Chapter 1

Literature review

1.1 Introduction

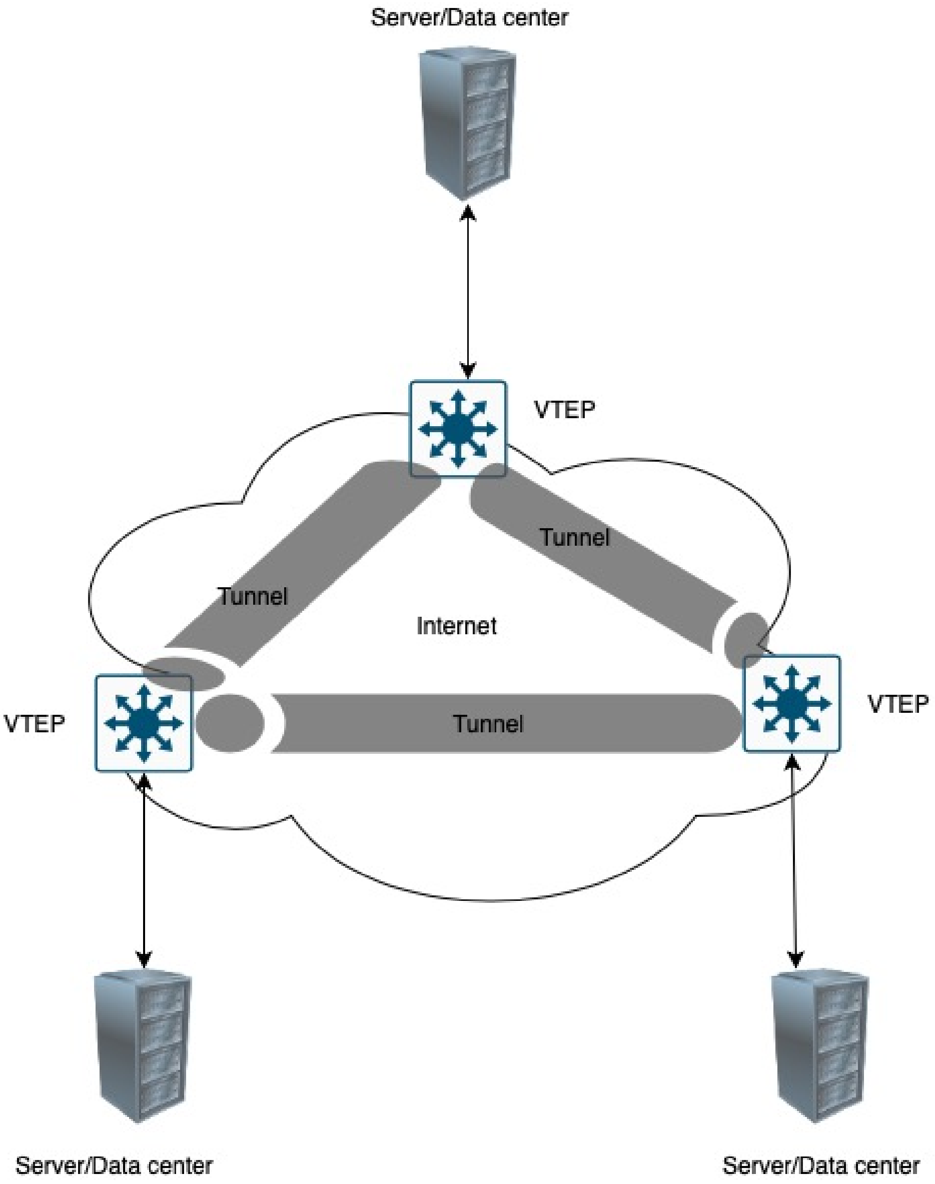
These days usage of LAN[1] extensions are widely used by organisations who have sites geographically apart and organisations have to rely on public internet to make the extensions possible. Having connected by public cloud, there are risks in exchanging data in plain text. In this section author is briefing the studies author performed during the course of this research. The study includes the existing LAN extension technologies, existing security solutions and their shortcomings.

1.2 Major Layer2 extension technologies

Multi-Protocol Label Switching (MPLS) and Virtual Extensible LAN (VXLAN) are the most used protocols for connecting LANs

1.3 Virtual Extensible LAN (VXLAN)

Virtual extensible Local Area Network (VXLAN) is one of the Network Virtualization over Layer 3 technologies defined by the Internet Engineering Task Force (IETF) and is an extension to Virtual Local Area Network (VLAN). VXLAN encapsulates a Layer 2 Ethernet frame into a UDP packet and transmits the packet over a Layer 3 network.



VxLAN Network

As shown in Figure VxLAN Network, VXLAN is essentially a tunneling technology. It establishes a logical tunnel on the IP network between the source and destination network devices to encapsulate user-side packets and forward them through the tunnel. Servers are connected to different ports of network devices in the data center VXLAN network, which can be considered as a virtual Layer 2 switch. VXLAN has become the mainstream technology for constructing data center networks because it can meet the requirements of dynamic virtual machine (VM) migration and multi-tenancy in data center networks. It was initially designed to address the issues related to scalability in large-scale network deployments such as ISPs or cloud providers. As the name implies, VxLAN virtually extends a layer 2 segment across the layer 3 network infrastructure. VxLAN encapsulates the layer 2 Ethernet frames inside a VXLAN packet that includes an IP address.

VxLAN segments are identified by a 24-bit VNID (VxLAN Identification) field which can scale to 16 million segments. The VxLAN is a standardized specification created by the collaboration of VMware, Cisco, and Arista Network vendors. VxLAN is defined in the RFC 7348. VxLAN is very similar to VLAN, which also encapsulates layer 2 frames and segments networks. The main difference is that VLAN uses the tag on the layer 2 frame for encapsulation and can scale up to 4000 VLANs. VXLAN, on the other hand, encapsulates the MAC in UDP and is capable of scaling up to 16 million VxLAN segments.

1.3.1 Major advantages of VxLAN

It is a fact that one of the significant benefits of VxLAN is scalability. But when you can span layer 2 networks across IP network infrastructure, there are also many more benefits.

Scalability and flexibility

VxLAN improves the scalability in a network or virtualized data center, and it also makes its fabric more flexible. The number of VLAN layer 2 identifiers are drastically increased from 4,000 to 16 million.

Segmentation and Multi-tenancy

VxLAN provides a high level of security by segmenting the network. The VxLAN traffic is limited to VNI, so it is isolated. This segmentation can also help in multi-tenant architectures, where a single infrastructure must be shared.

Layer 2 Simplification

Simplify the network and reduce the need for layer 2 Spanning Trees, Trunking, and VLAN stretching.

Allow IP Mobility

VMs can be migrated from a host in a subnet to another host in another subnet without having to change the IP address.

Layer 2 and layer 3 Connectivity

A virtual layer 2 running VNIs is built upon a layer 3 infrastructure running IP. VxLAN switches encapsulate layer 2 frames into layer 3 packets.

It is a Software-Defined Network (SDN)

VxLAN decouples the central network controller (virtual network) from the data plane (physical network). Having a centralized controller simplifies network management, deployment, and monitoring. An example of a software-based virtual network switch that supports VxLAN overlays is Open vSwitch.

Hardware Support

Although it is more common to run VxLAN in software, some platforms implement it in hardware through ASICs. An example is Ciscos Nexus 9000-EX platform switches.

It is a standard

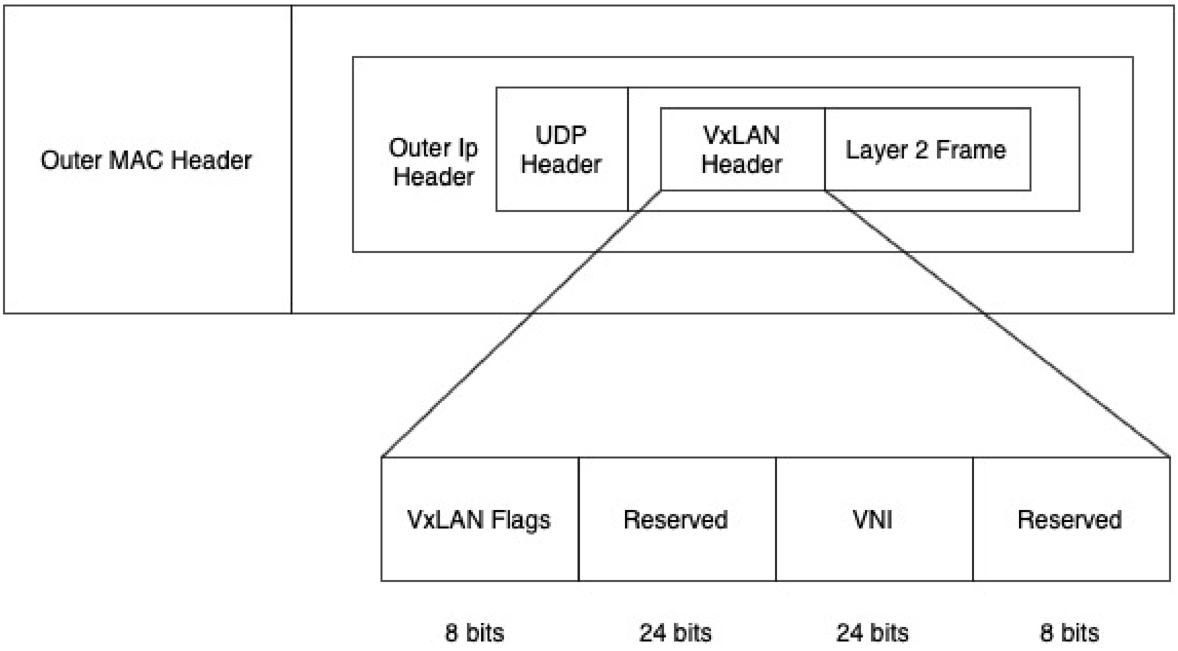
VXLAN is a technical standard. When you implement it, you are not locked by any vendor.

1.3.2 VXLAN Encapsulation

We know so far that VxLAN stretches the layer 2 subnets across the layer 3 network limits. It builds a logical overlay network on top of a switching fabric like the Spine-and-Leaf.

It uses a VLAN-like encapsulation technology to encapsulate OSI layer 2 Ethernet frames into layer 4 UDP datagrams, with 4789 as the default IANA-assigned destination UDP port number. VXLAN tunnel endpoints, which might be virtual or actual switch ports, are VXLAN endpoints that terminate VXLAN tunnels.

The following picture shows the VxLAN packet format.



VxLAN Header

VxLAN adds the following fields to the original Layer 2 frame.

Outer MAC header

This is the header that contains information for next-hop transport. It includes the destination and the source MAC address of the VxLAN endpoints, a VLAN ID (16 bits), and Type. The size of the outer MAC header is 14 bytes.

Outer IP header

This header allows transport across the IP network. It includes the destination and the source IP address of the VxLAN endpoints. The size of the outer IP header is 20 bytes.

Outer UDP header

This header identifies the packet as VxLAN. It contains the UDP source port, VxLAN port, and UDP length. The size of the UDP header is 8 bytes.

VxLAN header

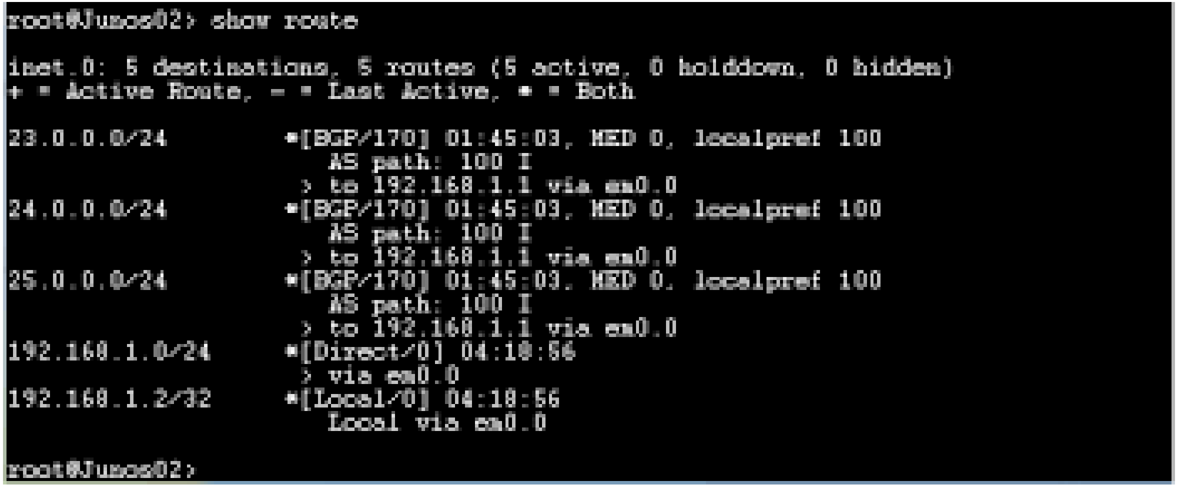
This header is also referred to as the VxLAN Network Identifier (VNI). The VNID is used to identify the VxLAN segment. It is similar to the VLAN ID tag (16 bits) found on the MAC header but with a size of 24 bits, which allows up to 16 million different segments.

1.3.3 VxLAN Tunnel Endpoints (VTEPs)

Any endpoint like a host, switch, or router that supports VxLAN can be referred to as a VTEP (VxLAN Tunnel Endpoint). As the name implies, the job of VTEPs is to create and terminate tunnels between each other. In other words, they encapsulate and decapsulate VxLAN traffic.

Working of VTEP

The VTPE is connected to the underlay network using a layer 3 IP address. VTPEs may have one or more VNIs associated with it. When a layer 2 frame with the same VNI arrives at the ingress VTEP, it encapsulates the frame with a VxLAN and UDP/IP headers. Then sends it over using the underlay IP network transport towards the table.png



```
root@Junos02> show route

inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

23.0.0.0/24        *[BGP/170] 01:45:03, MED 0, localpref 100
                      AS path: 100 I
                    > to 192.168.1.1 via em0.0
24.0.0.0/24        *[BGP/170] 01:45:03, MED 0, localpref 100
                      AS path: 100 I
                    > to 192.168.1.1 via em0.0
25.0.0.0/24        *[BGP/170] 01:45:03, MED 0, localpref 100
                      AS path: 100 I
                    > to 192.168.1.1 via em0.0
192.168.1.0/24     *[Direct/0] 04:18:56
                    > via em0.0
192.168.1.2/32     *[Local/0] 04:18:56
                      Local via em0.0

root@Junos02>
```

Figure 1.1: Sample routing table

egress VTEP for decapsulation. The egress VTEP removes the IP and UDP headers and delivers the original layer 2 frame.A VTEP can be either a virtual or a physical switch port and is usually configured on leaf switches.

1.4 Multi Protocol Label Switching (MPLS)

In MPLS Networks, Packets are forwarded using the 20 Byte Labels unlike the 32 bit IP Address. In order to understand the working of MPLS and its advantages over conventional IP Network, we must understand how the traditional IP traffic processed.

1.4.1 IP Routing

IP routing[2] is the process of sending packets from one L3 host to another. The hosts can be in same or different networks and the networks are identified using the IP Addresses. Each packet will have a field for source address and destination address and the packets are forwarded based on the destination address. All the IP Networking devices will maintain a routing table. The devices can be a host machine or a router. The routing table consists of an address field where we can see a 32 bit address and an interface field where we can see a physical or logical interface corresponding to the address.

Network.png

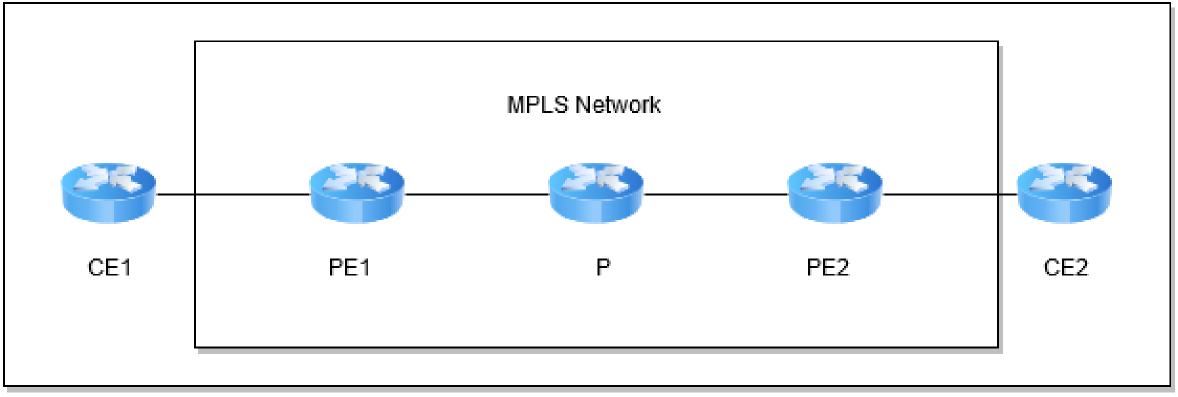


Figure 1.2: MPLS Network

The figure 1.1 is a sample of routing table from a Juniper router. We can see the networks and the corresponding exit interfaces. Theses routing tables are created and maintained by different routing protocols and each routing protocol have its own mechanisms of finding the best route to the destination. OSPF, RIP and BGP are the well-known routing protocols[3].

1.4.2 MPLS Switching

Multi-protocol label switching (MPLS)[4], is a technique that uses 20-bit labels instead of 32-bit IP Address for sending packet from one MPLS router to another. The Labels are pre populated using different protocols such as Label Distribution Protocol (LDP), Resource Reservation Protocol (RSVP) or Multiprotocol BGP (MP BGP). The packet switching is happening at 2.5 header of the OSI reference model and hence it's called switching. As MPLS need the help of other protocols to create the labels, the name multi-protocol labelled switching

In the Figure 1.2 the CE1 is a L3 router which operates exclusively on IP address and PE1 is called provider edge router which will operate on both IP address and labels. P is provider router which works exclusively on labels. The incoming packets from CE1 in PE1 taken to a class called Forward equivalence class which assign a label corresponding to the destination IP address. The PE1 then forward the packet to P router which will pop the existing label and add its label corresponding to the destination and finally PE2 will pop the MPLS header from the packet and forward

Network.png

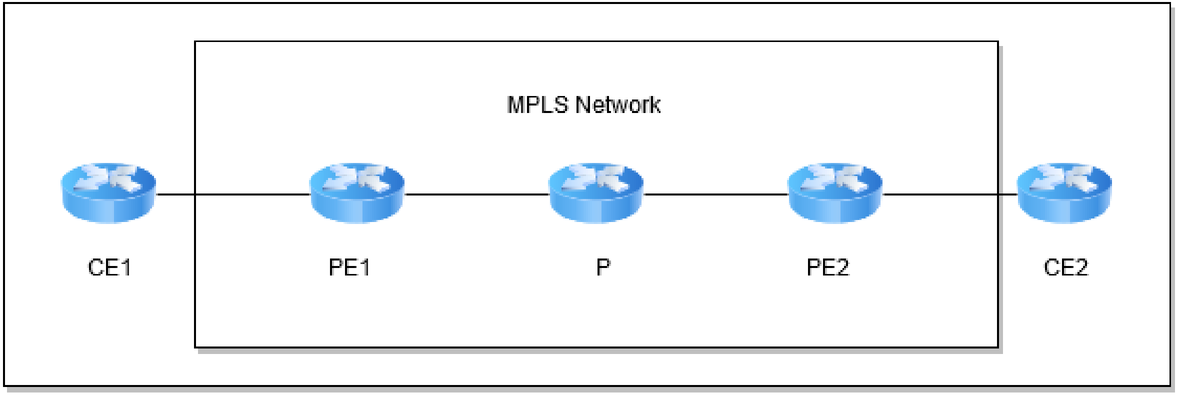


Figure 1.3: MPLS Network

the packet to CE2 using IP routing table.

MPLS header gets in between the Ethernet header and the IP Header. The header is 4 bytes in size. The first 20 bits are for the labels, the next 3 bits are for class of service and the next 1 bit for the bottom of stack flag which basically say where the label is positioned. The last 8 bits are for the TTL (time to live).

Both VXLAN and MPLS have no inbuilt mechanism for protecting the data and headers. A combination of various technologies is used to address security when needed.

1.5 Possible attacks in MPLS and VXLAN

MPLS can be attacked in many ways[5]. There are tools available which can target various signalling protocols by sending dummy messages to initiate a session, keep the session open or close the session. Loki is one such tool which can use to attack MPLS. Security attacks were divided into four kinds: Data Plane Attacks, Control Plane Attacks, Network Operational and Management Attacks, and Insider Attacks. Similar to MPLS, VXLAN also prone to all these attacks because of the plain text nature

1.5.1 Attacks on the Data Plane

Attacks aimed mainly at User or Service Provider data are categorized into data-plane security attacks. These attacks are either aimed at manipulating the data flowing

Header.jpg

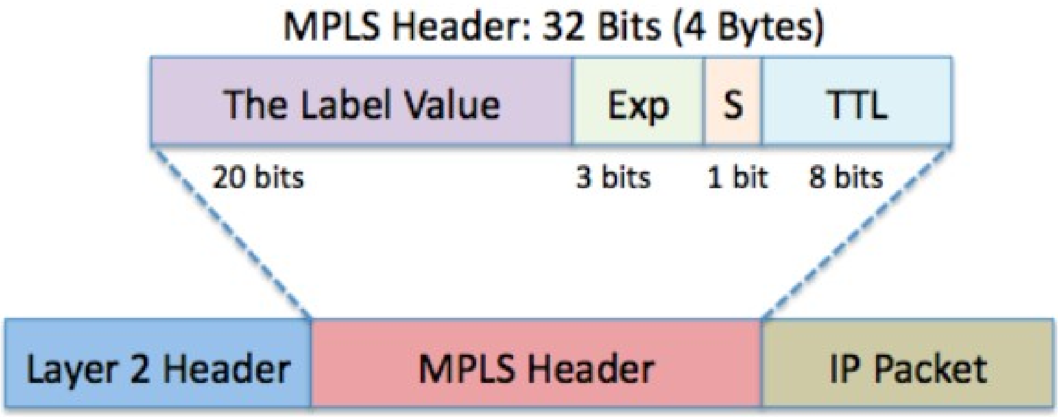


Figure 1.4: MPLS Header

through the network, removing the data flowing through the network, injecting malicious data or simply observing maliciously unauthorized data.

1.5.2 Taking the traffic outside the core

If an attacker has access to any core device, he can relabel or encapsulate an udp header with a destination address which attacker desired to send. Thus, the attacker can read or access the data from attacker's convenience. In order to do this, the attacker should be aware of the labels used in the traffic. Service providers usually hide the internal architecture of the core, but still it's not 100 percent safe.

1.5.3 Modify the Data Traffic

Manipulating or changing the header fields of the packets can cause severe damage to MPLS Network. This is only possible when the MPLS Internals are exposed to the attacker. Getting the access of the MPLS core is however not easy since service providers usually hide the core from outside. Service providers use firewalls and other filters in their core to filter and block illegitimate packets and accesses. But once the attacker somehow managed to gain the core access, He/ She can make sever damage to the Networks.

Listed few of the attacks which is possible by packet manipulations, they are:

1.5.4 Modify the routes

Attacker can manipulate the network field of the packets the CE router can route the packets to a different destination out of the MPLS Cloud. Attacker can change the L3 field, Labels or encapsulate an UDP Header with completely different Network information. If the attacker gain access to packets part of financial transactions, we can imagine the damage. Rerouting of traffic can take one customers traffic to another customers network.

1.5.5 Data Insertion attacks

This type of attacks is done by injecting forged traffic into the MPLS network and making the MPLS switch accept it as a genuine traffic and thus making it to forward the packets to the end devices. These packets are sent with malicious intentions to gain certain access to the end device or to read sensitive information.

1.5.6 Denial-of-Service (DOS) Attacks

DOS is a type of attack which make any service unavailable to its legitimate users. Each system have an upper scale on the number of requests in a second to handle. If the requests coming in are beyond its capacity, then the overloading requests may not be able to serve. If the requests are basically from an attacker just to make the system busy handling the request maximum to its capacity, then the legitimate requests from genuine users wont be served. Financial services, e commerce websites etc are very vulnerable to such attacks since these types of services expects huge number of transactions in a second.

Bibliography

[1] “Rfc 1918 - address allocation for private internets.”

[2] “Ip routing,” *TCP/IP Architecture, Design, and Implementation in Linux*, p. 499589, 2008.

[3] “Routing protocols,” *Designing and Developing Scalable IP Networks*, p. 4969, Jan 2005.

[4] A. Farrel, “Multiprotocol label switching (mpls),” *The Internet and Its Protocols*, p. 385490, 2004.

[5] D. Grayson, D. Guernsey, J. Butts, M. Spainhower, and S. Shenoi, “Analysis of security threats to mpls virtual private networks,” *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, p. 146153, 2009.