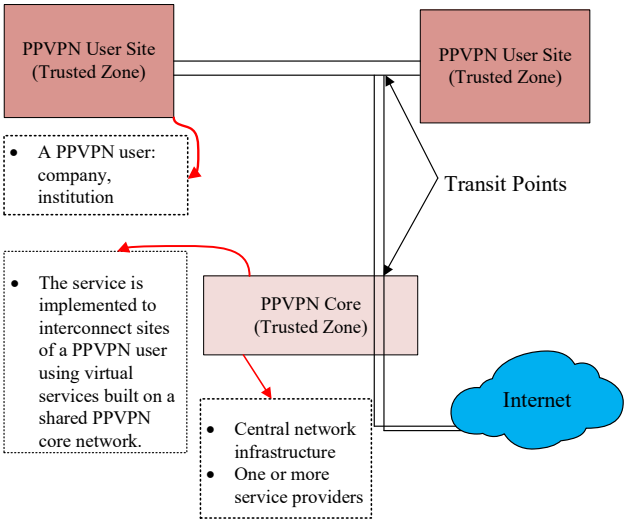

Fig. 11: Trusted Zones in PPVPNs [82]

The foremost requirement of a VPN is to share core infrastructure with other VPNs, which should not expose the security of a trusted zone. A primary security concern is an attack from outside the trusted zone that penetrates inside this zone [82]. Figure 11 illustrates the concept of trusted zones. Besides this, threats can also be posed by - user of other

PPVPNs sharing the same PPVPN service provider, the person handling the PPVPN for the service provider, attacks from the Internet and intra VPN threats [83] [84]. Various threats to the security of PPVPNs can be categorised as:

1) Attacks on the data plane: Attacks that involve a threat to user data (from the point of service provider) are included in this category.

- *Sniffing:* Sniffing of user data can be done in two ways based on [82]. First is unauthorised monitoring of VPN packets and analysis of their content. This threatens the confidentiality of the information. The data captured in this way can be modified and re-inserted into the network by an attacker. The second is an unauthorised analysis of VPN packets and inspecting aspects or meta aspects of packets so that they can be interpreted even if the packets are encrypted. Useful information can be gained by observing the flow and timing of traffic, size of packets, and source and destination addresses. Such attacks are significantly less of a concern compared to other attacks.
- *Spoofing and Replay:* Spoofing refers to impersonation by an attacker as an authorised user of a network [85]. Using this identity, the attacker inserts unauthorised packets into a VPN, with the aim of these packets being accepted as legitimate data by an authorised recipient [86]. Replay means recording legitimate data sent earlier and then re-inserting copies of the same data on the network.
- *Unauthorised modification and deletion of data:* This refers to illegitimate modification in the contents of packets or dropping of packets while they are traversing the network [87].
- *Denial of Service (DoS) attack:* In DoS attacks, the attacker aims to interrupt or prevent a legitimate user from accessing services [88]. DoS attacks can be carried out by flooding network devices with service requests (resource exhaustion), taking network devices out of service and changing the configuration of devices. Resource exhaustion targets resources like bandwidth, CPU power, routing, and session capacity. For instance, resource exhaustion can be carried out on the data plane of a particular PPVPN by trying to spoof an enormous quantity of data into the VPN from outside [89]. Such an activity may exhaust the bandwidth available to the VPN or overwhelm the cryptographic authentication algorithm.

2) Attacks on the control plane: These attacks target control structures operated by VPN service providers.

- *DoS attacks on network infrastructure:* These attacks target the general infrastructure of the service provider, for instance, routers or mechanisms that a service provider requires to provide VPN services, e.g. tunnels [82]. One special kind of DoS attack is when one of the VPN users is consuming excessive network resources, denying services to other VPN users.
- *Unauthorized access to network equipment:* In this attack, the service provider's equipment is reconfigured to obtain desired information. These attacks are carried out by gaining unauthorized access to the service provider infrastructure [82].
- *Social Engineering attack:* These attacks may be mounted through manipulation of a service provider employee [90]. Compromised personnel may inappropriately disclose confidential information or damage or reconfigure the network. PPVPNs are more susceptible to these types of attacks than CPVPNs [82].
- *Traffic Cross Connections:* Misconnections in VPN may happen because of service provider or vendor error or by the action of an attacker [82]. These attacks breach the isolation between distinct PPVPNs, which can lead to a site being connected to a wrong VPN, improper merging of two or more VPNs, or packets or frames being improperly delivered outside the VPN. The breach may be logical (improper device configuration) or physical (CE-PE link).
- *Attack against routing protocol:* These are the attacks mounted against the routing protocols operated by a service provider that directly supports VPN services [83]. These attacks relate to membership discovery (in layer-3 VPNs) or membership and endpoint discovery (in layer-2 VPNs).

  In BGP-based VPLS, all the exchanges on the control plane are done using BGP messages. To enhance security at this level, a new TCP option was introduced [91] for carrying a Message Digest5 (MD5) in a TCP segment. MD5 is defined as essentially a checksum which is used to validate the authenticity of a file or a string [92]. A new security architecture was proposed by [93] which effectively addressed various vulnerabilities in BGP. Significant threats to LDP-based VPLS are Spoofing and DoS attacks based on [94]. HIP-based VPLS mitigates DoS attacks, TCP reset attacks and spoofing attacks by encrypting both the control and data traffic of the VPLS [95]. Simulation outcomes of [96] show zero dropped packets during a TCP SYN DoS attack. In session key based HIPLS (S-HIPLS), PEs are authorized using ACLs provided by the operator. It also restricts CEs from misbehaving [97].

3) Security of SD-VPLS: We have taken up the security of SD-VPLS as a separate section because SD-VPLS is a comparatively new architecture for VPLS, and its security has not been explored much. In addition to this, SD-VPLS is vulnerable to additional security threats that are not discussed in the previous section. As there is centralized control in SD-VPLS, security policies can be efficiently implemented without any redundancy. SD-VPLS supports centralized control and orchestration of security mechanisms. Malicious behaviour can be easily detected, as the controller can analyse historical and real time network status and performance. The controller is capable of making proactive decisions to mitigate security attacks, with a higher degree of accuracy [98].

In SDN architecture, the controller is responsible for the implementation of the policies. So, it naturally becomes a single-point-of-failure and a target of DoS attacks for all SDN-based systems, including SD-VPLS [14]. The controller itself is a software application running on some operating

TABLE VIII: Various attacks on SDN system and their possible effects on SD-VPLS [79] [99] [100] [101]

Plane	Attacks	Attack Description	Possible Effects on SD-VPLS
Application Plane	Third party Attack	Malicious application takes complete control of network as they have visibility of complete network	Attackers can avoid intrusion detection system and compromise the tunnel management functions, i.e., tunnel establishment, life cycle management and encryption of the VPLS network
	Storage Attack	Application gets access to shared storage which can be illegally exploited	Manipulation of internal database and unauthorized access to the security key material
	Control Message Attack	Application generates arbitrary control messages which affect network functioning like addition or deletion of flow rules	Change in flow rules or overflow of flow tables to jeopardise the routing in the VPLS network
	Resource Attack	Compromised application may exhaust critical resources like CPU and memory	Degradation of network performance.
Control Plane	Manipulation Attack	Adversary manipulates the understanding of SDN controller about the network, which results in improper decision making	Compromised decision making like packets diverting from the actual path can leading to high latency and congestion in VPLS tunnels
	Availability Attack	Attacker's aim is to make SDN controller unavailable for some period or to some part of network	Unavailability of controller leads to delay in traffic routing functions such as flow rule communication, delayed routing decisions and also VPLS tunnel management decisions
	Software Hacking	As the controller is hosted on a server, which has a variety of software including OS, it is susceptible to software hacking	If the OS of the controller is hacked, it can bring down the whole VPLS network, attack on other software can lead to illegal updating of information.
Data Plane	Device Attack	Software and hardware vulnerabilities of SDN enabled switches are exploited to compromise data plane	Compromised device can lead to unavailability of services and forwarding policy leaks. In this way, attackers can either terminate VPLS tunnels or extract the user data in VPLS tunnels.
	Protocol Attack	Attacker takes advantage of vulnerabilities of a network protocol in forwarding devices like exploiting vulnerabilities	Denial of Service and information disclosure.
	Side Channel Attack	Forwarding policy and identities of devices are deduced by the attacker just by analysing the performance of the forwarding device	Leak in routing patterns may result in identifying important devices/ components in VPLS network. Later, this information can be used to mount attacks on such devices
North Bound API	Availability Attack	Information exchanged between application plane and control plane is hampered by disrupting the functioning of API	As communication is interrupted between application plane and control plane, tunnel establishment and traffic routing within the tunnels are hampered and latency increases.
South Bound API	Eavesdropping	Attacker tries to learn about the information exchanged between control plane and data plane by monitoring traffic	By analysing traffic patterns, an attacker might obtain sensitive information and identify the key components in VPLS network to mount future attacks.
	Interception	Attacker tries to manipulate network behaviour by modifying control messages exchanged between control and data plane	Manipulation of control messages may lead to unpredictable behaviour of network like network policy not implemented properly, and disclosure of forwarding policy.

system (OS). This OS, in turn, has its own threats such as security patches that are not up to date and use of insecure protocols [79]. Various security challenges of SDN are shown in Figure 12.

Data plane devices are shared with other network services that are also in the SD-VPLS architecture. Such sharing opens the door for a direct or indirect attack on data plane devices. Moreover, any attack on other network services might result in a total halt of operation of SD-VPLS.

Since SD-VPLS is based on software controlling the need for a robust authentication mechanism at the application level, it becomes imperative for the uninterrupted operation of SD-VPLS, as it is comparatively easier to attack a software-based system than it is to manipulate black box type hardware. The introduction of new elements in SD-VPLS also increases the surface for attacks. It is critical for the security of SD-VPLS to ensure trust between management applications and new elements like hypervisors, virtual machines and virtual switches [98].

Related Work on VPLS Security: Security related work on VPLS can be categorised according to VPLS implementation (BGP and SD-VPLS). In [102] and [103], the authors propose solutions to deal with the security threats of BGP, whereas, security solutions for SDN-based VPLS are presented in [104]–[108]. Recent solutions like [109] and [110] use linear equations and dynamic packets respectively. DoS attack mitigation approaches for SD-VPLS have been proposed in [111]–[113]. A security kernel is used by [114] to elude rule conflicts. An OpenFlow based solution is proposed by [115]. Next, we discuss each of these related works.

Due to the lack of complete integrity and authentication messages, BGP is vulnerable to various attacks such as prefix hijacking, route leaks, and spoofing, which result in significant disruption of services and performance degradation. A prefix is a set of consecutive IP addresses. Prefix hijacking refers to the generation of prefixes (owned by other networks) by an unauthorised network. It is a serious threat to data privacy as well as service availability. In this context, [102] proposed

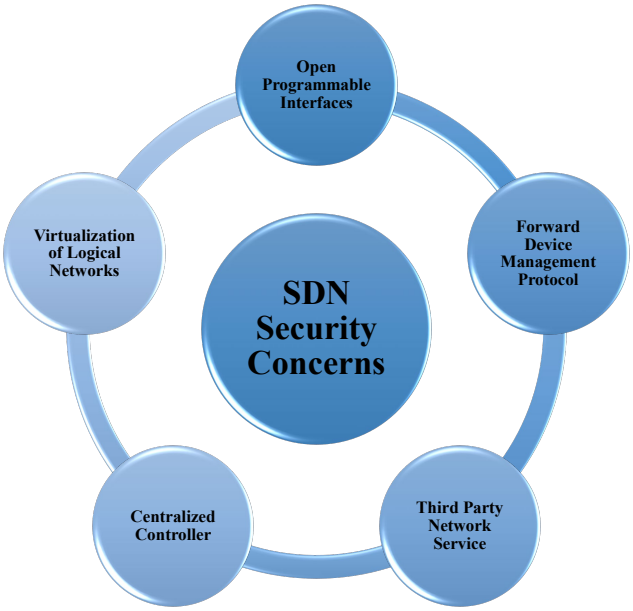

Fig. 12: SDN security challenges

the BGP graph approach, which used visualisation methods for root cause analysis. This proposal identifies both small scale and large-scale anomalies in a system. Previous solutions aim to identify time windows that had anomalies and required further processing for root cause analysis. The authors in [103] applied a machine learning approach to quickly collect anomalies and take action when they occurred. In this approach, an unsupervised clustering technique is applied to message logs for anomaly detection.

As compared to traditional networks, SD-VPLS helps in making the network programmable and agile. However, along with this, the network also inherits security threats associated with an SDN architecture. Frontiers on which attacks can happen in an SDN architecture include: open programmable interfaces, management protocol installed on forwarding device, logical networks, third party network services and centralized controller. Figure 12 shows various attack points in the SDN architecture.

There are three programmable interfaces in SDN: -i) Northbound API (application plane to control plane) ii) Southbound API (Control plane to data plane) iii) Interface for communication between different interconnected controllers. The forwarding device management protocol helps in the configuration and management of programmable forwarding devices. Virtual logical networks consist of NFV, which focuses on optimising network services by decoupling network functions. Third party services are allowed in SDN to facilitate easy customization and reduction in the cost of proprietary services. The centralized controller has a global view of the network and instructs forwarding devices, following the rules defined in the application plane. Attackers can thus target different SDN planes to carry out various types of attacks [116]. Table VIII describes security threats related to different SDN planes.

Various solutions to improve the network security of SDN have been proposed, like FortNOX [104], FlowChecker [105], and Veriflow [106]. However, none of these has been able to provide comprehensive security. Moreover, solutions like [106]–[108] work under the assumption that all or a majority of forwarding devices in the data plane are trustworthy, which is not always the case. Therefore, these solutions are incapable of handling adversarial settings (untrustworthy forwarding devices). SPHINX [117] and Wedgetail [118] consider the possibility of untrustworthy forwarding devices. SPHINX makes use of flow tables, which helps in incremental validation. Wedgetail is proposed as the first intrusion prevention system for the SDN data plane. More recently, FOCES [109] has been proposed as a solution that captures correct forwarding behaviour as a linear equation system. FOCES can detect network-wide anomalies without defining dedicated rules for them. DynPFV [110] is another solution that uses dynamic packet sampling to verify the integrity of packets on the network.

Solutions like McNettle [111], Disco [112], and HyperFlow [113] aim to handle DoS attacks by increasing the processing power of NOS, using a distributed approach. FRESCO [114] is another solution that consists of an application layer and security enforcement kernel. The security enforcement kernel is used for avoiding rule conflicts. COFFEE [115] is an OpenFlow-based solution for detecting and mitigating botnets.

Summary: Due to distributed control in traditional networks, the use of security enforcement and updating configuration is complicated. By separating the control plane and the data plane, SDN provides an opportunity to address these issues. The use of machine learning and linear equations has helped in detecting anomalies more accurately in the network. Most of the solutions do not consider adversarial settings such as untrustworthy devices or internal threats. As such threats are more detrimental and difficult to detect, solutions addressing such adversaries should be designed. Wedgetail and Sphinx consider such attacks for SDN-based systems, but they still need to be tested on real world network setups, which would allow testing of Wedgetail and SPHINX on parameters such as trajectory projection, more attack scenarios, strength of hash, and different use cases. Furthermore, though various works have addressed different security issues in VPLS, it is challenging to propose an overall comprehensive framework for the security of VPLS due to the diversity of protocols and technologies used in VPLS. For better utilization of VPLS technology, more focus needs to be placed on addressing security threats so that users can send sensitive data over a public network more reliably and securely.

B. Scalability

Scalability refers to the ability of a system to grow or shrink with an increase or decrease in the size of the network without affecting its efficiency or quality. As VPLS is widely used by corporate offices that continue to expand their ventures all over the globe, scalability becomes a major concern. The scalability of VPLS can be categorised into three subsections: (1) Control plane scalability, (2) Data plane scalability and (3) Security plane scalability.

1) Control Plane Scalability: Auto discovery and establishment and withdrawal of PWs are two primary functions of a control plane in a VPLS architecture. In a flat VPLS architecture, the scalability issue arises because of the requirement of a full mesh of PWs among VPLS peers for communication. In addition to this, broadcasting messages to all speakers also deteriorates the scalability of VPLS [119].

The hierarchical architecture of VPLS solves the scalability issues to a great extent. VPLS architectures like HIPLS and SD-VPLS have higher control plane scalability than flat architectures like BGP based VPLS and LDP based VPLS. In [120], the authors proposed a method to use the same tunnels or PWs for multiple customers to increase the scalability of VPLS.

2) Data Plane Scalability: Encapsulation of Ethernet frames and forwarding packets are two vital tasks performed by the data plane in VPLS. A major scalability issue in the data plane is MAC table explosion [11]. Suppose N customer terminals are connected with every PE router for each service instance. Assuming M sites in the customer network, the total entries stored in each PE are $N \times M$. If there are 25k terminals and 10 sites, then each PE router has to store 250K entries. This number is considerably larger than most Ethernet switches can handle [34].

The authors in [121] proposed a MAC address translation scheme using Locally Administered Address (LAA) to resolve the MAC table explosion problem. LAA is used in Network Management. The proposed scheme used LAA for MAC address translation in PE routers. Using this scheme, the number of entries in PE routers can be reduced from $N \times M$ to $N+M(M-1)$. A MAC address ageing mechanism should also be included in PEs so that unused entries can be removed, to efficiently utilize the limited memory.

3) Security Plane Scalability: HIPLS introduced a security plane into the VPLS architecture, and thus it was the first architecture capable of providing secure VPLS. Security was not considered in previous architectures like BGP-based VPLS and LDP-based VPLS. In HIPLS, scalability issue in the security plane arose because of complexity in key storage [6]. Every PE has to store $O(n)$ keys, where n is the number of PE routers in the network. This was very resource exhausting. To overcome this, the authors in [97] introduced Session-key based HIPLS (S-HIPLS). It overcame the scalability issue by using the session key for the security mechanism. The number of keys stored on PEs was reduced from $O(n)$ to $O(m+1)$, where m is the number of VPNs and n is the number of PEs in the network. So the number of keys stored on each PE became independent of the number of PEs in the network.

SD-VPLS is another secure VPLS architecture [98]. In SD-VPLS, security is a concern for forwarding devices as well as the controller. The SD-VPLS data plane and control plane are exposed to several attacks like DDoS and flow poisoning. With an increase in the size of the network, it becomes difficult to ensure security in SD-VPLS [79]. Any attack initiated by other network services can affect SD-VPLS, as they share data plane devices. The introduction of new elements in SD-VPLS creates new attack surfaces. Various schemes to mitigate DoS attacks on SDN architecture have been discussed in [39].

Related Work on VPLS Scalability: Broadly, [122] and [74] present comparisons of different VPLS implementations with respect to scalability, [123] describes a scalable L2 implementation and [124]–[127] proposed various solutions to improve scalability of VPLS. We discuss each of them as follows.

In [122]a comparison of control plane scalability of MPLS-based Layer 2 and Layer 3 VPNs is presented. This paper emulates and compares the operation of L2VPN and L3VPN against a number of criteria: creation time, deletion time, control plane memory consumption and total memory consumption. This paper is used as a basis to further compare legacy VPNs with its SDN version for scalability. The authors in [123] propose a scalable virtual layer 2 implementation. In this work, the scalability of virtual layer 2 is discussed for geographically scattered applications and applications that use a cluster of servers, such as Data centres. In [74] a comparison of traditional IPsec-based VPN services with MPLS-based VPNs is presented. The presented results imply that MPLS is far better in terms of scalability and security than traditional industry standard encrypted tunnels. Thus, the authors advocate the use of MPLS for Layer 2 and Layer 3 VPN services. Scalable, dynamic multipoint VPNs using group encryption keys is proposed in [124]. In this work, a concept of group keys is used instead of a dedicated server for key distribution. Use of group authentication instead of central key management reduces complexity. [125] gave a scalable solution for load balancing of servers in large networks. To achieve this, Virtual Internet Protocol (VIP) is used along with scalable VIP appliances. In [126], a scalable solution for BGP route information handling in VXLAN using the EVPN control plane is presented. In [127], a solution using S-HIPLS to improve both control plane and data plane scalability is proposed.

Summary: The use of EVPN and VXLAN increases the scalability of the network but along with this, the complexity of the network also increases. Current server load balancers do not scale smoothly if traffic and/ or number of servers in server farms (collections of servers) increases. Link aggregation employs a single broadcast domain. For this reason, it becomes impractical to use link aggregation in environments like data centre, where there is a hierarchy of switches.

C. Complexity

The complexity of a network is defined by the number of devices, the number of possible paths between devices and the amount of interaction among them. Complexity also includes network protocols and communication medium. High levels of interaction among its components is often manifested by a complex system [128]. Since VPLS is deployed by corporate houses to connect their offices worldwide, complexity is a significant concern.

VPLS needs to maintain a full mesh of PWs. If there are N PEs, then $O(N \times (N-1)/2)$ PWs are required. This increases complexity in large scale deployment of VPLS architecture [11]. Large scale VPLS networks also require strong authentication and authorization policy so that each instance can be isolated from others. For efficient management

of the VPLS network, it is required to manage IP addresses and access control rights under tight control [129]. H-VPLS alleviates complexity issues in provisioning and operation [7]. VPLS also faces issues in deployment due to different interfaces using different protocols. So integrating them into one large network increases the complexity of the network.

Related Work on Complexity: The work in [129]–[133] aims to reduce the complexity of networks. Work domain analysis is presented in [134] based on Ecological Interface Design (EID). A credential management scheme is described in [135]. The authors in [136] highlight the comparison between MPLS-based LSP and L2TPv3. We discuss each of them as follows.

Reducing the complexity of the network by using a firewall is discussed in [130], [131]. Instead of establishing an enterprise level firewall, which is time consuming and complex, tunnels are used for a firewall. Unlike enterprise level firewalls in which all non-active nodes are also engaged, tunnels firewall only those communications that are active at a given time. This reduces time as well as complexity. The complexity of VPLS can be reduced by efficient management of IP addresses and by exercising tight control over access [129]. Dynamic Host Configuration Protocol (DHCP) is used along with the IPsec protocol for efficient IP address management. In [134], Ecological Interface Design (EID) is used on control process-based VPNs and work domain analysis is also presented. This design is helpful for a system in which there is tight control over process flow and unpredictable events can be crucial, such as nuclear plants. EID is a type of interface design technique in which the work structure of the control process is analysed to gain insights into process goals and constraints that affect the actions of the operator. In [132] and [133], the authors discuss reducing the complexity of the network by using MPLS labels. These labels inherit properties of Destination Address (DA), and this DA remains constant for a particular forwarding path, thus obscuring hop-by-hop signalling and label swapping. The authors in [135] present a credential management scheme for large scale deployment of VPN networks. A comparison in terms of complexity between MPLS using LSP and MPLS using L2 tunneling protocol version3 (L2TPv3) is presented in [136]. An IP-based implementation of VPNs for cellular networks is proposed in [137]. The authors also discuss the complexity of L2VPN and L3VPN.

Summary: As the complexity of a network increases, it becomes more prone to security attacks. In a complex network like VPLS, many networking rules are implemented, which creates inconsistency as conflict(s) may arise between different rules. Moreover, complexity may result in less predictable behaviour of the large network, which can lead to security vulnerabilities. Tracking the root cause of an error or an abnormality in a complex system is also very tedious. This is because improper behaviour of the network can occur for a number of reasons such as configuration error, bugs in algorithms, or faulty hardware. A complex system needs effective troubleshooting, efficient monitoring and robust configuration.

VI. VPLS Operational Aspects

In this section, operational aspects affecting the implementation and operation of VPLS are discussed. There can be many factors affecting the operations of VPLS, however, this section presents a broad discussion of some of the operational aspects.

A. Tunnel Management

Tunnel management consists of creation of a tunnel from one source address to multiple destination addresses, allowing private data to traverse the public network safely. Each endpoint of a tunnel is further subdivided into two sub-endpoints. One sub-endpoint has a public network address, and the other one has a private network address [138]. Since in VPLS private data moves through tunnels that traverse public networks, efficient tunnel management is essential to VPLS.

1) Generic Routing Encapsulation (GRE): To encapsulate MPLS labelled packets in IP (tunnel mode), several techniques have been proposed and documented by the MPLS working group of the IETF [139]. One of the techniques is to employ Generic Routing Encapsulation (GRE). GRE is traditionally used for creating tunnels between IP routers. In MPLS, GRE encapsulates an MPLS packet. After encapsulation, this packet consists of an IP header followed by a GRE header followed by an MPLS label stack. This encapsulation enables the MPLS packet to traverse through GRE tunnels.

As mentioned in [35], it is required for a local PE router to specify the GRE tunnel interface for every remotely situated PE router. Operationally, this can be very exhausting. To overcome this, some vendors have evolved soft GRE, which reduces the a mount of effort invested in GRE tunnel establishment. It is achieved by configuring a single multipoint GRE tunnel interface that connects to all remote PE routers. The GRE header does not include any field that can be used for source PE router verification. Towards the receiver's end of the tunnel, the packet is decapsulated by removing the IP and GRE headers. So the packet received by a PE is treated as an MPLS packet whose topmost label is of MPLS.

2) Secure Socket Layer (SSL) Transport Layer Security (TLS): Netscape developed the SSL protocol, which was later improved by the IETF to its successor TLS [140], [141]. It is a cryptographic protocol that provides security and data integrity. SSL TLS can secure traffic over insecure networks like the public domain and the Internet. SSL is a union of four protocols: handshake protocol, record protocol, alert protocol and change cypher suite protocol. SSL TLS is transparent to higher layers and compatible with popular web and e-commerce applications. Diffie - Hellman key exchange and ESP encapsulation are used by SSL TLS to provide the same level of security as IPsec [142]. SSL VPNs can be used as an alternative to IPsec VPNs, as IPsec tunnels face issue with Network Address Translation and firewall rules [143]. SSL TLS is a session-oriented protocol that provides session-based security, unlike IPsec, which uses permanent parameters between hosts. The SSL protocol is extensively used over the Internet for e-mail, web browsing, Voice over Internet(VOIP), instant messaging and VPNs. In the latest improvement to

TABLE IX: Comparison of tunnel management protocols

Features	**GRE**	**SSL TLS**	**IPsec**
Working Mode	Peer to Peer	Peer to Peer	Peer to Peer
Security	Authentication	Encryption, Confidentiality and Integrity	Built-in complete security mechanism
Tunnel Configuration	Network	Asymmetric Key Cryptography	IKE Interchange
Tunnel Establishment	Explicit	Implicit	Implicit
Tunnel Management	None	None	None
Support for Multiplexing	Supports	Supports	Supports
Multi-Protocol Support	Supports	Supports	Does not Support
Packet Sequencing	Does not Support	Supports	Supports

the TLS protocol, static RSA and Diffie-Hellman have been replaced by an all public key exchange mechanism to provide secrecy [144]. However, SSL TLS require stateful connection and lacks support for User Datagram Protocol traffic.

3) IPsec: IPsec Tunnels are established to provide a secure association between components in order to shield communication from unauthorized access or modification. This is called a flow-based security function [145]. In public networks, the risk of a security breach in communication is very high. To address this issue, the network implements specialized security functions, each one handling one specific type of attack. For example, firewalls are used for tracking and controlling communication, and Intrusion Detection Systems (IDS) for detecting intrusions and mitigating them. However, they do not offer communication security.

IPsec can be used to secure host-to-host, gateway-to-gateway and host-to-gateway communication. The IPsec protocol works at the network layer and provides authentication, integrity and confidentiality to data flows at the IP layer between two network resources [146].

Therefore, IPsec is generally used to create point-to-point L3VPNs. However, some VPLS architectures use the IPsec tunnels to establish the PWs in a VPLS network. For instance, the HIP nodes use the IPsec Encapsulating Security Payload (ESP) protocol on Bound End to End Tunnel (BEET) mode tunnels [147], [148] to communicate with each other. However, HIP can support other IPsec tunnel modes as well [149]. Therefore, IPsec tunnels play an important role in all the HIP-based VPLS architectures [13], [80], [150].

IPsec is a security architecture that describes a security protocol to guard the contents of IP packets. The IPsec Security protocol consists of an Authentication Header (AH) and the Encapsulation Security Payload (ESP) [60], [61], [78]. The AH, as the name suggests, provides authentication. Moreover, ESP additionally provides data encryption. Data security can be provided in two main modes:

- **Transport mode-**The data of the upper layer merged into the payload of a packet is protected.
- **Tunnel mode-**A new outer IP packet encapsulates a complete IP packet to provide protection.

In addition, Bound End to End Tunnel (BEET) tunnels mode is supported by the HIP protocol. The BEET mode augments the existing ESP tunnel and transport modes. In end-to-end tunnels, the BEET mode offers a lightweight header without the regular tunnel mode overhead [151].

Related Work on Tunnel Management: The work related to this technical aspect revolves around comparing different tunnelling protocols, using SDN for improving tunnel management, and using redundant tunnels for fault tolerance and connectivity. We discuss the related work as follows.

In [33], the authors compare different tunneling protocols based on features like security, tunnel configuration and establishment, and support for multiplexing. This work emphasizes standardization of tunneling protocols for VPN. The use of Customer Premise Equipment (CPE) to extend the layer 2 tunneling protocol is described in [152]. An enhanced CPE can support the multipoint-to-multipoint services that are required for VPLS. In [98], the authors used SDN to improve tunnel management in secure VPLS architecture. The authors reported a decrease in the number of tunnels per PE and a decrease in the total number of tunnels compared to legacy VPLS architectures. The interoperability of EVPN and VPLS using pseudo-wires is discussed in [153]. EVPN provides features that are not present in VPLS, but completely replacing VPLS with EVPN would be enormously costly, so in this work, EVPN is used along with VPLS to provide features like flow-based load balancing. The use of redundant tunnels for fault tolerance in VPLS is described in [154]. Redundant tunnels enhance the resiliency of VPLS networks. In [155], tunnels are used to provide redundant connectivity across the network. By using backup tunnels, uninterrupted communication is established.

Summary: Tunnels in VPLS are vital for ensuring access control and data integrity and isolation. However, the failure of a tunnel could result in communication disruption. To address this problem, redundant tunnels are used. In case the primary tunnel fails, the backup tunnel will automatically carry the traffic. This ensures uninterrupted services, but it also increases the cost and complexity of the network. Such tunnelling schemes are needed, which reduces the complexity at L2 and lessens security threats due to configuration errors.

B. Compatibility Issues

Compatibility means the ability of two systems to work together and coexist without making any alterations. It refers to the interoperability of two systems [156]. VPLS deploys different types of protocols to provide services. These protocols may

sometimes interfere with each other's functioning, creating inconsistencies in the system. For the proper functioning of VPLS, the compatibility of protocols is essential.

VPLS architecture consists of geographically distributed sites that share the same Ethernet domain. In an Ethernet network, various L2 network protocols such as Spanning Tree Protocol (STP), Address Resolution Protocol (ARP), and Reverse Address Resolution Protocol (RARP) are used by traditional equipment. VPLS architecture makes use of tunnels for inter-site connectivity. These tunnels are not visible to L2 devices and L2 protocols. As a result, many L2 protocols fail to function properly and thus create a compatibility issue in the VPLS network. For example, STP is responsible for discovering loops in the provider network. Failing to which causes issues like higher spanning tree convergence time, multiple frame transmission, broadcast storms and forwarding table instability [20], [80].

Related Work on Compatibility Issues: The work discussed in this section can be grouped into two categories: implementations of spanning tree protocol for different purposes [157]–[160] and use of spanning tree protocol in PEs [161].

A method based on the spanning tree protocol for automatic discovery of VPN tunnels is proposed in [157]. In [158] and [159], implementation of spanning tree protocol in VPN is presented. Signalling labels are used on label-switched tunnels for controlling communication. In some sense, these works, try to bridge the gap between L2 protocols and tunnels. Reviews about migrating from spanning tree protocol to Ethernet ring protection switching protocol for loop-free networks are discussed in [160]. In [161] the author talks about PEs in VPLS and how they use the spanning tree protocol. By taking the first PE as a root, a minimal spanning tree is generated, and a broadcast MAC table is calculated.

Summary: Compatibility issues in VPLS may arise due to both hardware and software. Due to the large size and wide geographical coverage, VPLS includes devices from various vendors, which may create compatibility issues. To address this issue, dependency on vendor-specific hardware should be minimized.

C. Other Operational Issues

The term "operational issues", in general, means any issue in an operating network that can make the network less efficient. A VPLS network consists of various devices, several different protocols, QoS standards, and tunnel management, which can affect the efficiency of the network if not appropriately handled.

To provide security, VPLS establishes a full mesh of tunnels between customer sites, increasing the number of tunnels exponentially as the number of PEs increases. This leads to an increase in tunnel management overhead and operational cost of VPLS. Dynamic mechanisms for preventing attacks or restricting attack propagation are not present in legacy VPLS architectures [79]. For large-scale deployment of VPLS architecture, provisioning of services is a challenge. Traffic isolation becomes a very demanding task with the increase in the size of the network. Traffic engineering functions like load balancing, minimizing traffic transport delay, and optimum routing are not available in legacy VPLS architectures [79]. There is no automatic network management support in traditional VPLS architectures. In large VPLS architectures, network management also becomes difficult because of the presence of devices from different vendors. VPLS routers should support a large set of protocols as vendor-specific devices cannot be mixed and matched.

Related Work on Operational Issues: Broadly, the works related to the operational issues are concerned with traffic engineering in VPNs [162]–[164], QoS [165], [166] and use of VPNs in cloud and virtual mobile [167], [168]. We briefly discuss each of them.

In [162], the use of Traffic Engineering (TE) tunnels in VPNs is covered. Dynamic establishment and deletion of TE tunnels is discussed. A multipath routing algorithm was proposed by [165] for bandwidth QoS. An algorithm ensures bandwidth QoS by finding the least number of paths. It works for point-to-multipoint VPLS. In [163], a method for traffic engineering in connectionless VPNs using restricted physical and logical topology is presented. Restrictions are applied to provide information about the single path between edge nodes and limited bandwidth. In [164], a new approach for MPLS-based VPNs for path protection using loop-free traffic engineering is given. This paper presents a solution for the multi-commodity flow problem. System and method for provisioning of QoS in IP based VPN are presented in [166]. The system uses the identification of a class of traffic for QoS criteria. VPNs as a Service for cloud architecture is proposed in [167]. The use of cloud architecture for VPN will help in enhancing communication and reducing cost. In [168], methods and apparatus for configuring virtual mobile networks using VPN Wireless communication with VPNs client are described.

Summary: TE tunnels are unidirectional tunnels in MPLS. Unlike other tunnels, if a TE tunnel is established between two nodes (A to B), the reverse tunnel (from B to A) will not be created automatically. TE tunnels save bandwidth, provide QoS and offer several security features. For efficient operation of VPLS, issues like bandwidth utilization, congestion control, load balancing among multiple paths, optimum resource utilization, and network performance should be considered.

VII. Evolved VPLS Solutions

With the ever-increasing popularity of virtual networks and the increasing size of data centres, it has become difficult for the current VPLS architecture to keep pace. Therefore, new schemes have been proposed that enable current architectures to provide better security, scalability and provisioning simplicity.

A. Identity Defined Networking (IDN)

To enhance security for IP-based networks, Tempered Networks proposed a new architecture based on an identity-first approach: Identity Defined Networking (IDN) [23]. IP addresses were devised only to identify the location and provide reliable connection, but not security. IDN is a virtualized

private overlay network using HIP as its base. Host identities are assigned to all network devices so that each endpoint is recognized using a cryptographic identity in place of insecure IP addresses. For communication between legitimate devices, an encrypted and secure communication tunnel is established. Since devices are in the overlay, the IDN network is hidden from the underlying network, so these devices cannot be hacked using an underlay network. IDN architecture is comprised of two major components:*Conductor* and *HIP services*. The conductor is a centralized engine responsible for service orchestration and has all of the intelligence. It is responsible for connecting, disconnecting and protecting globally-located resources. The conductor defines and enforces policies for HIP services but does not handle any traffic. The conductor connects with HIP switches deployed on the network automatically using cryptographic identities assigned to each switch [169].

HIP services are responsible for enforcing software-based policy, providing secure connectivity among IDN services, cloaking and segmentation of devices, Identity-based routing and IP mobility. IDN can handle Ethernet, wireless, radio and serial over IP networks. This architecture can be stationed without causing any operational disturbance. Management of IDN is easy, as well as revocation of devices and security services. IDN provides fast, flexible and scalable protection to devices, reducing the attack surface [170].

B. *EVPN*

The extensive use of Ethernet L2VPN services and the emergence of novel applications for technology like data centre interconnect (DCI) resulted in a new set of requirements that cannot be handled by current VPLS architectures. Ethernet VPN (EVPN) provides solutions to issues like redundancy, multicast optimization and complexity of provisioning faced by traditional VPLS architectures. Because of its versatile nature, it is not easy to provide a generic picture of EVPN [171] [172].

EVPN supports all-active redundancy mode with multi-homing, whereas current VPLS architecture only supports single-active redundancy mode. In single-active redundancy mode, only one PE is connected to an Ethernet segment and can direct traffic in and out of that segment, whereas in all-active redundancy mode, all PEs are connected to an Ethernet segment and can direct traffic (known unicast) in and out that segment, for a given VLAN [173].

In EVPN, MAC learning between PEs occurs in the control plane, unlike current VPLS where address learning is done in the data plane. This provides better control over the MAC learning process and the ability to apply policies. Control plane learning also facilitates isolation of groups of interacting devices from each other. EVPN can use a Provider Back-Bone (PBB) VPN to address the scalability issue faced by the MAC learning process. PBB EVPN differs from "plain" EVPN in that several MAC addresses that are required to be stored in a PE in the core. In PBB EVPN, a small number of backbone MACs are discovered in the EVPN control plane using BGP. MAC data forwarding is applied for learning the larger number of customer MACs. The forwarding plane provides MAC addresses to all CEs (local or remote) in PBB EVPN [173].

EVPN also provides better methods of DCI. EVPN facilitates DCI with efficient provisioning of services, scalability (operates like L3VPN) and capability to provide L2 and L3 services on the same interface (not possible in traditional VPLS). In addition to this, EVPN also supports PE nodes that offer multi-homed connectivity access networks or CE devices to be placed in the same or distant geographical locations. Such PE nodes are geo-redundant. This feature ensures business continuity for critical applications in scenarios like a natural disaster or power failures. In EVPN, this is achieved without establishing dedicated connections among PEs in a multi-homed group. This approach is cost-effective [174]. The authors in [67] proposed the use of EVPN as an overlay network.

C. Virtual eXtensible LAN (VXLAN)

In data centre where Virtual Machines (VMs) are clubbed according to their Virtual LAN (VLAN), the current limit of 4094 VLANs might prove to be insufficient. This is because thousands of VLANs are required to divide traffic according to the particular group to which the VM may belong. Virtual eXtensible LAN (VXLAN) is an IETF standard proposal [66], consisting of a Layer 2 overlay scheme over a layer 3 network. It can be used in any IP network as an overlay to provide Ethernet services. VXLAN, like a core network connection, can be used as an alternative to MPLS. VXLAN supports pre-existing resiliency and load balancing mechanisms, as it works with any type of underlay network [175].

Each overlay is addressed as a VXLAN segment. Communication can be established between VMs in the same VXLAN segment. A 24-bit segment ID "VXLAN Network Identifier (VNI)" is used to identify each segment. Thus, using VNI allows up to 16 Million VXLAN segments to co-exist within the same administrative domain. The outer header encapsulates the VNI and the inner MAC frame. The individual VM originates the inner MAC frame, and VNI is responsible for identifying the scope of this frame. This scheme avoids cross-over as traffic isolation is achieved using VNI, but the overlapping of MAC addresses can happen.

VXLAN, when used as a data plane for EVPN, enables it to extend tunnels up to hypervisor, which is hosting the VM executing the application of interest. This cannot be achieved in the absence of VXLAN. The scalability provided by VXLAN over IEEE801.2Q (STP) VLANs is the most remarkable feature in large networks. [176]–[178] proposed various architectures using VXLAN.

VIII. VPLS Applications and Projects

This section discusses some of the prominent VPLS applications and projects. Various applications of VPLS from the personal to the industrial level are discussed briefly. Different VPLS-based projects are presented, which range from ongoing to completed.

A. VPLS Applications

VPNs have versatile applications in terms of the services for which they can be used. Some of the significant applications are discussed below.

1) Personal VPN services: Because of its unique technical advantage of the flexibility of deployment, based on customer types and service attributes, VPLS has found applications in the field of individual distributed services. By simplifying the complexities of the access network, VPLS provides its customers with a simple Ethernet interface. The customer has the flexibility to define their data formats and routing protocols. One of the most promising applications for VPLS is Customer Centered Communication, which interconnects Personal Area Networks (PANs), Home Networks (HNs) and Office Networks (ONs) through Metropolitan Area Networks (MANs) and Wide Area Networks (WANs). VPLS enables the user to control devices and sessions on all subnets and obtain secure and reliable communication anytime and anywhere.

2) Enterprises VPN services: With VPLS added to VPNs, all remote offices behave as if they are working on the same LAN. This enables customers to maintain control of their network routing while supporting IP and non-IP traffic. It also provides a single platform for convergence of voice, data, video and multimedia [179].

3) Data Centres: VPLS is the most common data centre interconnecting model. Because of its very high level of standardization, most industries use VPLS architecture to do the deployment [180].

4) Industrial Internet: HIPLS based networks are being used by Boeing in the assembly line of Boeing 777 aeroplanes. Two prominent SCADA network appliances manufacturing companies are working on HIP-based security appliances.

5) Mobile Backhaul Networks: In Mobile backhaul networks, VPN architecture is used along with IPsec to provide not only security but also a different level of Quality of Service (QoS) to a different type of traffic. This architecture also helps in directing different backhaul traffic to the correct destination [181]–[183].

6) Grid Computing: Features of VPLS like support for IP, transparent layer 2 connectivity, good security features and efficient connection between two devices help better implementation of grid computing.

7) Internet Protocol Television (IPTV): VPLS has also found its implementation in the digital multimedia broadcast network. IPTV broadcast network architecture uses VPLS and tree-based VPLS (TVPLS) to provide scalable, cost efficient and reliable services [184] and [185].

B. VPLS Projects

This section presents some significant ongoing and completed research projects, carried out by academic and industrial collaboration.

1) SIGMONA [186]: SDN Concept in Generalized Mobile Network Architecture (SIGMONA) was a project conducted between June 2013 and April 2016. Under this project, SDN concepts were applied to various mobile network architectures, including VPLS. The concept of SDN was applied to VPLS architecture, and its evaluation was done under this project. The project's main focus was to evaluate, specify, and validate SDN concepts designed onto network virtualization, software defined networking, and cloud computing principles. The project evaluated feasibility, performance, scalability and application opportunities of SDN-based networks [187].

2) SECUREConnect [188]: SECUREConnect is another project that started in September 2016 and continued untill August 2020. It is a joint project of the University of OULU and Aalto University, Finland. The main objective of this project is to evaluate security and limitations in current cyber physical communication systems and identify potential areas for improvement, and to use SDN and NFV concepts for the same. This project specifies applicable scenarios and use cases for cooperation, coexistence, and integration of cloud service-based solutions and SDN and NFV-based techniques with cyber physical communication in network security [189]. An improvement in tunnel management systems for VPLS using SDN was proposed under this project.

3) TWAREN [190]: TWAREN (Taiwan Advanced Research and Education Network) was an initiative under the Taiwanese government's "Challenge 2008" program funded by the National Science Council between 2003-2008. It was responsible for planning, designing and establishing the next generation research and education network. It is a combined platform for big data science and network research. It assisted in the growth of technologies and applications such as MPLS, multicast, IPV6 and performance measurement. Since VPLS is also based on the MPLS protocol, it was also a part of this project. It also provides SDN testbed architectures [191].

4) MEVICO [192]: MEVICO (Mobile Networks Evolution for Individual Communications Experience), a project funded by Celtic between April 2010 and December 2012. Celtic is a European research and development program working in telecommunication. Under MEVICO, research was carried out in areas of mobility management, routing optimization, packet transport network technologies, traffic management and cost models for network Capital Expenditure (Capex) and Operational Expenditure (Opex) [193]. This project focused on novel network concepts for future demands of Long Term Evolution (LTE) technologies, services and uses of the Internet, so it also involved working on aspects of VPLS.

5) Train Wireless Bus (TWB) [187]: Train Wireless Bus is a joint project of General Electric (GE) transportation and Center for Wireless Communication (CWC), University of Oulu. This project, which started in May 2012, aims to investigate train communication in an urban transit environment. The purpose of this project is to present a low power, innovative and reliable solution in a demanding radio propagation environment for the vehicle-to-vehicle onboard communication. It aims to improve the performance of onboard railway devices and to give passengers highly accurate information.

6) Pacific Rim Application and Grid Middleware Assembly-Experimental Network Testbed (PRAGMA-ENT) [194]: PRAGMA is an international collaboration of researchers established in 2013, who are actively working on addressing problems related to eScience. The goal of this community is to construct a test bed for SDN/ OpenFlow that can be used by

PRAGMA researchers and collaborators. This project initially focused on establishing an international L2 backbone. Later it worked on an evaluation of technologies for the control plane. The network testbed established by PRAGMA gives total freedom to researchers for accessing the network without worrying about interference with the production network. The collaborators in this project are Florids Lambda Rail, Internet2, Pacific Wave, Japan Gigabit Network and TWAREN.

7) L2OVX [195]: This is an Open VirteX based system, which provides VPLS-like services in SDN at a lower cost. It was proposed in 2016. It is a three-layered model: Network Resource layer, Virtualization layer and Management layer. L2VOX uses layer2 for virtualization instead of layer3. It improves the transfer bandwidth of the network by providing a load balancing function for each VPLS service. To improve efficiency, L2OVX also supports on demand configuration.

8) SDN for end to end Networked Science at the Exascale (SENSE) [196]: This project started in 2019 under Tom Lehman. The SENSE system allows National Labs and Universities to request and provide end-to-end intelligent network services for their application workflows leveraging SDN capabilities. It is a model-based real time system with multi-resource cyber infrastructure awareness. SENSE provides a framework that leverages artificial intelligence and machine learning technologies to improve network monitoring, provisioning, optimization and troubleshooting. The major contributor in this project is Energy Sciences Network (ESnet).

IX. Lessons Learned and Future Work

VPLS is a widely accepted and used technology, so it is also sought after by researchers. Various VPLS related open research challenges need to be handled efficiently. This section briefly discusses lessons learned from related work and possible future work for VPLS.

A. Security

1) Lessons Learned: Security is one of the significant concerns in VPLS technology. In VPLS networks, private data traverse through the public network, which is susceptible to various attacks like DDoS, Spoofing, Sniffing, and packet re-routing. VPLS implementation uses various protocols like BGP, LDP and HIP. Recently, technologies like SDN and NFV have also been used alongside VPLS. However, these protocols and technologies have threats of their own. For example, BGP is susceptible to prefix hijacking due to a lack of solid integrity and authentication. Using SDN in VPLS makes the network programmable and robust, but it also opens many frontiers for an attack on programmable interfaces.

2) Future Work: Security plays a very vital role in VPLS. Although various solutions have been proposed, so far there are still loopholes in VPLS security. All the suggested secure VPLS solutions have an impact on latency, throughput, and jitter. The inclusion of security features in VPLS results in increased latency, decreased throughput, and a rise in jitter. In the future, such a secure VPLS will be required to provide security with minimal effect on latency, throughput, and jitter.

B. Scalability

1) Lessons Learned: Despite advancements in technology, VPLS has still not reached its full potential in implementation because of scalability issues. Although the introduction of H-VPLS has addressed the issue of control plane scalability, it increased provisioning and operational complexity. The data plane involves packet forwarding and encapsulation. Thus, a scalability issue arises in large networks due to MAC table explosion. Security plane issues involve key generation.

2) Future Work: In terms of scalability, future VPLS architecture should have high scalability in all three planes, i.e., control plane, data plane, and security plane. The use of technologies like SDN and NFV along with VPLS increases the scalability. However, they have not been successfully implemented in large-scale networks. Efforts should be made to implement these technologies in more extensive networks to check the performance. Quantum Key Distribution (QKD) can be used to address key generation for the security plane, but it needs to be cost-effective, as the cost of equipment used for QKD is high.

C. Complexity

1) Lessons Learned: Complexity in VPLS arises mainly because of the use of different tunneling and other protocols. Each protocol has its own set of requirements that VPLS needs to incorporate which increases the overall complexity. In addition, all hierarchical architecture of the current VPLS also makes it complex. This is further aggravated as the size of the network increases. Due to this, traffic isolation becomes a challenge, requiring tight access control.

2) Future Work: In VPLS, there will always be a certain degree of complexity, both because of its size and because of the services provided. However, in the future, a common framework can be designed that will effectively integrate all protocols, reducing complexity. Also, strong authentication and access control are required to provide traffic isolation in large networks.

D. Tunnel Management

1) Lessons Learned: In VPLS, tunnels are required to be established between PEs. Therefore, an increase in the number of PEs causes exponential growth in the number of tunnels in the current VPLS architecture. An increase in the number of tunnels, in turn, results in a high cost of tunnel establishment and maintenance. Also, tunnel parameters are predefined and static in all VPLS architectures, except for SD-VPLS, where tunnel parameters are predefined but can be changed dynamically. There is also a difference in the working mode of various tunnels. For example, GRE and IPsec work on a peer-to-peer model, whereas L2TP follows the client-server model. Thus, to be symmetric, VPN needs to incorporate both.

2) Future Work: Tunnels are very vital to VPLS for providing encryption and authentication. Various solutions, including SDN for tunnel management, have been proposed for dynamic tunnel establishment and reducing tunnel establishment delay. However, all of these solutions are conducted on testbeds and

still have not been implemented by industry. In the future, solutions proposed so far need to be tested against industrial VPLS applications. Dynamic routing is required in the future from tunnel management.

E. Operational Issues

1) Lessons Learned: VPLS routers are of concern for operational issues, because such a router needs to support various protocols being used in a VPLS space. Traffic engineering capabilities are another issue, as legacy VPLS architectures do not provide support for traffic engineering functionalities. The absence of any dynamic mechanism for mitigating attacks on VPLS is also an issue. Current VPLS architectures do not have any such mechanism.

2) Future Work: In the future, efforts can be made to reduce the load on the VPLS router. Using technologies like SDN can help with implementation of traffic engineering features such as load balancing, optimum routing, and reduction in traffic transport delay in VPLS. SDN should also be explored in terms of enhancing the security of VPLS by including dynamic attack mitigation in VPLS.

F. Compatibility

1) Lessons Learned: In VPLS, due to tunnels that are not visible to L2, sometimes L2 protocols fail to function in the intended manner. Improper functioning may cause disturbances in the normal operation of VPLS. Due to the use of multiple protocols in VPLS to facilitate various functionalities like STP for loop-free VPLS, maintaining tunneling protocol compatibility sometimes becomes difficult. Compatibility issues also arise due to vendor-specific hardware. As VPLS networks consist of geographically distant sites, each site may be using its own set of hardware based on availability. Each vendor hardware uses different protocols and interfaces. These protocols cannot be mixed, so VPLS must handle an extensive set of protocols to avoid conflicts.

2) Future Work: In the future, work can be done to make VPLS free from vendor-specific hardware. SDN removes the dependency on hardware by making the network programmable, and it can also be used in VPLS to eliminate hardware compatibility issues. Efforts should also be made to ensure the proper functioning of L2 protocols.

G. Evolved VPLS Solutions

1) Lessons Learned: Enhancements like IDN, EVPN, and VXLAN have added value to the VPLS. IDN, which is a HIP-based overlay for IP-based networks, increases the security of the network. IDN helps in reducing attack surfaces and is easy to manage. IDN supports Ethernet, radio, wireless and serial technologies over IP networks. EVPN made the use of VPLS easier for new technologies like DCI. Features like support for all active redundancy, MAC learning at the control plane, and the use of PBB to address scalability and cost effectiveness, have made EVPN popular. To resolve the problem of limited VLAN ids, VXLAN was proposed. It is the IETF standard for a layer 2 overlay scheme over a layer 3 network. A 24 bit segment id called the VNI is used in VXLAN, which can support 16 million VXLAN segments within the same administrative network domain. The scalability provided in an extensive network over STP VLANS by VXLAN is the most outstanding feature.

2) Future Work: Although evolved VPLS solutions help increase security, reduce cost, and provide better scalability, and easier management, some features will still bring improvements down the line. Currently, IDN can only be used on windows-based systems - the addition of support for other operating systems will help in the future. IDN also lacks standardization. In EVPN, security is a concern. Any change in the information used for forming the encapsulation header or choosing the tunnel in EVPN may lead to user data packets getting dropped, delivered to the wrong address, or routed incorrectly. This problem needs to be addressed for better implementation. Flooding of frames is one of the issues with VXLAN. As VXLAN is used in large networks, a security assessment of protocols like IGMP should be done. An attack on VXLAN table entries in an overlay network could result in redirection of traffic towards an attacker. For future research, security threat mitigation in VXLAN and overhead management could be explored.

H. VPLS Applications

1) Lessons Learned: Because of its user friendliness and high security features, VPLS is used for connectivity from individual houses to industry giants across the globe. As it is customer-centric, VPLS is used in PANs, ONs, and HNs. For LAN-like connectivity, VPLS is used by enterprises whose offices are located across the globe. One of the most popular VPLS applications is in data centres. As VPLS is highly standardized, it is used for the deployment of DCI. Industrial use of VPLS in SCADA is one of the oldest applications of VPLS. Currently, VPLS is also being used in mobile backhaul networks to provide better QoS. In Grid computing, VPLS is used to establish a connection between two devices.

2) Future Work: Although VPLS is one of the most popular networking technologies, certain issues still need to be addressed down the line. For enterprise and industry, the issue with VPLS is scalability. Although various solutions like H-VPLS and the use of SDN are proposed, their practical implementation is still limited. Security is another issue that needs to be improved in future. The possibility of using SDN for enhancing the security of VPLS might be explored in future work.

X. Conclusion

With ever-growing network interconnections, the scope of VPLS is also growing. VPLS is evolving due to increased demand and the services VPLS provides. In this paper, we have explored VPLS and its various aspects through discussions based on available literature, and have tried to present a relevant summary of the issues faced in VPLS. Our survey covered a holistic investigation of the use of SDN in VPLS. We have explored various advantages of using SDN, along with VPLS in the network. The survey also

highlights different architectures using SD-VPLS. This paper has examined various technical aspects and related issues in VPLS through panoramic reviews. We have presented comprehensive details of security, scalability, complexity, tunnel management, compatibility, and operational issues in VPLS. Hence, a comprehensive list of future directions and open challenges has been included to encourage future research on VPLS.

ACKNOWLEDGEMENT

This work is partly supported by the Academy of Finland under the 6Genesis (grant no. 318927) project.

REFERENCES

[1] R. Venkateswaran, "Virtual private networks," *IEEE potentials*, vol. 20, no. 1, pp. 11–15, 2001.

[2] L. Andersson and E. Rosen, "Framework for Layer 2 Virtual Private Networks (L2VPNs)," IETF Requests for Comments, RFC 4664, September 2006.

[3] M. Carugi, D. McDysan *et al.*, "Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks (PPVPNs)," IETF Requests for Comments, RFC 4031, April 2005.

[4] T. Takeda, I. Inoue, R. Aubin, and M. Carugi, "Layer 1 virtual private networks: service concepts, architecture requirements, and related advances in standardization," *IEEE Communications Magazine*, vol. 42, no. 6, pp. 132–138, 2004.

[5] D. Fedyk, Y. Rekhter, D. Papadimitriou, R. Rabbat, and L. Berger, "Layer 1 VPN basic mode," IETF Requests for Comments, RFC 5251, July 2008.

[6] M. Liyanage, "Enhancing security and scalability of virtual private LAN services," Ph.D. dissertation, Ph. D. dissertation, University of Oulu, 2016.[Online]. Available: http://jultika. oulu. fi/Record/isbn978-952-62-1376-7. ....

[7] M. Liyanage, M. Ylianttila, and A. Gurtov, "Enhancing Security, Scalability and Flexibility of Virtual Private LAN Services," in *2017 IEEE International Conference on Computer and Information Technology (CIT)*. IEEE, 2017, pp. 286–291.

[8] S. T. Aung and T. Thein, "Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks," in *2020 IEEE Conference on Computer Applications (ICCA)*. IEEE, 2020, pp. 1–5.

[9] X. Dong and S. Yu, "VPLS: an Effective Technology For Building Scalable Transparent LAN Services," in *Network Architectures, Management, and Applications II*, vol. 5626. International Society for Optics and Photonics, 2005, pp. 137–147.

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

[11] M. Lasserre, V. Kompella *et al.*, "Virtual Private LAN service (VPLS) Using Label Distribution Protocol (LDP) signaling," IETF Requests for Comments, RFC 4762, January 2007.

[12] G. Di Battista, M. Rimondini, and G. Sadolfo, "Monitoring the Status of MPLS VPN and VPLS Based on BGP Signaling Information," in *2012 IEEE Network Operations and Management Symposium*. IEEE, 2012, pp. 237–244.

[13] T. Henderson, S. Venema, and D. Mattes, "HIP-based Virtual Private LAN Service (HIPLS)," *Internet Draft, IETF*, 2011.

[14] R. van der Pol, B. Gijsen, P. Zuraniewski, D. F. C. Romão, and M. Kaat, "Assessment of SDN Technology for an Easy-to-Use VPN Service," *Future Generation Computer Systems*, vol. 56, pp. 295–302, 2016.

[15] G. Lospoto, M. Rimondini, B. G. Vignoli, and G. Di Battista, "Rethinking Virtual Private Networks in the Software-Defined Era," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2015, pp. 379–387.

[16] D. Cavendish, "Operation, Administration, and Maintenance of Ethernet Services in Wide Area Networks," *IEEE Communications Magazine*, vol. 42, no. 3, pp. 72–79, 2004.

[17] A. Sajassi and D. Mohan, "Layer 2 Virtual Private Network (L2VPN) Operations, Administration, and Maintenance (OAM) Requirements and Framework," IETF Requests for Comments, RFC 6136, March 2011.

[18] J. Arco, J. Carral, A. García, and G. Ibañez, "RBP, Resilience and Traffic Balance Protocol in VPLS Access Network."

[19] A. Sajassi, "System and method to facilitate interoperability between virtual private LAN service (VPLS) and Ethernet virtual private network (EVPN) with all-active multi-homing," May 26 2020, US Patent 10,666,459.

[20] M. Liyanage, M. Ylianttila, and A. Gurtov, "A Novel Distributed Spanning Tree Protocol for Provider Provisioned VPLS Networks," in *2014 IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 2982–2988.

[21] S. A. Boyer, *SCADA: Supervisory Control and Data Acquisition*. International Society of Automation, 2009.

[22] T. Henderson, "Boeing HIP Secure Mobile Architecture," *Tech. Rep.*, 2008.

[23] "Whitepaper IDN," Website, 2017. [Online]. Available: https://www.tempered.io/

[24] "TofinoSecurity Project," Website, 2017. [Online]. Available: https://www.tofinosecurity.com

[25] L. Serrano and M. A. Sotos, "Interdomain VPLS and Deployment Experiences," *Computational Methods in Science and Technology*, vol. 11, no. 2, pp. 153–159, 2005.

[26] "Cisco VPLS Project," Website, 2019. [Online]. Available: https://www.cisco.com/c/en/us/products/ios-nx-os-software/virtual-private-lan-services-vpls

[27] "Juniper Networks-VPLS," Website, 2019. [Online]. Available: https://www.juniper.net/documentation/en_US/junos/topics/concept/vpls-security-overview.html

[28] "Samsung Research VPLS," Website, 2019. [Online]. Available: https://research.samsung.com/next-generation-communications

[29] "Nokia VPLS Course," Website, 2019. [Online]. Available: https://networks.nokia.com/src/course/virtual-private-lan-services

[30] "Vodafone VPN Services," Website, 2019. [Online]. Available: https://www.vodafone.co.uk/business/business-connectivity/data-connectivity/Ethernet-services/vpn

[31] "VPLS Estimation," Website, 2019. [Online]. Available: https://www.theexpresswire.com/pressrelease/\\Virtual-Private-LAN-Service-Market-is-Estimated-to-Reach\\-2420-Million-by-2025_11133956

[32] G. Armitage, "MPLS: The Magic Behind the Myths [Multi Protocol Label Switching]," *IEEE Communications Magazine*, vol. 38, no. 1, 2000.

[33] Z. Aqun, Y. Yuan, J. Yi, and G. Guanqun, "Research on Tunneling Techniques in Virtual Private Networks," in *WCC 2000-ICCT 2000. 2000 International Conference on Communication Technology Proceedings (Cat. No. 00EX420)*, vol. 1. IEEE, 2000, pp. 691–697.

[34] G. Chiruvolu, A. Ge, D. Elie-Dit-Cosaque, M. Ali, and J. Rouyer, "Issues and Approaches on Extending Ethernet Beyond LANs," *IEEE Communications Magazine*, vol. 42, no. 3, pp. 80–86, 2004.

[35] B. Daugherty and C. Metz, "Multiprotocol Label Switching and IP. Part I. MPLS VPNs Over IP Tunnels," *IEEE Internet Computing*, vol. 9, no. 3, pp. 68–72, 2005.

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

[37] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A Survey on Software-Defined Networking," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 27–51, 2014.

[38] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2317–2346, 2015.

[39] A. P. Fajar and T. W. Purboyo, "A Survey Paper of Distributed Denial-of-Service Attack in Software Defined Networking (SDN)," *International Journal of Applied Engineering Research*, vol. 13, no. 1, pp. 476–482, 2018.

[40] H. A. Seid and A. Lespagnol, "Virtual Private Network," Jun. 16 1998, US Patent 5,768,271.

[41] J. Longworth, "VPN: From An Obscure Network to a Widespread Solution," *Computer Fraud & Security*, vol. 2018, no. 4, pp. 14 – 15, 2018.

[42] A. Nagarajan, "Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN)," IETF Requests for Comments, RFC 3809, June 2004.

[43] L. Andersson and T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology," IETF Requests for Comments, RFC 4026, March 2005.

[44] T. Takeda, R. Aubin, M. Carugi, I. Inoue, and H. Ould-Brahim, "Framework and requirements for layer 1 virtual private networks," IETF Requests for Comments, RFC 4847, April 2007.

[45] I. Bryskin and L. Berger, "OSPF-Based Layer 1 VPN Auto-Discovery," IETF Requests for Comments, RFC 5252, July 2008.

[46] T. Takeda, D. Brungard, A. Farrel, H. Ould-Brahim, and D. Papadimitriou, "Applicability Statement for Layer 1 Virtual Private Network (L1VPN) Basic Mode," IETF Requests for Comments, RFC 5253, July 2008.

[47] B. Wen, G. Fioccola, C. Xie, and L. Jalil, "A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery," IETF Requests for Comments, RFC 8466, October 2018.

[48] W. Luo, "Layer 2 Virtual Private Network (L2VPN) Extensions for Layer 2 Tunneling Protocol (L2TP)," IETF Requests for Comments, RFC 4667, September 2006.

[49] P. Muley, M. Aissaoui, and M. Bocci, "Pseudowire Redundancy," IETF Requests for Comments, RFC 6718, August 2012.

[50] R. Aggarwal, Y. Kamite, L. Fang, Y. Rekhter, and C. Kodeboniya, "Multicast in Virtual Private LAN Service (VPLS)," IETF Requests for Comments, RFC 7117, February 2014.

[51] O. Dornon, J. Kotalwar, R. Hemige, V andQiu, and Z. Zhang, "Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)," IETF Requests for Comments, RFC 8220, October 2017.

[52] R. Singh, K. Kompella, and S. Palislamovic, "Updated Processing of Control Flags for BGP Virtual Private LAN Service (VPLS)," IETF Requests for Comments, RFC 8614, October 2019.

[53] H. Shah, E. Rosen, F. Le Faucheur, and G. Heron, "IP-Only LAN Service (IPLS)," IETF Requests for Comments, RFC 7436, January 2015.

[54] R. Callon and M. Suzuki, "A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNS)," IETF Requests for Comments, RFC 4110, July 2005.

[55] F. Gont, "Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks," IETF Requests for Comments, RFC 7359, August 2014.

[56] E. Rosen and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)," IETF Requests for Comments, RFC 4364, February 2006.

[57] P. Marques, J. Guichard, R. Raszuk, R. Bonica, K. Patel, L. Fang, and L. Martini, "Constrained Route Distribution for Border Gateway Protocol/ Multi Protocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)," IETF Requests for Comments, RFC 4684, November 2006.

[58] Y. Rekhter, R. Bonica, and E. Rosen, "Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks," IETF Requests for Comments, RFC 4797, January 2007.

[59] R. Raszuk, T. Boyes, and B. Fee, "Virtual Subnet: A BGP/MPLS IP VPN-Based Subnet Extension Solution," IETF Requests for Comments, RFC 7814, March 2016.

[60] P. Srisuresh, "Security Model with Tunnel-Mode IPsec for NAT Domains," IETF Requests for Comments, RFC 2709, October 1999.

[61] B. Patel, B. Aboba, W. Dixon, G. Zorn, and S. Booth, "Securing L2TP using IPsec," IETF Requests for Comments, RFC 3193, November 2001.

[62] D. Black and D. McGrew, "Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol," IETF Requests for Comments, RFC 5282, August 2008.

[63] J. Uttaro, S. Boutros, and J. Rabadan, "Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) and Provider Backbone Bridging EVPN (PBB-EVPN)," IETF Requests for Comments, RFC 8317, January 2018.

[64] J. Drake, K. Nagaraj, and S. Sathappan, "Framework for Ethernet VPN Designated Forwarder Election Extensibility," IETF Requests for Comments, RFC 8584, April 2019.

[65] A. Sajassi, J. Salam, S andRabadan, and T. P. B. B. P. Equivalents, "Seamless Integration of Ethernet VPN (EVPN) with Virtual Private LAN Service (VPLS) and Their Provider Backbone Bridge (PBB) Equivalents," IETF Requests for Comments, RFC 8560, May 2019.

[66] M. Mahalingam, D. G. Dutt, K. Duda, P. Agarwal, L. Kreeger, T. Sridhar, M. Bursell, and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks," IETF Requests for Comments, RFC 7348, August 2014.

[67] A. Sajassi, J. Drake, N. Bitar, R. Shekhar, J. Uttaro, and W. Henderickx, "A Network Virtualization Overlay Solution Using ETHERNET VPN (EVPN)," IETF Requests for Comments, RFC 8365, March 2018.

[68] J. Okwuibe, M. Liyanage, and M. Ylianttila, "Performance Analysis of Open-source Linux-based HIP Implementations," in *2015 IEEE 10th International Conference on Industrial and Information Systems (ICIIS)*. IEEE, 2015, pp. 60–65.

[69] M. Lewis, *Comparing, Designing, and Deploying VPNs*. Adobe Press, 2006.

[70] W. Augustyn and Y. Serbest, "Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks," IETF Requests for Comments, RFC 4665, September 2006.

[71] I. Hussain, *Ethernet services over MPLS networks*, 01 2006, pp. 425–456.

[72] W. NOBEL, "Deliverable D2 "Definition of Network Management and Control requirements of network scenarios and solutions supporting Broadband Services for All"," 2004.

[73] H. Lee, J. Hwang, B. Kang, and K. Jun, "End-to-End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network," in *Proceedings 2000. International Workshop on Parallel Processing*. IEEE, 2000, pp. 479–483.

[74] F. Palmieri, "VPN Scalability Over High Performance Backbones Evaluating MPLS VPN Against Traditional Approaches," in *Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC 2003*. IEEE, 2003, pp. 975–981.

[75] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF Requests for Comments, RFC 4271, January 2006.

[76] Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)," IETF Requests for Comments, RFC 4271, January 1995.

[77] T. Järvi, "Layer 2 Solutions in Access Provider Networks," 2020.

[78] R. Moskowitz, P. Nikander, P. Jokela *et al.*, "Host Identity Protocol (HIP) Architecture," IETF Requests for Comments, RFC 4223, May 2006.

[79] M. Liyanage, M. Ylianttila, and A. Gurtov, "Software defined VPLS architectures: Opportunities and challenges," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–7.

[80] ——, "Secure Hierarchical VPLS Architecture for Provider Provisioned Networks," *IEEE Access*, vol. 3, pp. 967–984, 2015.

[81] T. Bates, E. Chen, and R. Chandra, "BGP Route Reflection: An Alternative to Full Mesh Internal BGP," IETF Requests for Comments, RFC 4456, April 2006.

[82] L. Fang, "Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)," IETF Requests for Comments, RFC 4111, July 2005.

[83] A. Barbir, S. Murphy, and Y. Yang, "Generic Threats to Routing Protocols," IETF Requests for Comments, RFC 4593, October 2006.

[84] S. Bellovin, J. Schiller, and C. Kaufman, "Security Mechanisms for the Internet," IETF Requests for Comments, RFC 3631, December 2003.

[85] N. E. Hastings and P. A. McLean, "TCP/IP spoofing fundamentals," in *Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on Computers and Communications*. IEEE, 1996, pp. 218–224.

[86] M. H. Behringer and M. Morrow, *MPLS VPN Security*. Cisco Press, 2005.

[87] D. E. Whitehead and A. D. Risley, "System and method for optimizing error detection to detect unauthorized modification of transmitted data," March 2010, US Patent 7,680,273.

[88] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP," in *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097)*. IEEE, 1997, pp. 208–223.

[89] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet computing*, vol. 10, no. 1, pp. 82–89, 2006.

[90] F. Salahdine and N. Kaabouch, "Social engineering attacks: A Survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019.

[91] A. Heffernan, "Protection of BGP Sessions via the TCP MD5 Signature Option," IETF Requests for Comments, RFC 2385, August 1998.

[92] R. Rivest, "The MD5 Message-Digest Algorithm," 1992.

[93] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (S-BGP)," *IEEE Journal on Selected areas in Communications*, vol. 18, no. 4, pp. 582–592, 2000.

[94] L. Andersson, P. Doolan, N. Feldman, A. Fredette, and B. Thomas, "LDP Specification," IETF Requests for Comments, RFC 5036, October 2001.

[95] M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Secure Virtual Private LAN Services: An Overview with Performance Evaluation," in *2015 IEEE International Conference on Communication Workshop (ICCW)*. IEEE, 2015, pp. 2231–2237.

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

[97] 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.

[98] M. Liyanage, M. Ylianttila, and A. Gurtov, "Improving the Tunnel Management Performance of Secure VPLS Architectures with SDN," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2016, pp. 530–536.

[99] K. S. Sahoo, S. K. Panda, S. Sahoo, B. Sahoo, and R. Dash, "Toward secure software-defined networks against distributed denial of service attack," *The Journal of Supercomputing*, vol. 75, no. 8, pp. 4829–4874, 2019.

[100] A. Shaghaghi, M. A. Kaafar, R. Buyya, and S. Jha, "Software-Defined Network (SDN) Data Plane Security: Issues, Solutions, and Future Directions," in *Handbook of Computer Networks and Cyber Security*. Springer, 2020, pp. 341–387.

[101] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, "Secure Communication Channel Architecture for Software Defined Mobile Networks," *Computer Networks*, vol. 114, pp. 32–50, 2017.

[102] S. Papadopoulos, K. Moustakas, A. Drosou, and D. Tzovaras, "Border Gateway Protocol Graph: Detecting and Visualising Internet Routing Anomalies," *IET Information Security*, vol. 10, no. 3, pp. 125–133, 2016.

[103] P. Edwards, L. Cheng, and G. Kadam, "Border Gateway Protocol Anomaly Detection Using Machine Learning Techniques," *SMU Data Science Review*, vol. 2, no. 1, p. 5, 2019.

[104] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A Security Enforcement Kernel for OpenFlow Networks," in *Proceedings of the first workshop on Hot topics in software defined networks*, 2012, pp. 121–126.

[105] E. Al-Shaer and S. Al-Haj, "FlowChecker: Configuration Analysis and Verification of Federated OpenFlow Infrastructures," in *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*, 2010, pp. 37–44.

[106] A. Khurshid, X. Zou, W. Zhou, M. Caesar, and P. B. Godfrey, "Veriflow: Verifying Network-Wide Invariants in Real Time," in *Presented as part of the 10th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 13)*, 2013, pp. 15–27.

[107] T. Feng, J. Bi, G. Yao, and P. Xiao, "InSAVO: Intra-AS IP Source Address Validation Solution with OpenRouter," in *proceedings of INFOCOM*, 2012.

[108] P. Kazemian, M. Chang, H. Zeng, G. Varghese, N. McKeown, and S. Whyte, "Real Time Network Policy Checking Using Header Space Analysis," in *Presented as part of the 10th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 13)*, 2013, pp. 99–111.

[109] P. Zhang, S. Xu, Z. Yang, H. Li, Q. Li, H. Wang, and C. Hu, "Foces: Detecting Forwarding Anomalies in Software Defined Networks," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2018, pp. 830–840.

[110] Q. Li, X. Zou, Q. Huang, J. Zheng, and P. P. Lee, "Dynamic Packet Forwarding Verification in SDN," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 915–929, 2018.

[111] A. Voellmy and J. Wang, "Scalable Software Defined Network Controllers," in *Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication*, 2012, pp. 289–290.

[112] K. Phemius, M. Bouet, and J. Leguay, "DISCO: Distributed Multi-Domain SDN Controllers," in *2014 IEEE Network Operations and Management Symposium (NOMS)*. IEEE, 2014, pp. 1–4.

[113] A. Tootoonchian and Y. Ganjali, "Hyperflow: A Distributed Control Plane for Openflow," in *Proceedings of the 2010 internet network management conference on Research on enterprise networking*, vol. 3, 2010.

[114] S. W. Shin, P. Porras, V. Yegneswara, M. Fong, G. Gu, M. Tyson *et al.*, "Fresco: Modular Composable Security Services for Software-Defined Networks," in *20th Annual Network & Distributed System Security Symposium*. Ndss, 2013.

[115] L. Schehlmann and H. Baier, "COFFEE: A Concept Based on OpenFlow to Filter and Erase Events of Botnet Activity at High-Speed Nodes," *INFORMATIK 2013–Informatik angepasst an Mensch, Organisation und Umwelt*, 2013.

[116] M. Liyanage, M. Ylianttila, and A. Gurtov, "Securing the Control Channel of Software-Defined Mobile Networks," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*. IEEE, 2014, pp. 1–6.

[117] M. Dhawan, R. Poddar, K. Mahajan, and V. Mann, "SPHINX: Detecting Security Attacks in Software-Defined Networks," in *Ndss*, vol. 15, 2015, pp. 8–11.

[118] A. Shaghaghi, M. A. Kaafar, and S. Jha, "Wedgetail: An Intrusion Prevention System for the Data Plane of Software Defined Networks," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017, pp. 849–861.

[119] K. Khandekar and T. Regan, "Hierarchical Virtual Private LAN Service," IETF Requests for Comments, RFC, June 2002.

[120] L. Martini, A. Sajassi, W. M. Townsley, and R. M. Pruss, "Scalable Virtual Private Local Area Network Service," July 2010, US Patent 7,751,399.

[121] P.-C. Wang, C.-T. Chan, and P.-Y. Lin, "MAC Address Translation for Enabling Scalable Virtual Private LAN Services," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, vol. 1. IEEE, 2007, pp. 870–875.

[122] G. López and E. Grampín, "Scalability Testing of Legacy MPLS-Based Virtual Private Networks," in *2017 IEEE URUCON*. IEEE, 2017, pp. 1–4.

[123] L. Dunbar, T. B. Mack-Crane, S. Hares, R. Sultan, P. Ashwood-Smith, and G. Yin, "Virtual Layer 2 and Mechanism to Make it Scalable," Mar. 6 2018, US Patent 9,912,495.

[124] O. Ben-Shalom, A. Nayshtut, and N. M. Smith, "System, Apparatus And Method For Massively Scalable Dynamic Multipoint Virtual Private Network Using Group Encryption Keys," Jan. 18 2018, US Patent App. 15/209,949.

[125] T. Hammam, A. Franzen, S. Abdallah, and F. Beste, "Method And Apparatus for Connecting a Gateway Router to a Set of Scalable Virtual IP Network Appliances in Overlay Networks," May 30 2017, US Patent 9,667,538.

[126] L. Dong and Y. Yang, "Scalable Handling of BGP Route Information in VXLAN with EVPN Control Plane," Apr. 4 2017, US Patent 9,614,763.

[127] M. Liyanage, M. Ylianttila, and A. Gurtov, "Fast Transmission Mechanism for Secure VPLS Architectures," in *2017 IEEE International Conference on Computer and Information Technology (CIT)*. IEEE, 2017, pp. 192–196.

[128] R. Behringer and H. White, "A Framework for Defining Network Complexity," IETF Requests for Comments, RFC 7980, October 2016.

[129] A. Steffen, "Virtual Private Networks Coping with Complexity," in *DFN-Arbeitstagung über Kommunikationsnetze*. Citeseer, 2003, pp. 289–302.

[130] A. Shelest and C. Huitema, "Reducing Network Configuration Complexity with Transparent Virtual Private Networks," Dec. 4 2007, US Patent 7,305,705.

[131] J. Keane, C. Macey, and S. Bendinelli, "Methods and Systems for Firewalling Virtual Private Networks," May 12 2009, US Patent 7,533,409.

[132] S. Beker, D. Kofman, and N. Puech, "Off-Line Reduced Complexity Layout Design for MPLS Networks," in *Proceedings of the 3rd IEEE Workshop on IP Operations & Management (IPOM 2003)(IEEE Cat. No. 03EX764)*. IEEE, 2003, pp. 99–105.

[133] I. H. Duncan and N. L. Bragg, "Reduced Complexity Multi Protocol Label Switching," Jun. 26 2014, US Patent App. 13/724,400.

[134] J. Kuo and C. M. Burns, "A Work Domain Analysis for Virtual Private Networks," in *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0*, vol. 3. IEEE, 2000, pp. 1972–1977.

[135] M. Walter, N. Campagna, Y.-Z. Chen, and M. S. Gill, "Credentials Management in Large Scale Virtual Private Network Deployment," Apr. 5 2016, US Patent 9,306,911.

[136] O. Z. Zheng, M. Ali, and K. Basu, "Comparing the Complexity of Two Network Architectures," *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, pp. 2516–0281, 2017.

[137] M. Liyanage, M. Ylianttila, and A. Gurtov, "IP-Based Virtual Private Network Implementations in Future Cellular Networks," in *Handbook of Research on Progressive Trends in Wireless Communications and Networking*. IGI Global, 2014, pp. 44–66.

[138] C. C. Aysan and R. C. Wadasinghe, "Tunneling scheme optimized for use in virtual private networks," May 2008, US Patent 7,379,465.

[139] D. Farinacci, T. Li, S. Hanks, D. Meyer, and P. Traina, "Generic routing encapsulation (GRE)," IETF Requests for Comments, RFC 2784, March 2000.

[140] A. Freier, P. Karlton, and P. Kocher, "The Secure Sockets Layer (SSL) Protocol Version 3.0," IETF Requests for Comments, RFC 6101, August 2011.

[141] T. Dierks and E. Rescorla, "RFC 5246-The Transport Layer Security (TLS) Protocol Version 1.2," IETF Requests for Comments, RFC 5246, August 2008.

[142] A. Alshamsi and T. Saito, "A technical comparison of IPSec and SSL," in *19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers)*, vol. 2. IEEE, 2005, pp. 395–398.

[143] R. Stanton, "Securing VPNS: Comparing SSL and IPsec," *Computer Fraud & Security*, vol. 2005, no. 9, pp. 17–19, 2005.

[144] E. Rescorla and T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF Requests for Comments, RFC 8446, August 2018.

[145] G. Lopez-Millan, R. Marin-Lopez, and F. Pereniguez-Garcia, "Towards a Standard SDN-based IPsec Management Framework," *Computer Standards & Interfaces*, p. 103357, 2019.

[146] C. R. Davis, *IPSec: Securing VPNs*. McGraw-Hill Professional, 2001.

[147] P. Jokela, R. Moskowitz, and P. Nikander, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)," *RFC5202, April*, 2008.

[148] P. Nikander and J. Melen, "A Bound End-to-End Tunnel (BEET) mode for ESP: draft-nikander-esp-beet-mode-09," *Work in progress*, 2008.

[149] A. Gurtov, *Host identity protocol (HIP): Towards the Secure Mobile Internet*. John Wiley & Sons, 2008, vol. 21.

[150] M. Liyanage and A. Gurtov, "A scalable and secure VPLS architecture for provider provisioned networks," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2013, pp. 1115–1120.

[151] O. Ponomarev and A. Gurtov, "Stress Testing of Host Identity Protocol (HIP) Implementations," in *proceedings of Third International Conference on Internet Technologies and Applications*, 2009.

[152] M. Emmendorfer, T. Cloonan, and E. Arnold, "Extended Layer Two Tunneling Protocol Applications and Architectures," May 10 2016, US Patent 9,338,024.

[153] S. Salam, A. Sajassi, and S. Boutros, "Mechanism for E-VPN Interoperability with VPLS," Feb. 3 2015, US Patent 8,948,169.

[154] D. A. Proulx, "Pseudowire Tunnel Redundancy," Jun. 14 2011, US Patent 7,961,599.

[155] J. K. Frick, C. A. Alexander Jr, O. L. Stokes Jr, C. F. Burton III, and D. B. Grosser Jr, "Methods and Systems for Providing Redundant Connectivity Across a Network Using a Tunneling Protocol," Sep. 11 2007, US Patent 7,269,135.

[156] "Compatibility Definition," Website, 2013. [Online]. Available: https://whatis.techtarget.com/definition/compatibility

[157] Y. N. Rajakarunanayake, "Virtual L2TP/VPN Tunnel Network and Spanning Tree-Based Method for Discovery of L2TP/VPN Tunnels and Other Layer-2 Services," Jul. 20 2004, US Patent 6,765,881.

[158] Y. Kotser, "Spanning Tree Protocol Traffic in a Transparent LAN," Oct. 24 2006, US Patent 7,127,523.

[159] K. Kompella, "Spanning Tree Protocol Synchronization Within Virtual Private Networks," Nov. 29 2011, US Patent 8,068,442.

[160] D. M. Colven, M. Mukhopadhyay, and H. Sudharshan, "Seamless Migration from Multiple Spanning Tree Protocol to Ethernet Ring Protection Switching Protocol," Mar. 20 2018, US Patent 9,923,731.

[161] Z. Gao, "Provider Edge in Virtual Private LAN Service Network," Jul. 11 2017, US Patent 9,705,788.

[162] Z. Li, Y. Jingming, and D. Qu, "Virtual Private Network Implementation Method and System Based on Traffic Engineering Tunnel," Aug. 7 2014, US Patent App. 14/252,055.

[163] S. A. Wright, "Method for Traffic Engineering of Connectionless Virtual Private Network Services," Jan. 12 2010, US Patent 7,646,734.

[164] M. Naraghi-Pour and V. Desai, "Loop-Free Traffic Engineering with Path Protection in MPLS VPNs," *Computer Networks*, vol. 52, no. 12, pp. 2360–2372, 2008.

[165] N. AbuAli, H. T. Mouftah, and S. Gazor, "Multi-Path Traffic Engineering Distributed VPLS Routing Algorithm," in *2005 Systems Communications (ICW'05, ICHSN'05, ICMCS'05, SENET'05)*. IEEE, 2005, pp. 275–280.

[166] R. R. Talpade, G. T. Kim, S. Samtani, L. H. Wong, and P. Mouchtaris, "Method and System for Quality of Service Provisioning for IP Virtual Private Networks," Mar. 1 2005, US Patent 6,862,291.

[167] A. Z. Bhat, D. K. Al Shuaibi, and A. V. Singh, "Virtual Private Network as a Service—A Need for Discrete Cloud Architecture," in *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. IEEE, 2016, pp. 526–532.

[168] J. Van Der Merwe, A. Baliga, X. Chen, B. Coskun, G. De Los Reyes, S. Lee, S. Mathur, and G. Xu, "Methods and Apparatus to Configure Virtual Private Mobile Networks with Virtual Private Networks," Aug. 7 2018, US Patent 10,044,678.

[169] K. Dolan, "Introduction to IDN," ESG, 2017, https://www.esg-global.com/validation/esg-lab-review-identity-defined-networking-from-tempered-networks.

[170] E. G. Andrei Gurtov and M. Kaplan, "IDN Introduction," Website, 2017. [Online]. Available: https://www.ida.liu.se/TDDD17/lectures/slides/idn_tdd17.pdf

[171] A. Sajassi, R. Aggarwal, J. Uttaro, N. Bitar, W. Henderickx, and A. Isaac, "Requirements for ETHERNET VPN (EVPN)," IETF Requests for Comments, RFC 7209, May 2014.

[172] A. Sajassi, R. Aggarwal, N. Bitar, A. Isaac, J. Uttaro, J. Drake, and W. Henderickx, "BGP MPLS based ETHERNET VPN," IETF Requests for Comments, RFC 7432, February 2015.

[173] W. Goralski, "Chapter 21 - EVPN and VXLAN," in *The Illustrated Network (Second Edition)*, second edition ed., W. Goralski, Ed. Boston: Morgan Kaufmann, 2017, pp. 535 – 560. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780128110270000217

[174] T. Singh, V. Jain, and G. S. Babu, "VXLAN and EVPN for Data Center Network Transformation," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2017, pp. 1–6.

[175] C. DeCusatis, "Chapter 13 - Network Architectures and Overlay Networks," in *Handbook of Fiber Optic Data Communication (Fourth Edition)*, fourth edition ed., C. DeCusatis, Ed. Oxford: Academic Press, 2013, pp. 321 – 337. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780124016736000131

[176] Y. Nakagawa, K. Hyoudou, and T. Shimizu, "A Management Method of IP Multicast in Overlay Networks Using Openflow," in *Proceedings of the first workshop on Hot topics in software defined networks*, 2012, pp. 91–96.

[177] H. Zhang, "Communication Between Endpoints in Different VXLAN networks," Jun. 21 2016, US Patent 9,374,323.

[178] S. Bemby, H. Lu, K. H. Zadeh, H. Bannazadeh, and A. Leon-Garcia, "ViNO: SDN Overlay to Allow Seamless Migration Across Heterogeneous Infrastructure," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 2015, pp. 782–785.

[179] A. Gurtov, M. Liyanage, and D. Korzun, "Secure Communication and Data Processing Challenges in the Industrial Internet," *Baltic Journal of Modern Computing*, vol. 4, no. 4, pp. 1058–1073, 2016.

[180] M. Borhani, M. Liyanage, A. H. Sodhro, P. Kumar, A. D. Jurcut, and A. Gurtov, "Secure and Resilient Communications in the Industrial Internet," in *Guide to Disaster-Resilient Communication Networks*. Springer, 2020, pp. 219–242.

[181] M. Liyanage and A. Gurtov, "Secured VPN Models for LTE Backhaul Networks," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*. IEEE, 2012, pp. 1–5.

[182] M. Liyanage, P. Kumar, M. Ylianttila, and A. Gurtov, "Novel Secure VPN Architectures for LTE Backhaul Networks," *Security and Communication Networks*, vol. 9, no. 10, pp. 1198–1215, 2016.

[183] M. Liyanage, I. Ahmad, M. Ylianttila, A. Gurtov, A. B. Abro, and E. M. de Oca, "Leveraging LTE Security with SDN and NFV," in *2015 IEEE 10th International Conference on Industrial and Information Systems (ICIIS)*. IEEE, 2015, pp. 220–225.

[184] B. Raahemi and B. Bou-Diab, "A Minimum-Cost Resilient Tree-Based VPLS for Digital TV Broadcast Services," in *2006 Canadian Conference on Electrical and Computer Engineering*, 2006, pp. 995–998.

[185] S. Pompei, M. Teodori, A. Valenti, S. Di Bartolo, G. Incerti, and D. Del Buono, "Experimental implementation of an IPTV architecture based on Content Delivery Network managed by VPLS technique," in *International Congress on Ultra Modern Telecommunications and Control Systems*, 2010, pp. 576–581.

[186] "SIGMONA Project," Website, 2013. [Online]. Available: https://www.celticnext.eu/project-sigmona/

[187] "TDP Project," Website, 2017. [Online]. Available: https://www.oulu.fi/cwc/tdp

[188] "SecureConnect Project," Website, 2016. [Online]. Available: https://sites.google.com/view/secureconnect/home

[189] "TDP Project," Website, 2017. [Online]. Available: https://nakedapproach.fi//

[190] "TWAREN Project," Website, 2020. [Online]. Available: http://www.twaren.net/english/AboutTwaren/Initiative/

[191] "International GENI," Website, 2018. [Online]. Available: https://groups.geni.net/geni/raw-attachment/wiki/IGENI/GEC11-poster-Jul18\%5b1\%5d.pdf
[192] "MEVICO Project," Website, 2010. [Online]. Available: http://www.mevico.org/pressrelease1.pdf
[193] "CELTIC Project," Website, 2010. [Online]. Available: https://www.celticnext.eu/
[194] K. Ichikawa, P. U-Chupala, C. Huang, C. Nakasan, T.-L. Liu, J.-Y. Chang, L.-C. Ku, W.-F. Tsai, J. Haga, H. Yamanaka *et al.*, "PRAGMA-ENT: An International SDN testbed for cyberinfrastructure in the Pacific Rim," *Concurrency and Computation: Practice and Experience*, vol. 29, no. 13, p. e4138, 2017.
[195] J.-W. Hu, C.-S. Yang, and T.-L. Liu, "L2OVX: An On-Demand VPLS Service with Software-Defined Networks," in *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. IEEE, 2016, pp. 861–866.
[196] X. Yang, "SDN for End-to-end Networked Science at the Exascale (SENSE)-Final Technical Report," Univ. of Maryland, College Park, MD (United States), Tech. Rep., 2019.