الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
جامعة عين تموشنت بلحاج بوشعيب
Université –Ain Temouchent- Belhadj Bouchaib
Faculté des Sciences et de Technologie
Département Génie électrique

Projet de Fin d'Etudes
Pour l'obtention du diplôme de Master en :
Domaine : Sciences et Technologie
Filière : Télécommunication
Spécialité : Réseaux et Télécommunications
Thème

Overlay Network and Tunneling

Présenté Par :
1) Mr. Mebarki Abdelilah
2) Melle. Ouahab Bahidja

Devant le jury composé de :

Dr Bentaieb Samia	MCB	UAT.B.B (Ain Temouchent)	Présidente
Dr Bengana Abdelfatih	MCB	UAT.B.B (Ain Temouchent)	Examinateur
Dr Slimane Zohra	MCA	UAT.B.B (Ain Temouchent)	Encadrante
Dr Bencherif Kaddour	MCA	UAT.B.B (Ain Temouchent)	Co-Encadrant

Année Universitaire 2020/2021

Dedication

First and foremost, to my parents, who taught me to work hard for the things I aspire to achieve. Thank you for giving me the strength to pursue my dreams.

I also dedicate this project to my brother ***Mourad****; my sisters and theirs husband; my nephews, my dear friend* ***Radia*** *and for all the people who have helped me from near or far to the realization of this work.*

Finally, I want to thank ***Abdelillah*** *for convincing me to work with him as a co-author on this thesis.*

Although the process was arduous at times, it was a blessing to be able to work together on this effort with someone as dedicated, intelligent, and motivated as ***Abdelillah****. I wish him all the best.*

Miss.BahidjaOUAHAB

Dedication

I dedicate this memory in the first place to my beloved parents who supported me during my years of study, my brother ***Ilyes*** *and my sisters, Ben Safi* ***Meriem*** *and any member of my family.*

My dear friends Ouaret ***Abdelkader****, NEDJARI* ***Houssem****, KHERIBAT* ***Youcef****, MEGHERBI Fatmi* ***Noureddine*** *who have supported me throughout the process. I will always appreciate all they have done.*

Finally, I want to thank Ouahab ***Bahidja*** *for convincing me to work with him as a co-author on this project.*

Thank you for always being here for me.

Mr.MEBARKI Abdelillah

Acknowledgement

We thank, first of all, Allah who has given us the strength and fortitude to achieve this modest development work.

We would like to express our special thanks of gratitude to our teacher Mrs ***Zohra SLIMANE.***

Secondly, we would also like to thank our parents and friends who helped us a lot in finalizing this project within the limited period.

Finally, we would like to thank Miss. ***Bentaieb Samia*** *and Mr.* ***Bengana Abdelfatih*** *and* ***Bencherif Kaddour*** *for being our jurors in this project.*

We take this opportunity to express our gratitude to all our teachers who have contributed by their collaboration, availability and sympathy with us during our presence at this institute.

Mr.Adelillah MEBARKI

Miss.Bahidja OUAHAB

Abstract

Multiprotocol Label Switching (MPLS) has long been the standard for wide area network (WAN), one of the most benefits of MPLS is that it delivers packets providing high Quality of service and proficiently manages and avoids packet loss. However, MPLS is complex, time-consuming to manage, and so expensive to upgrade and scale. SD-WAN comes to overcome many of those problems while creating security and predictability issues, it is considered as an overlay network which is a virtual network that is built on top of an underlying Network infrastructure such as MPLS.

Key words: MPLS, SD-WAN, Underlying, overlay.

Résumé

Le Multi-Protocol Label Switching a été pendant longtemps la norme pour les réseaux étendus. L'un des plus grands avantages du MPLS est qu'il délivre des paquets offrant un service de haute qualité avec une bonne gestion et il évite la perte de paquets. Toutefois, le MPLS est complexe, prend du temps à gérer et si coûteux pour améliorer et évoluer. SD-WAN vient surmonter plusieurs de ses problèmes tout en criant la s´sécurité et la prévisibilité. Il est considéré comme un réseau de superposition qui est un réseau virtuel construit au-dessus d'une infrastructure de réseau sous-couche telle que le MPLS.

Mots clés : MPLS, SD-WAN, sous-couche, superposition

الملخص

لطالما كان تبديل الملصقات متعدد البروتوكولات (MPLS) هو المعيار لشبكة المنطقة الواسعة، ومن أكثر فوائد MPLS أنه يقدم حزمًا توفر جودة عالية للخدمة ويدير ويتجنب فقدان الحزم بكفاءة. ومع ذلك، فإن MPLS معقد، وتستغرق إدارته وقتًا طويلاً ، كما أن ترقيته وتوسيع نطاقه مكلف للغاية. يأتي SD-WAN للتغلب على العديد من هذه المشكلات أثناء إنشاء مشكلات الأمان والقدرة على التنبؤ، ويعتبر بمثابة شبكة تراكب وهي شبكة افتراضية مبنية على البنية التحتية للشبكة الأساسية مثلMPLS .

الكلمات الرئيسية:MPLS SD-WAN، ،الأساس، التراكب.

List of acronyms

A

ATM: Asynchronous Transfer Mode

B

BGP: Border Gateway Protocol.

BoS: Bottom of Stack

C

CBWFQ: Class-Based Weighted Fair Queuing

CE: Customer Edge

CEF: Cisco Express Forwarding

D

DiffServ: Differentiated Services

DSCP: Differentiated Services Code Points

F

FIFO: First-In, First-Out

H

HDLC: High-Level Data Link Control

I

IntServ: Integrated Services

L

LFIB: Label Forwarding Information Base

LLQ: Low-Latency Queuing

M

MP-BGP: Multiprotocol-Border Gateway Protocol

MPLS: Multi-Protocol Label Switching

OMP: Overlay Management Protocol

O

OSPF: Open Shortest Path First

P

PE: Provider Edge

PHB: Per-Hop Behavior

PPP: Point-to-Point Protocol

PQ: Priority Queuing

Q

QoS: Quality of Service

R

RD: Route Distinguisher

RT: Route Target

S

SD-WAN: Software-Defined Wide Area Networks

SDN: Software-Defined Networking

T

TCP: Transmission Control Protocol

TDP: Tag Distribution Protocol

TTL: Time To Live

U

UDP: User Datagram Protocol

V

VPN: Virtual Private Network

VRF: Virtual Routing Forwarding

Contents

List of Figures

General Introduction

As enterprises expand and grow, they need to build a network infrastructure that connects their branch offices in different locations to the corporate head office or the data center in another geographical location. For years, enterprises have used private WAN services like MPLS which is provided by Internet service providers for enterprise WAN. When MPLS technology first appeared, there were no cloud-based apps and no mobile access to workplace systems. MPLS was a technology suitable for the requirements of the time. Moreover, it is so expensive, difficult to build and maintain, which enforce companies to move to a hybrid SD-WAN, which utilizes the best features of both traditional WANs and their software-defined counterparts. SD-WAN is a virtual solution that addresses the problems that traditional WANs like MPLS try to solve, but are cheaper, more efficient, and are able to be managed from a centralized application.

This document comprises four chapters:

Chapter I: In this chapter, we will talk about the fundamentals of MPLS in general, its benefits, MPLS applications... etc. After, we will show its process for forwarding the traffic by using some protocols and gives the architecture of MPLS.

Chapter II: which is the continuation of the previous chapter where we go to talk about one of the most popular applications (MPLS/VPN) and how its work and we will see the different protocols applied and the label forwarding mechanism.

Chapter III: In this chapter will go to explain how the MPLS network can leverage technical implementations to provide the various forms of quality of service (QoS) that businesses want.

Chapter IV: In this last chapter, we will talk about the need for SD-WAN in networking and we will discuss its functionalities by taking the example of Cisco SD-wan implementation.

I.1 Introduction

There were a variety of popular networking protocols in use before the advent of MPLS, including Frame Relay, ATM, and Ethernet. At the OSI Model's data-link layer, these networks are utilized to carry packets between multiple sites and offer connectivity and transit throughout a wide area network.

Over time, as networking grew exponentially in volume, the Previously used technologies and protocol didn't offer diversity or variety in terms of building a well scalable network and are closely related to single transport technology. Especially with the change in the structure format of packets, cells, and frames. Another important factor is that traffic engineering wasn't developed enough to allow a service provider to optimize the traffic flow and use of links as would be required of a service provider's network. MPLS was designed to overcome these problems by eliminating the need to inspect every field of every packet and the need to re-format or encapsulate frames and cells.

I.2 Definition of MPLS

MPLS is a data forwarding technology that boosts network traffic speed and control. It's a collection of protocols that establishes a new way for routers to forward packets. Instead of forwarding packets based on the IP addresses, MPLS introduces a new way to define packet routes, which is the MPLS label, depending on routing tables, each router on which a data packet arrived must make its own decision about the packet's next stop on the network. MPLS assigns a label to each packet before sending it down a specific path [1].

I.3 Benefits of MPLS

This section summarizes the advantages of using MPLS in your network.
The following are some of the advantages: The use of one unified network infrastructure.

- Border Gateway Protocol (BGP)-free core.
- The peer-to-peer model for MPLS VPN.
- Traffic engineering.

I.3.1 The use of one unified network infrastructure

The main idea for using the one unified network infrastructure with MPLS is to label ingress packets based on their address destination or other pre-configured criteria and switch all the traffic over a common infrastructure. This is the major advantage of MPLS. Many technologies can be transferred via IP, which is one of the main reasons why it has become the only protocol to dominate the networking industry. Telephony and data are both transmitted over IP. By integrating MPLS with IP, you can broaden the scope of what you can transport. Adding labels to packets allows various protocols other than IP to be carried across an MPLS-enabled Layer three IP backbone, comparable to what was previously only possible with Frame Relay or ATM Layer two networks. MPLS can transport IPv4, IPv6, Ethernet, even HDLC, PPP, and other Layer two technologies. Any Transport over MPLS is a feature that allows any Layer two frame to be carried via the MPLS backbone (AToM). The routers that need to switch AToM traffic don't need to know anything about MPLS; all they need to know is how to switch labeled traffic by looking at the label above. Basically, MPLS label switching is simply a method of switching multiple protocols into a single network. At the same time, the service provider needs one unified network infrastructure to transport all types of customer traffic. [2].

I.3.2 Border Gateway Protocol (BGP)-free core

When MPLS cloud is utilized at ISP core, BGP can be implemented at the network edges with the core routers carrying just the information about external prefixes, such as the customer prefixes or the Internet prefixes, and share routing information among the autonomous systems. This means that all routers in the service provider core must run BGP. MPLS, however, enables the forwarding of packets based on a label lookup instead of a lookup of the IP addresses. MPLS enables a label to be associated with an egress router instead of the destination IP address of the packet. The label is the information attached to the packet that tells each core router to which egress LSR router it must be forwarded. The Packets no longer need to be forwarded based on the destination IP address by intermediate LSR routers therefore, BGP is no longer necessary for core routers in the service provider's network. The router at the MPLS core's edge must still look at the packet's destination IP address, which necessitates the use of BGP. Each BGP prefix on the ingress LSR is issued a BGP next-hop IP address. This BGP next-hop IP address belongs to an egress LSR router. The label BGP next-hop IP address is the label that is connected with an IP

packet. BGP next-hop IP address. Each BGP next-hop IP address of an egress MPLS router must be configured for all core routers because every core router sends a packet based on the attached MPLS label that is associated with the BGP next-hop IP address. This can be done with any inner gateway routing protocol (IGP), such as OSPF or ISIS [2].

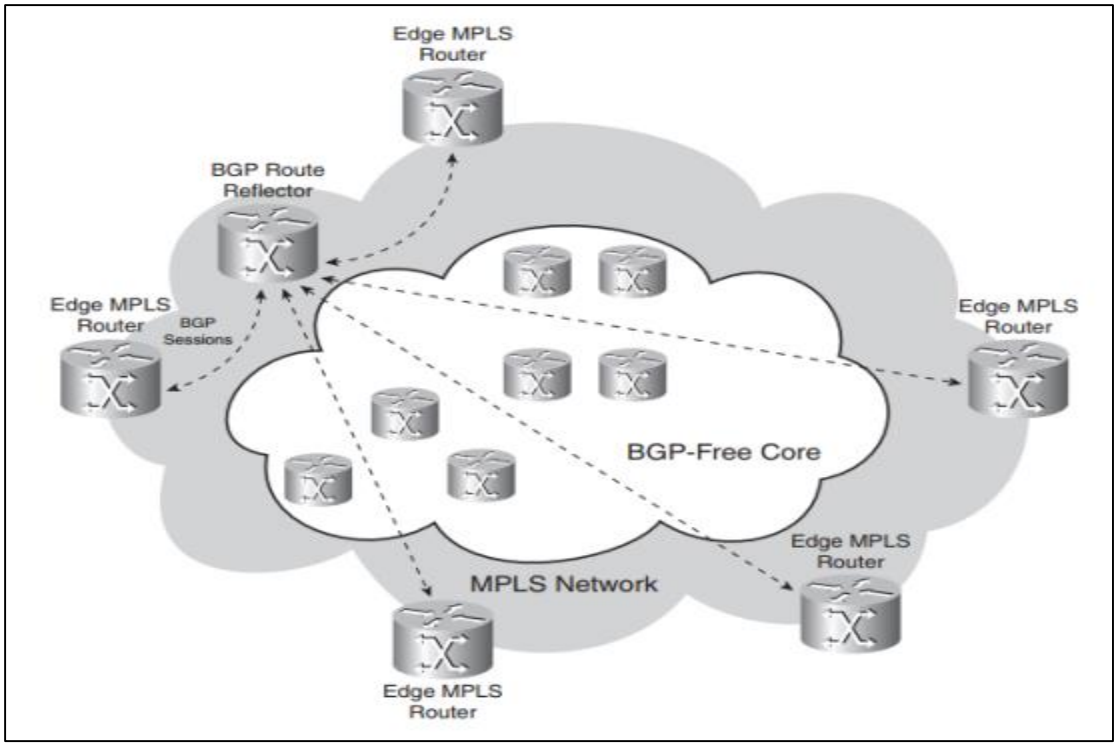


Figure 1.1: BGP-Free MPLS Network.

I.3.3 The peer-to-peer model for MPLS VPN

The service provider routers convey customer data across the network in the peer-to-peer VPN architecture, but they also engage in customer routing. In other words, at Layer 3, the service provider routers communicate directly with the consumer routers. As a result, the customer and the service provider router have only one routing protocol neighborship or adjacency. Figure 1.2 below shows the concept of the peer-to-peer VPN model [3].

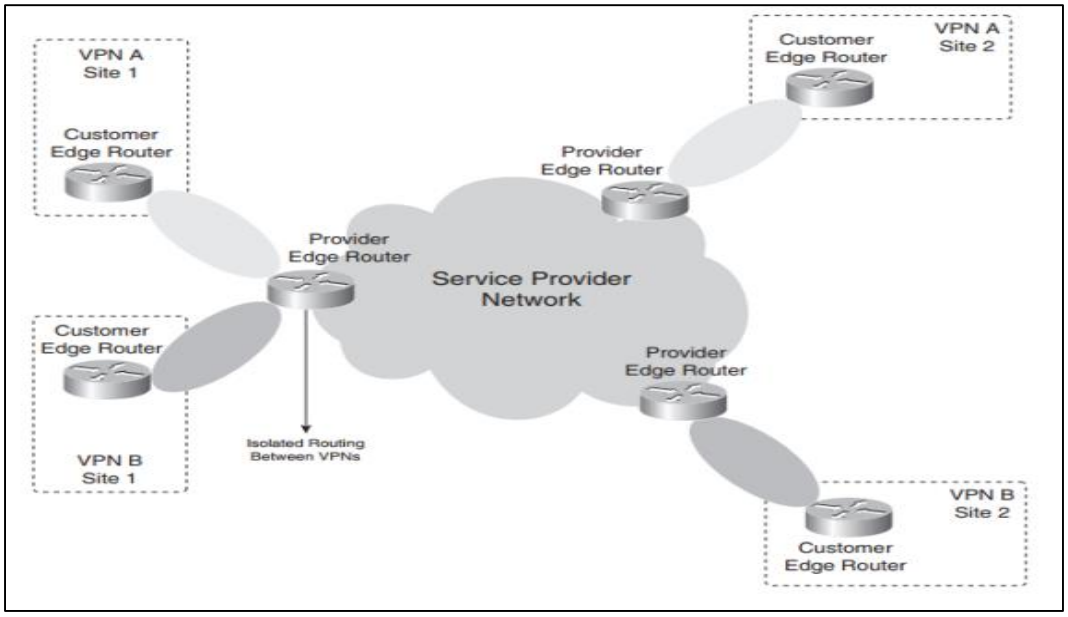


Figure 1.2: Peer-to-Peer VPN Model.

I.3.4 Traffic engineering

Traffic engineering is important for service providers to use the backbone efficiently and provide high flexibility, it's a method of optimizing the performance of network infrastructure, including unused links, as they are not located on the preferred path. This means that traffic engineering must provide the possibility to route traffic across the network on different paths from the preferred path, which is the least expensive path provided by IP routing. The least expensive path is the shortest path as calculated by the Dynamic Routing Protocol. With the implementation of traffic engineering in the MPLS network, you can have traffic destined for a certain prefix or with a particular quality of service flow from point A to point B along a different route than the less expensive one. The result is that the traffic can be spread more evenly over the available links in the network and make more use of unused links in the network. Figure 1.3 shows an example of this [4].

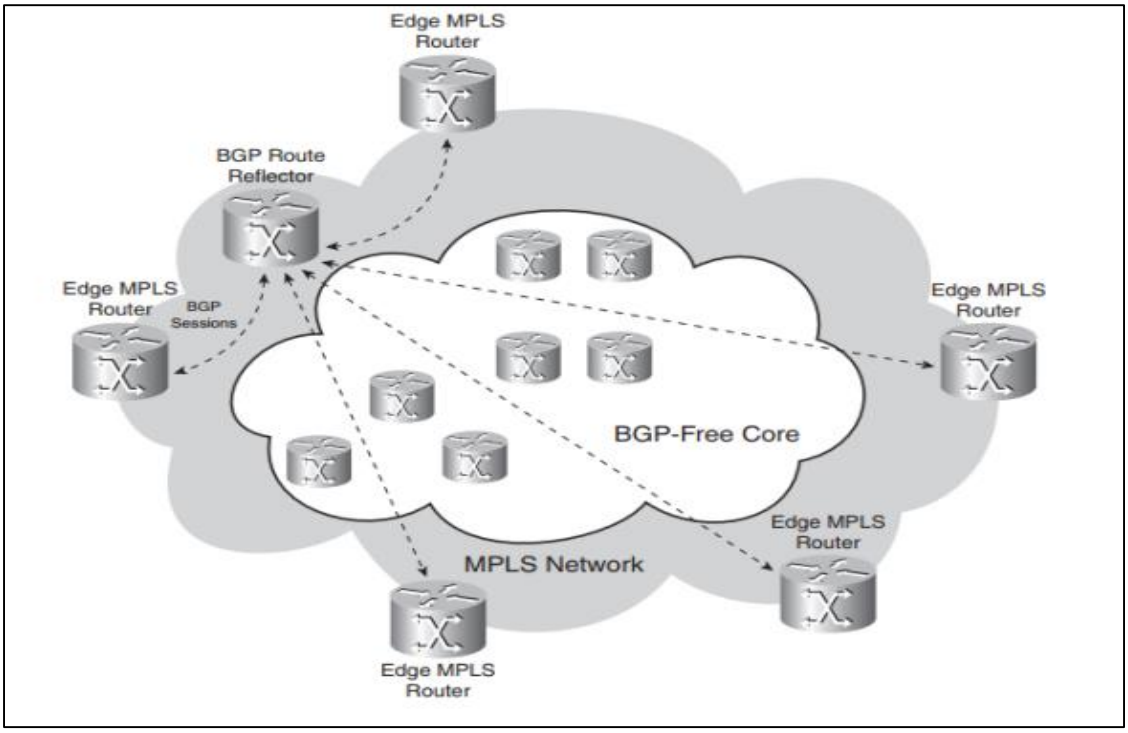


Figure 1.3: Traffic Engineering Example.

I.4 MPLS Labels and Label Stacking

I.4.1 MPLS Labels

One MPLS label is a field of 32 bits composed of four fields, the Label, EXP, BoS and the TTL as the figure below shows:

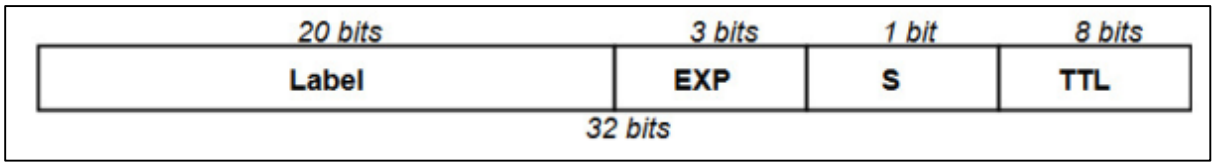


Figure 1.4: Syntax of One MPLS Label.

The label value is the first 20 bits. This number can range from 0 to 220–1, or 1,048,575. The first 16 values, on the other hand, are exempt from typical use; they have a specific significance.

The three experimental (EXP) bits are bits 20 to 22. These bits are used to indicate the quality of service. The bit 23 is the Bottom of Stack (BoS) bit. It is a one-bit flag, when set to 1, it means that the header directly precedes the IP header while the rest are set to zero. The stack is the

collection of labels that are found on top of the packet. The stack can consist of just one label, or it might have more. The number of labels (that is, the 32-bit field) that you can find in the stack is limitless, although you should seldom see a stack that consists of four or more labels.

Bits 24 to 31 are the eight bits used for Time to Live (TTL). serves as the number of hops left for the packet before it is discarded by the router, with a maximum of 256 hops.

When an unlabeled packet enters an MPLS network, the LSR pushes a label and copies the IP TTL to the MPLS TTL field, then it will be decreased as it goes through the MPLS network while the IP TTL will stay intact, once the last label is popped the egress LSR copies the MPLS TTL value to the IP TTL field [5].

I.4.2 MPLS Stacking

MPLS applications require several labels per packet, which is accomplished by stacking MPLS headers on top of one another. The top label in the stack is referred to as the top label, while the bottom label is referred to as the bottom label. In between, we can have any number of labels. Figure 1.5 shows the structure of the label stack.

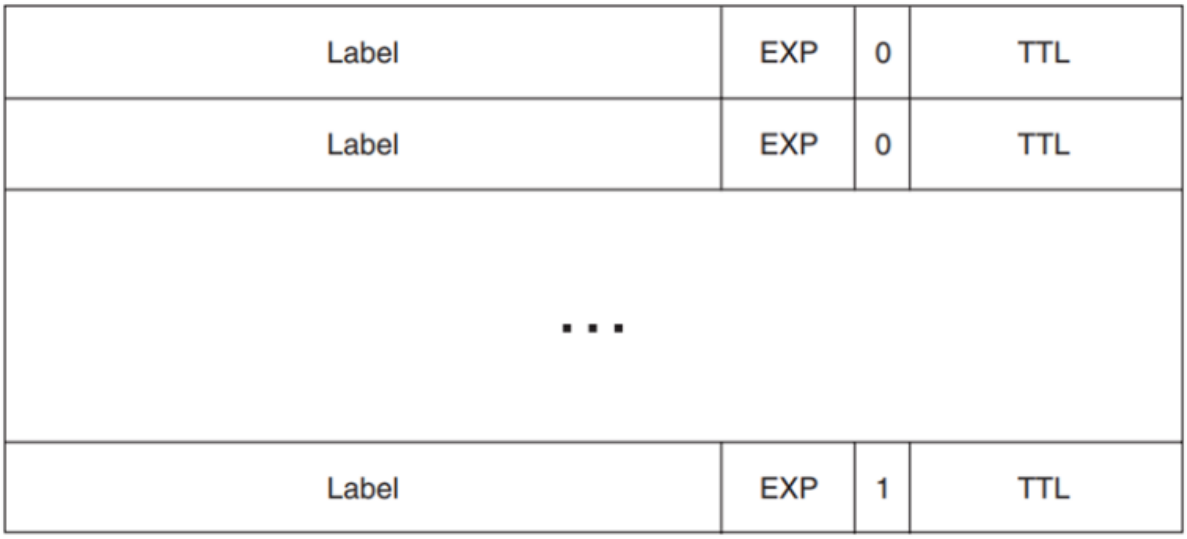


Figure 1.5: Label stack.

The label stack in Figure 1.5 shows that the BoS bit is 0 for all the labels, except the bottom label, the BoS bit is set to 1. Some MPLS applications actually need more than one label in the label

stack to forward the labeled packets. Two examples of such MPLS applications are MPLS VPN and AToM. Both of them put two labels in the label stack [5].

I.5 Label Distribution Protocol

In order for IP routing to work, we need a control plane protocol to populate the routing table and allow the packets to be forwarded, which is one of the Interior Gateway Protocols (IGP) or Border Gateway Protocol (BGP), however, in MPLS, we need an IGP and another control plane protocol in order to populate the Label Forwarding Info Base (LFIB) which is the Label Distribution Protocol (LDP). Before exchanging label information, LDP builds a neighbor adjacency, just like most other protocols. It differs from most protocols in that it functions in a unique way.

The following section demonstrates the operation of MPLS unicast IP forwarding: To start, we broadcast UDP multicast hello packets to see who else is around. When two routers decide to become neighbors, they establish a TCP connection to establish the neighbor adjacency. The exchange of label information takes place across this link. Normally a loopback interface is used for the neighbor adjacency. Here's an example: The two routers above will send multicast hello packets on their FastEthernet interfaces.

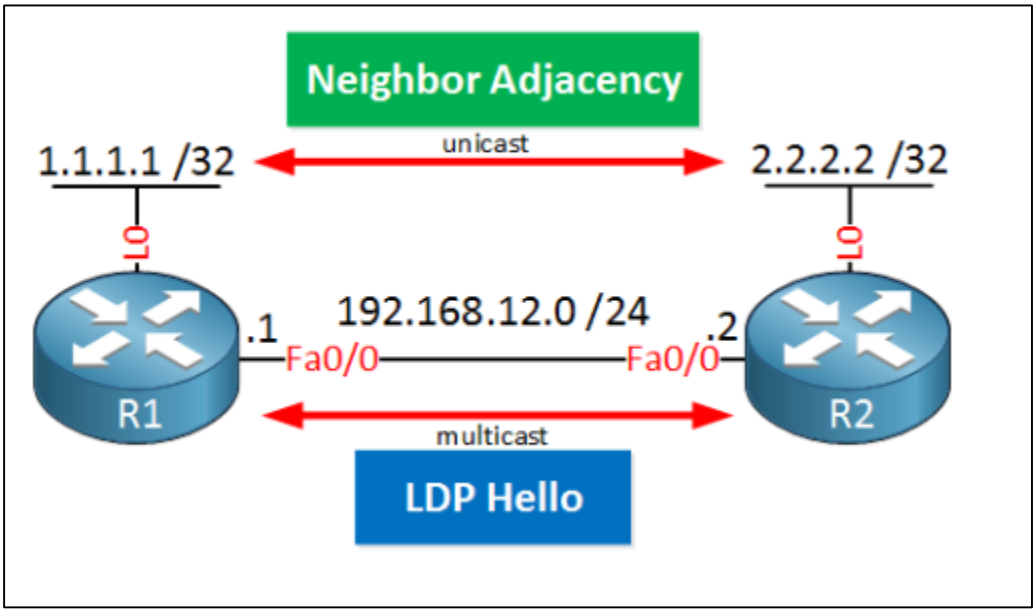


Figure 1.6: LDP.

In this hello packet, they will advertise a transport IP address. This IP address is then used to establish a TCP connection between the two routers. This is how the hello packet appears in Wireshark: We can see a handful of intriguing features in the image above:

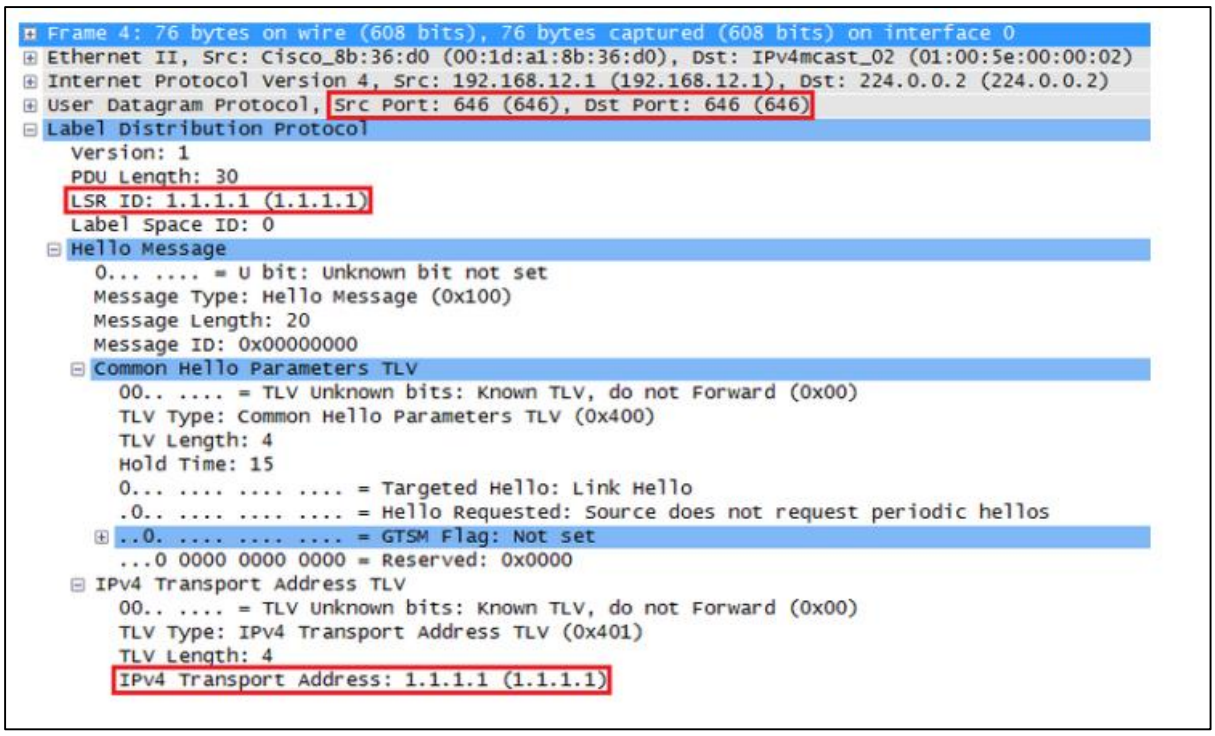


Figure 1.7: Wireshark LDP capture.

- Using source/destination UDP port 646, hello packets are broadcast to multicast address 224.0.0.2.
- Each router's LSR (Label Switch Router) ID is a unique identifier. On a loopback interface, it will choose the highest IP address by default, similar to how most protocols determine an ID. If we don't have any loopback interfaces, we'll use the highest IP address on a physical interface.
- The transportation address can be found at the bottom of the page. This is what we utilize to create the TCP connection itself. The router chose the IP address on the loopback interface as the transport address, just like the LSR ID. [6]**.**

I.6 MPLS Architecture

The MPLS Architecture is divided between the Control Plane and the Data Plane.

I.6.1 Control

The MPLS control plane specifies how updates are delivered from one PE router to each PE router, and it's in charge of constructing the FIB table using information from the Routing Information Base (LFIB), which is based on the label exchange protocol. The Control plane uses a label exchange protocol to create and manage labels internally, as well as to exchange labels with other MPLS equipped routers. Labels are linked to networks learned through a routing protocol through the labeling protocol exchange. MPLS Label Distribution Protocol (LDP), as well as Cisco's earlier Tag Distribution Protocol, are examples of label exchange protocols (TDP).

- TDP is a Cisco proprietary technology for attaching tags (also known as MPLS labels) to routing table network routes.
- LDP is the IETF version of Cisco's TDP. Labels are bound to network routes via LDP. The label information base (LIB) is a database that contains a mapping of incoming labels to outbound labels, as well as information on outbound interfaces and links. [7].

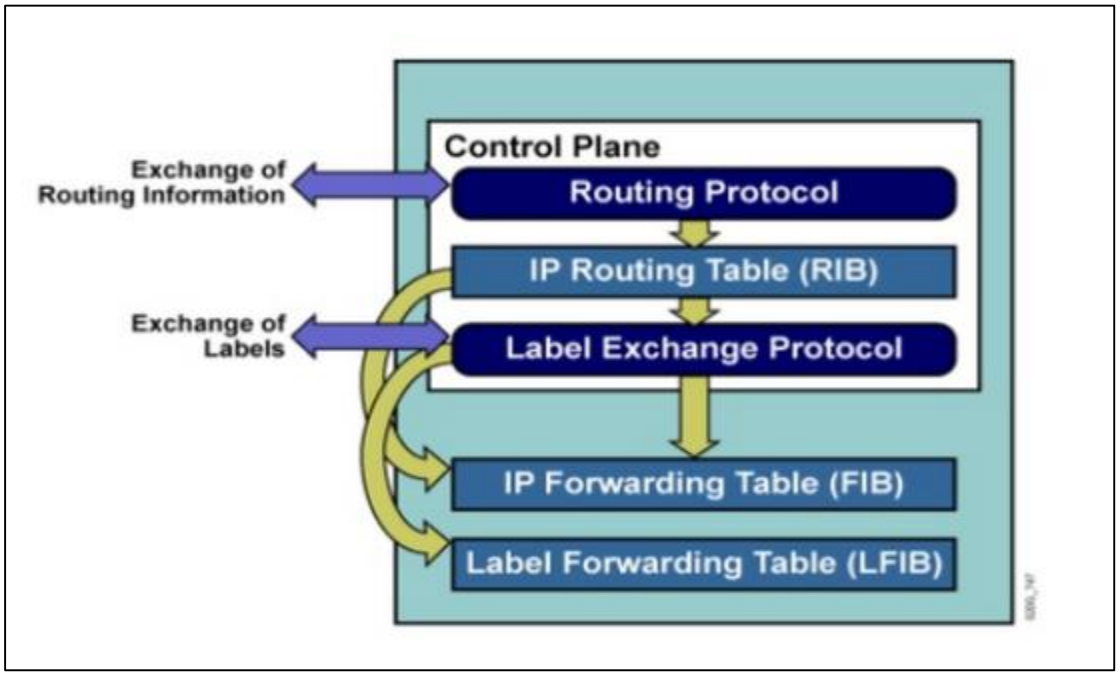


Figure 1.8: Control plane.

I.6.2 Forwarding

The information created by the control plane is used and retained in the forwarding component of the MPLS architecture. Simply said, it explains how data will be transferred from one PE router to the next. The routing table is created in the control plane and cached in the forwarding plane briefly. The LIB is built in the control plane for labels, and only those labels that are currently in use are stored in the label forwarding information base (LFIB). The Label Information Based table is a subset of the Label Information Based table (LIB). The forwarding information base is an additional device in the forwarding plane (FIB). Cisco Express Forwarding creates the FIB (CEF). The FIB is a cached version of the IP routing table that does away with the need for a route cache, the CEF must be enabled, so MPLS or tag switching can operate [7].

I.7 Conclusion

In this chapter, we have seen how MPLS functions, the MPLS encapsulation, how label forwarding protocol LDP functions and how MPLS logic could be used to introduce different applications.

II.1 Introduction

As mentioned in the first section, the introduction of Multiprotocol Label Switching (MPLS), which combines the benefits of Layer 2 switching with Layer 3 routing and switching, has made it possible to develop a technology that combines the advantages of an overlay VPN (such as security and isolation between clients) with the advantages of simplified routing that allows for peer-to-peer VPN implementation. The new MPLS/VPN technology allows for easier customer routing and service provider provisioning, as well as various topologies that are difficult to implement in either peer-to-peer or overlay VPN models.

II.2 Virtual Privet Network

If we break down the term virtual private network into its constituent parts, we may say that a network allows two devices to communicate. Local area networks (LANs) or wide area networks (WANs) could be those two devices (WAN). In any case, a network provides the essential link between the two. A logical link between two devices is referred to as "virtual" in a VPN. For example, one user could be connected to the Internet in New York and another in Paris, and we could utilize the Internet to construct a logical or virtual network between the two machines [8].

A virtual private network (VPN) is a generic word for a communication network that employs a variety of ways to protect a tunnel connection over an unsecured or untrusted network. Rather than having a dedicated connection, such as a leased line, you can use a shared connection, a "virtual" connection between geographically dispersed users and networks are made over a shared or public network, like the Internet. The data is transmitted as if it passes through private connections.

II.3 Types of VPN

Remote-access and site-to-site VPNs are the two major categories into which VPNs can be classified. The following are the specifics for each, as well as when they might be used:

II.3.1 Remote-access VPNs

Remote-access VPNs: Some users may need to establish a VPN connection between their personal computer and the company's headquarters (or to the destination they want to connect to). This is a VPN connection for remote access. For their VPNs, remote-access VPNs can leverage or

technologies.

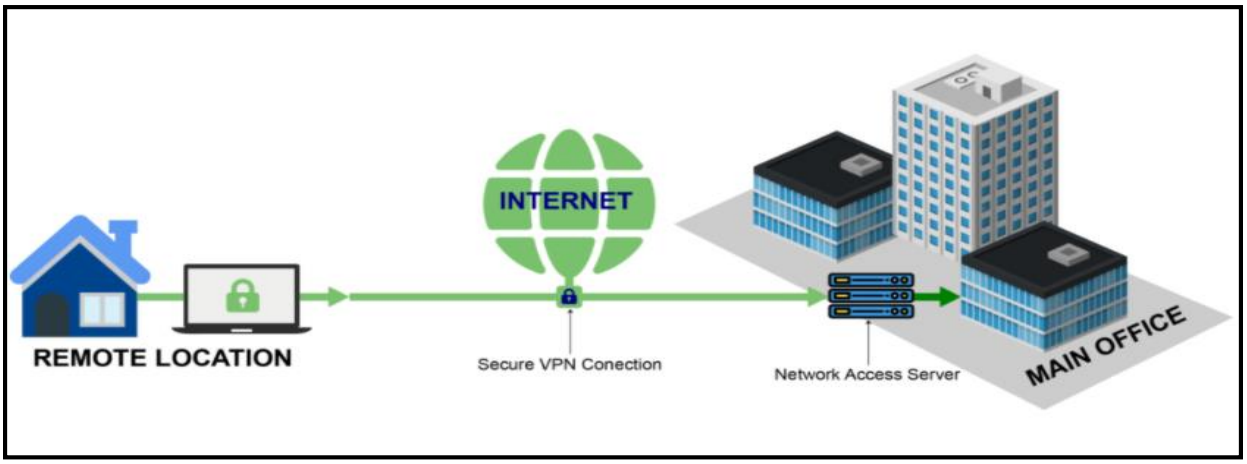


Figure 2.9: Remote-access VPNs

II.3.2 Site-to-site VPNs

The other major VPN is used by businesses with two or more sites who want to securely connect (most likely over the Internet) so that each site may communicate with the others. A site-to-site VPN is the name for this configuration. Site-to-site VPNs have typically relied on a collection of VPN technologies known as IPsec.

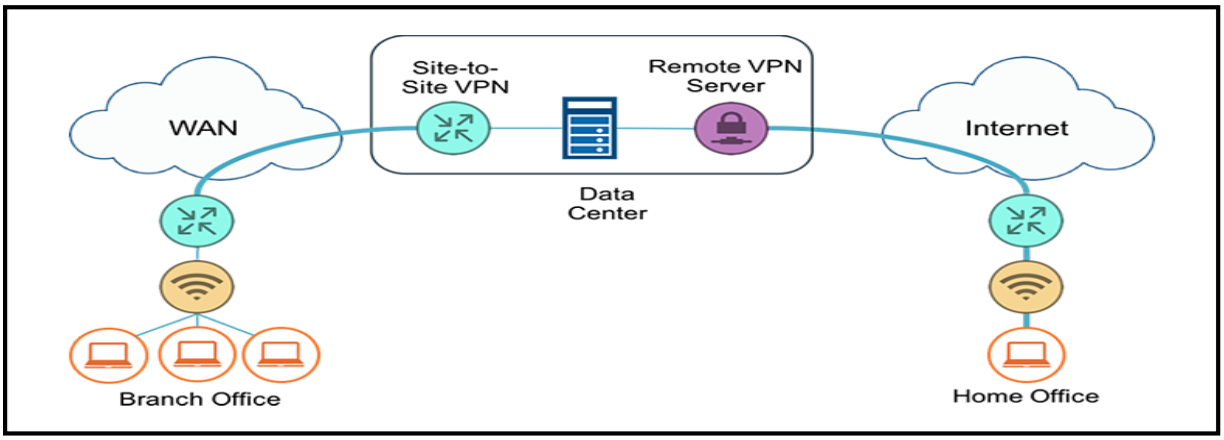


Figure 2.10: Site-to-site VPNs

II.4 MPLS Layer 3 VPNs

MPLS virtual private networks are the most prevalent MPLS applications (VPNs). Layer 3 VPN services can be provided by a service provider or even a major corporation using MPLS VPNs. ISPs frequently use an MPLS VPN service to replace outdated Layer 2 WAN services like Frame Relay and ATM. MPLS VPNs allow the ISP to provide a wide range of additional services to its customers because they are aware of the Layer 3 addresses at the client locations. Layer 2 WAN services can also give the same level of anonymity as MPLS VPNs.

II.4.1 Layer 3 VPN Control Plane

In L3 VPN Networks, the Control Plane is defined as the time when routing exchange actions are carried out. These are the L3 VPN routers' required routing information exchanges. Starting with a CE device, PE devices continue the exchange with other PEs until it returns to the CE device at the other end. CE, as previously indicated, uses a routing mechanism on its internal network. As a result, there are internal pathways. With PE devices, CE employs a different or the same routing protocol. If CE and PE employ distinct protocols, then redistribution is required. CE delivers the routers to the PE using this routing technique, also known as redistribution. The PE router receives routes from the CE router and allocates them. The VPNv4 route is then redistributed into MP-BGP. Route Distinguisher is used to isolate distinct consumer pathways during this operation. As a result, distinct customer routes can safely travel through the Service Provider's IP/MPLS network. The L3 VPN service is sent to the destination at the receiving PE device, according to Route Targets.

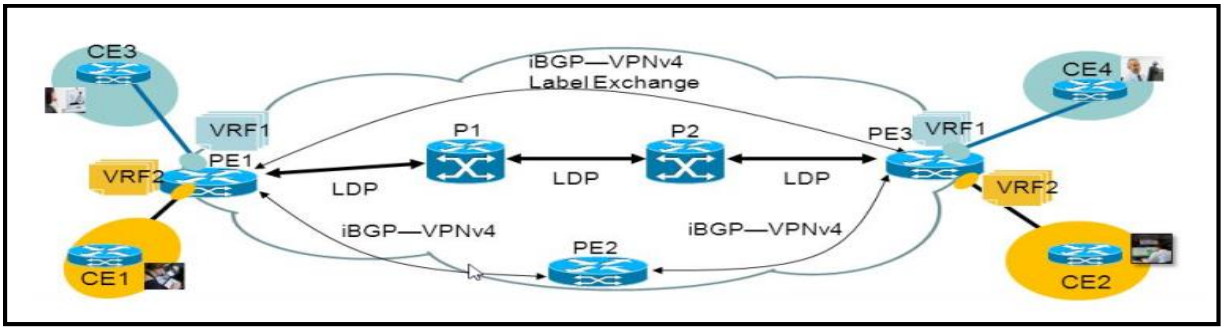


Figure 2.11: MPLS VPN Control plane

II.4.2 MP-BGP (Multi-Protocol BGP)

L3-VPN A PE device's VRF routes must be shared with the other PE devices running this L3 VPN Service. A special protocol is used to do this. MP-BGP is the name of the protocol (Multi-Protocol BGP). MP-BGP is a BGP variant that supports multiple address types. In these networks, several clients can utilize the same private blocks, but these private blocks must not be combined during transportation. To distinguish between distinct customer routes, we must use a new address format and update their prefixes. VPNv4 Addresses are created by appending a 64-bit long Route Distinguisher to the beginning of the customer's IPv4 addresses. Below, we'll go over the specifics of this address type. Between the PE devices a BGP session is established. This BGP session transports all of the information from the various L3 VPN customers. Consider that for a moment. If the L3 VPN does not use MP-BGP. What is the status of routes with the same prefixes for many customers? Simply put, several routes for the same prefixes would exist in the BGP routing tables. As a result, one of them would choose, and the data would be sent through. But these are different customer’s route? Is it enough sending only the best route and only one customer route to its destination? Certainly not. This is not a healthy and acceptable scenario [9].

To achieve this, three important instances has been introduced:

- Virtual Routing Forwarding (VRFs).
- Route Distinguishers (RDs).
- Route Targets (RTs).

II.4.2.1 Virtual Routing Forwarding (VRF)

We use VRFs to support multiple customers with overlapping address schemes. VRFs are virtual routers that only exist in MPLS aware routers and are typically enabled on PE routers. They allow us to store routes separately for each customer, preventing interference between customers' overlapping addresses [10]. A router typically requires a VRF for each client connected to the PE in question, which can be used to divide traffic between sites belonging to the same customer, where different VRFs can be utilized for the same customer [11].

The following figure puts the VRF concept more in-depth:

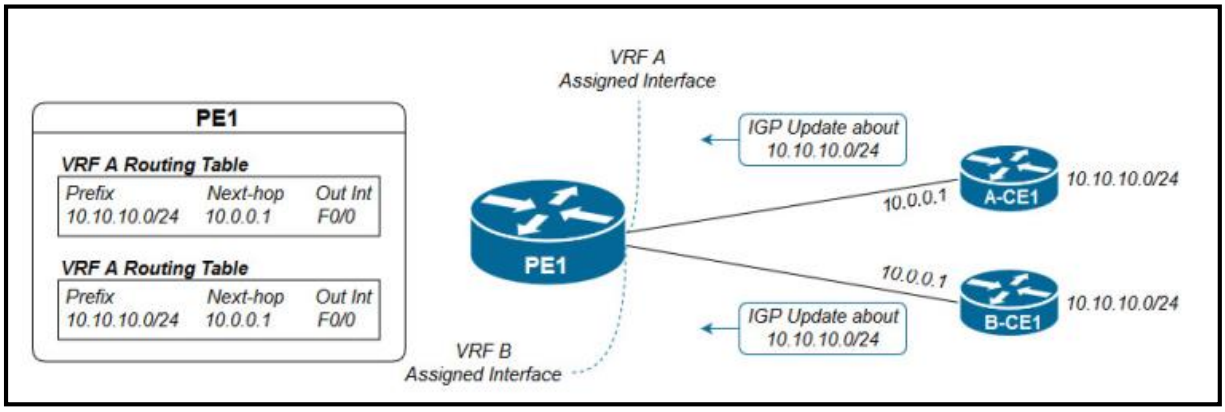


Figure 2.12: VRF Process

We can break this process to these two steps:

1. A-CE1 and B-CE1 send IGP updates to PE1 about the 10.10.10.0/24 subnet.

2. PE1 receives an IGP update about 10.10.10.0/24 on its VRF-A assigned interface, so it places it in the VRF-A routing table.

PE1 receives an IGP update about 10.10.10.0/24 on its VRF-B assigned interface, so it places it on the VRF-B routing table.

VRFs, being virtual routers, have these major instances as well:

- Routing Information Base (RIB).
- Forwarding Information Base (FIB).
- A separate instance or process of the IGP used to exchange routes with the CEs.

II.4.2.2 Route Distinguisher (RD)

While VRFs can be used to store routes on PEs independently, they can't be used to advertise routes between customers' sites separately, which is why the BGP update included an extra "number" before the network layer reachability information (NLRI) prefix, that was destined to make each route unique to a customer by assigning a unique number for each customer, all thanks to the MPBGP RFC 4760 that allows the redefinition of an additional number, conventionally called an Address Family to be added before the NLRI prefix, in order to support the MPLS VPN, namely, the Route Distinguisher (RD) [8].

Network Layer Reachability Information (NLRI) is exchanged between BGP routers using UPDATE messages. An NLRI is composed of a LENGTH and a PREFIX. The length is a network mask in CIDR notation (e.g. /25) specifying the number of network bits, and the prefix is the Network address for that subnet (10).

Route distinguishers, which are an MPBGP address family (VPNv4), are used to distinguish between duplicate addresses while advertising for them with MPBGP by adding them before the prefix in the NLRI which will make them unique, since every customer has his own RD, as a result the NLRI will become a 96 bits address composed of:

- A 64-bit Route distinguisher.
- A 32-bit IPv4 Address.

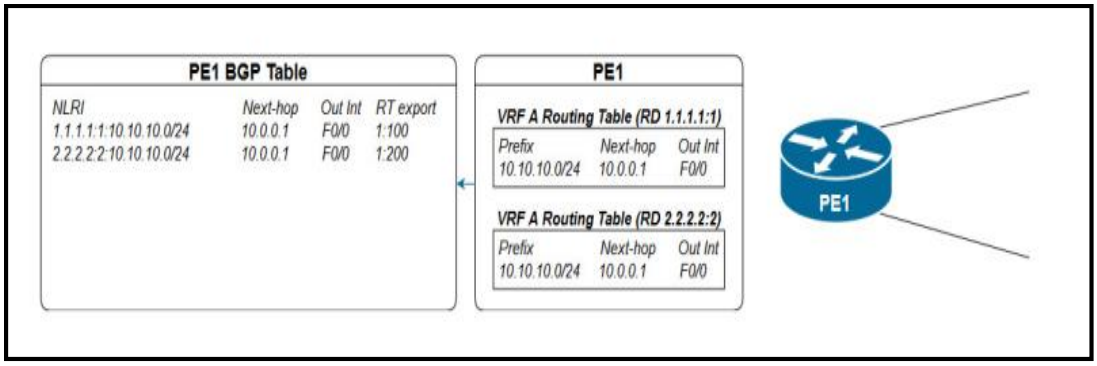


Figure 2.13: IGP to BGP VPNv4 Routes Exportation.

What happens is that the PE router redistributes the routes found in the VRFs learned by OSPF into BGP, resulting in extracting an RD from each VRF, and store them in its BGP table so it can advertise them to the other Pes, and since the BGP table has all redistributed routes, the appended RD value will make storing duplicate addresses possible.

RD is eight bytes long, while the first two bytes are reserved for the type, we can configure the rest of the six bytes under three formats:

- 4 bytes integer :2 bytes integer.
- 2 bytes integer : 4 bytes integer.
- 4 bytes in DDN: 2 bytes integer.

We must note that the first half of the RD has to be either an ASN number or an IPv4 address.

Route Distinguishers Usage in an MPLS VPN

- ✓ The RD has no special meaning.
- ✓ Used only to make potentially overlapping IPv4addresses globally unique.
- ✓ The RD could be used as a VPN identification; however, this architecture would not be able to handle all topologies that customers demand. [13].

II.4.2.3 Route Target (RT)

We have seen how MPLS VPN solved the duplicate addressing scheme, throughRDs and VRFs respectively, the only remaining problem, is how do egress PEs know in which VRFs should they place the advertisements?

Route Targets (RT), MPLS uses RTs to determine in which VRF the advertisements should be placed, RTs are also a redefinition of a BGP advertisement update field, called the extended community, an 8-byte field, while advertisements are bound to only one RD, they can be marked by several RT values, we can discern two types of RTs [10]:

- Export RT: Configured on the ingress PE
- Import RT: Configured on the egress PE.

When the advertisement arrives, the egress PE runs the export RTs against its import RTs and places the information into the respective VRF when a match occurs, as the following figure shows:

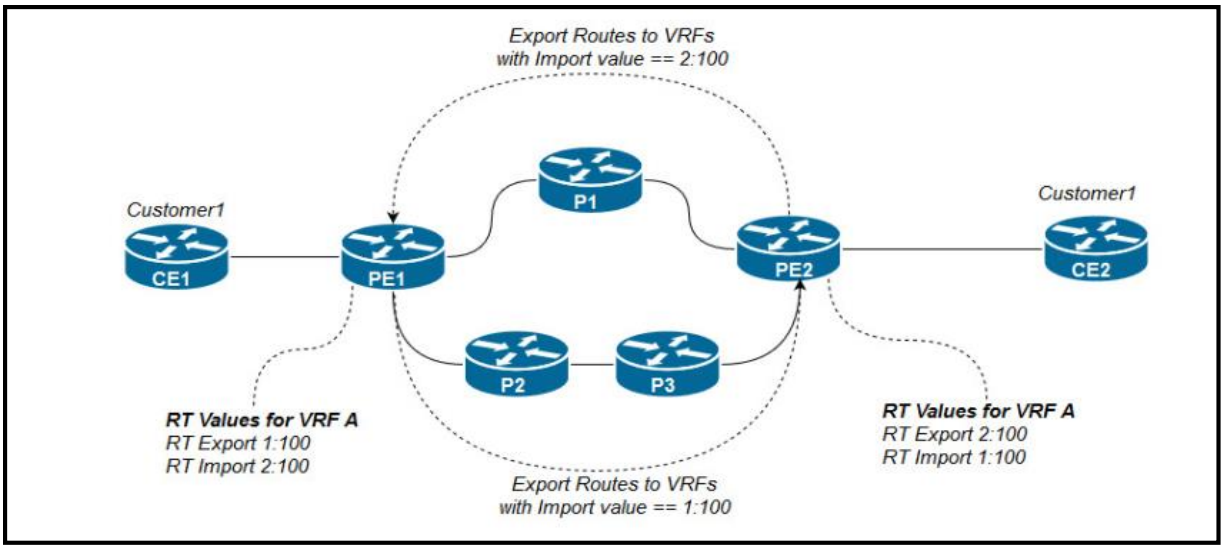


Figure 2.14: Routes Exportation and Importation.

It is important to note that this process is unidirectional, if the egress PE in this case, advertises routes from the CEs connected to it, it should have its own Export RT and the ingress PE should have its own Import RT.

II.4.3 Layer 3 VPN Data plane

MPLS VPN need more than one MPLS label on a particular IP packet. The concept of the MPLS label stack is not only how the router forwards VRF traffic across a global interface, but it also lets the receiving router know which VRF the traffic is destined for. So it's need two labels:

1. **Transport Label :**
   - ✓ Generated by LDP across an MPLS backbone.
   - ✓ Outermost label or top of label stack.
   - ✓ Used to forward traffic between PE routers.
2. **MPLS Label:**
   - ✓ Generated by BGP.
   - ✓ Innermost label, or bottom of stack.
   - ✓ Used to get traffic into the appropriate VRF.

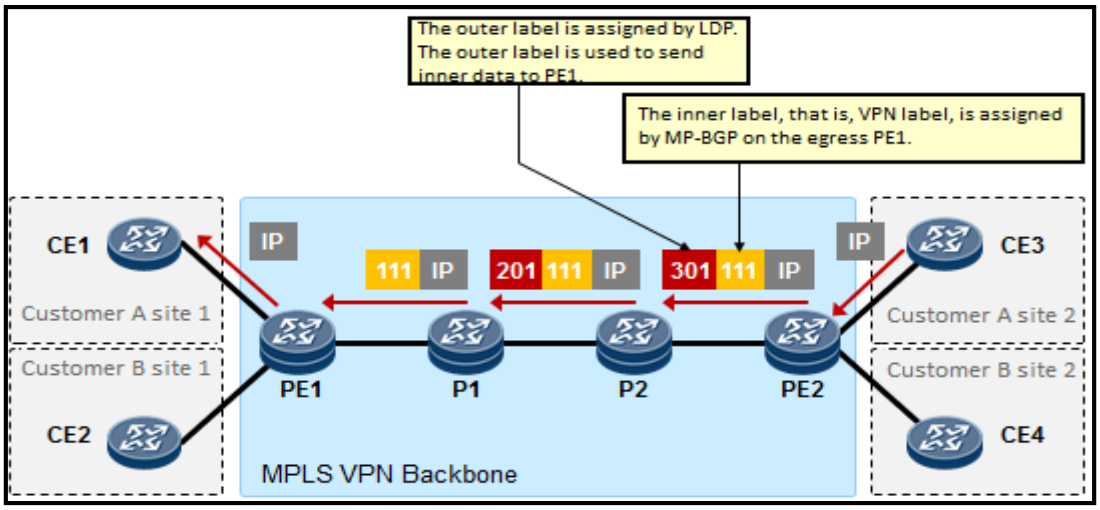


Figure 2.15: Data Forwarding Plan.

II.5 MPLS Layer two VPNs

Layer2 and Layer3 VPNs are available over the existing MPLS network. In a layer2 VPN, L2 frames (which might be Ethernet, ATM, Frame Relay, or PPP/HDLC) are transferred between locations. In a broader sense, it's akin to a virtual wire that connects two switches in different buildings. All layer 2 properties, such as learning MAC addresses (ARP Protocol), replicating broadcast and multicast packets, and so on, must be handled by the VPN. Tunneling frames across the VPN is a simple way to accomplish this. L2 VPNs that are tunneled are conceptually simpler than L3 VPNs, and they can be fully transparent to applications if properly built. On the other hand, it could be affected by all of the difficulties that face normal L2 extensions, such as security concerns and L2 instabilities. As previously illustrated, each side of the connection is on a different subnet in a layer 3 VPN, and IP packets are routed through the VPN. VPNs at the L3 level, on the other hand, rarely give the same level of transparency as L2 VPNs, and may conflict with apps for various reasons [10].

II. 6 Conclusion

The MPLS VPN network is the most widely used MPLS-enabled application in operations. This chapter discuss the different operation of MPLS VPN both in control plane in forwarding plan, explain different protocols applied and the label forwarding mechanism

III.1 Introduction

Quality of service (QoS) has become popular in the past few years. Because few networks have unlimited bandwidth, network congestion is always a possibility. QoS is a method of prioritizing and ensuring the delivery of vital traffic over less important traffic.

The objective of this chapter is to define the different types of quality of service (QoS) required by organizations for typical virtual private network (VPN) deployments, as well as the options and technological implementations for each.

III.2 QoS Overview

QoS is a technique that assigns various priorities to different types of traffic in order to reduce latency and packet loss. When the network is crowded, QoS can ensure the normal transmission of vital business traffic. Without QoS, datagrams are served in a network based on a first-in, first-out (FIFO) basis, also referred to as best-effort service. In such scenarios, datagrams do not take precedence, depending on the type of application they support. As a result, differential treatment for different types of application traffic is not possible. Therefore, service level agreements for any service other than best-effort service cannot be met. QoS allows the service provider to use network infrastructure to provide several application services, thereby saving the capital and operating costs involved in maintaining multiple networks for each application separately. Although network traffic flows are dynamic, QoS allows the service provider to maximize network resource utilization, by increasing its benefits. Quality of service maximizes the use of network resources and optimizes revenue generation by providing priority access to network bandwidth for high-priority traffic, and allowing low-priority traffic to obtain the bandwidth dedicated to high-priority traffic in the absence of high-priority traffic. [14].

III.3 Characteristics of network traffic

There are four features of network traffic:

- Bandwidth.
- Delay

- Jitter.
- Loss.

III.3.1 Bandwidth

Bandwidth is the capacity available on the link, (in bits per second). By using QoS, the router can be informed on how to use and exploit this bandwidth. With FIFO, packets are served on a first-in, first-out basis. Among the things we can do using QoS is create different queues and place some types of traffic on different queues. The router can then be configured so that the first queue gets 50% of the bandwidth, the second queue gets 20% of the bandwidth, and the last queue gets the remaining 30% of the bandwidth.

III.3.2 Delay

Delay is another parameter of QoS that comes before jitter and packet loss, is the time required to forward a packet from the source to a destination, this is called the one-way delay, and the time it takes to move from source to destination and back is called the round-trip delay. (For example, sending VOIP to the beginning of the queue), there are different types of delay:

- **Processing delay** It's the time required for the device to perform all the tasks necessary for the transmission of the packet.
- **Queuing delay:** is the amount of time that a packet is waiting in a queue. When an interface is congested, the packet will have to wait in the queue before it is transmitted.
- **Serialization delay:** is the time required to send all bits of a frame to the physical interface for transmission.
- **Propagation delay:** the time it takes for bits to cross a physical medium.

III.3.3 Jitter

Jitter is the variation in latency for a stream of packets. For example, an IP phone sends a constant flow of voice packets. Due to network congestion, some packets are delayed. The delay between packets 1 and 2 is 25 ms, the delay between packets 2 and 3 is 35 ms, the delay between packets 3 and 4 is 6 ms, etc. The receiver of these voice packets must handle the jitter, making sure the packets have a steady delay or you will have a poor voice quality.

III.3.4 Loss

Loss (Dropping less priority traffic if we have to) is the amount of lost data, usually expressed as a percentage of lost packets sent. For example, when there is congestion, packets will be queued but once the queue is full, the packets will be dropped. With QoS, we can at least decide which packets get dropped when this happens [15].

III.4 QoS Models

There are three different QoS implementation models:

III.4.1 Best effort

The best-effort model is relatively simple to understand as there is no prioritization and all traffic is treated the same regardless of its type, is the default mode for all traffic, it uses first-in, first-out (FIFO) queues, which simply transmit packets as they arrive in a queue without treatment. QoS is not enabled for this model.

III.4.2 Integrated Services (IntServ)

The IntServ model also known as hard QoS, was created for real-time applications such as voice and video that require bandwidth, delay, and packet-loss guarantees to ensure both predictable and guaranteed service levels. In this model, applications report their requirements to the network to reserve the end-to-end resources (like a bandwidth) they need to provide an acceptable user experience. The integrated services model uses RSVP for reserving bandwidth and resources across a network. RSVP stands for resource reservation protocol, is a resource reservation used for reserving bandwidth, and QoS tools for a particular flow. Here is a limitation of the intserv model if reserved no other traffic can use it and it is no scalable each flow required a separate admin configuration on the router.

III.4.3 Differentiated Services (DiffServ)

The DiffServ model is also known as soft QoS, is designed to overcome the limitation of best-effort and intserv models. With this model, there is no need for a signaling protocol, and there is no RSVP flow state to maintain on every single node, which makes it highly scalable; The DiffServ model is also called as soft QoS, is a technique for implementing QoS policies designed to

overcome the limitation of best-effort and intserv models. QoS features (such as bandwidth and delay) are managed on a hop-by-hop basis with QoS policies that are defined independently at each device in the network. The network traffic is defined in the diffserve model by categories and the QoS policy of the network imposes a different treatment of traffic categories (classes). Many levels of service can be selected with DiffServ. For example, voice traffic is very sensitive to latency and jitter, so it must always benefit from a specific preferential treatment over all other application traffic. On the other hand, e-mail can afford a great deal of delay and could be given best-effort service and non-business, non-critical scavenger traffic (such as from YouTube) can either be heavily rate-limited or blocked entirely. The Differentiated Services model is the most popular deployed QoS model [16].

III.5 QoS Mechanism

III.5.1 Classification and Marking

Before a QoS mechanism can be applied, IP Traffic must first be divided into classes, based on business requirements. Each class of traffic will receive the same type of QOS treatment. Network devices use classification to identify IP traffic as belonging to a particular category. After the IP traffic is classified, marking can be used to mark individual packets so that other network devices can apply QoS mechanisms to those packets as they traverse the network.

III.5.1.1 Classification

The classification is a QoS mechanism responsible for Classifying network traffic and distinguishing between different traffic streams. It uses traffic descriptors to classify an IP packet within a specific class. The classification of IP packets must take place at the perimeter of the network, as close to the source of the traffic as possible. Once an IP packet is classified, then the packets can either be marked/re-marked, queued, policed, shaped or any combination of these actions. [16].

Most common ways of classifying traffic:

- Addressing (Based on port number or destination network)
- ACL
- MAC address

- Application signature (A certain size of the packet or the traffic body has a specific URL or certain range of port numbers).
- Markings (A downstream device has marked the traffic)
- L2 classification.
- L3 classification.
- NBAR (Network-Based Application Recognition).

III.5.1.2 Marking

The marking is a QoS mechanism types that distinguishes a packet from other packets during the implementation of other QoS methods by modifying a field over a packet or a frame header with a traffic descriptor (such as re-marking, policing, queuing, or congestion avoidance). Packets in the same class are annotated on egress to make upstream device classification easier.

For traffic marking, the following traffic descriptors are used:

- ✓ **Internal:** QoS groups;
- ✓ **Layer 2:** Class of Service (CoS) bits;
- ✓ **Layer 2.5:** MPLS Experimental (EXP) bits;
- ✓ **Layer 3:** Differentiated Services Code Points (DSCP) and IP Precedence (IPP) [16].

IP Precedence: Differentiated QoS

As shown in Figure below, IP precedence uses the three precedence bits in the IPv4 header's Type of Service (ToS) field to identify the class of service for each packet.

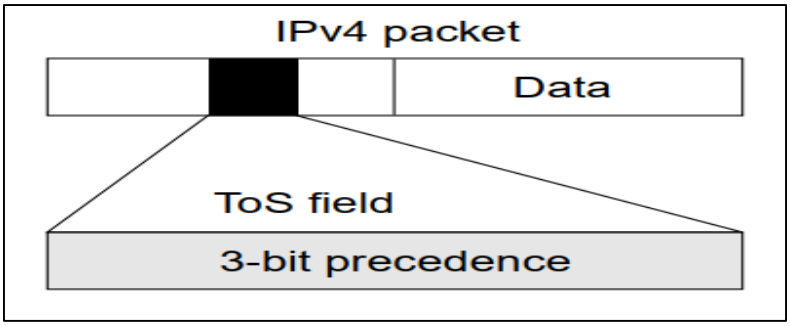


Figure 3.16: IPv4 Packet Type of Service Field.

Traffic can be separated into up to six classes, with network policies for congestion management and bandwidth allocation defined using policy maps and extended access lists for each class. The table below shows the numbers and their corresponding names, from the least to the most important [17].

Number	Name
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

Figure 3.17: IP Precedence Values.

The DS field (Differentiated Services) is the new term for the TOS byte, and the eight bits have also changed. Here's how it now appears:

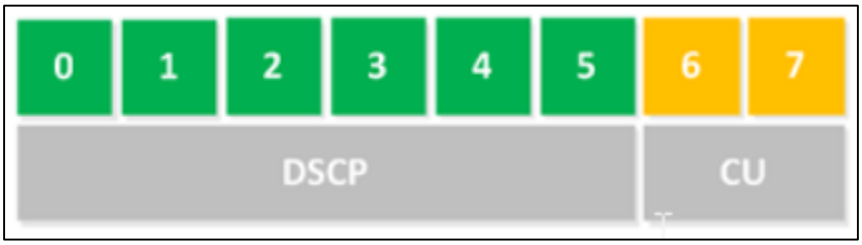


Figure 3.18: DiffServ with IP packets

III.5.2 Policing and Shaping

Traffic policers and shapers are QoS mechanisms used to classify traffic and limit traffic flow. They classify traffic in an identical way but differ in their implementation:

- **Policers:** the policing action is take a place at the provider-side, this action means that you Drop the exceeding ingress (coming) traffic or mark-down that traffic, to be dropped later in the network.

- **Shapers:** the shaping action is takes a place at the client-side to avoid misunderstanding or unwanted behavior with the provider, this action means that you store and delay peak traffic rates temporarily above the required rate until the egress traffic rate drops below the defined traffic rate. If the egress traffic rate is lower than the required rate, traffic is sent immediately Figure 3.4 illustrates the difference between traffic policing and shaping. Policers drop or re-mark excess traffic, while shapers buffer and delay excess traffic [16].

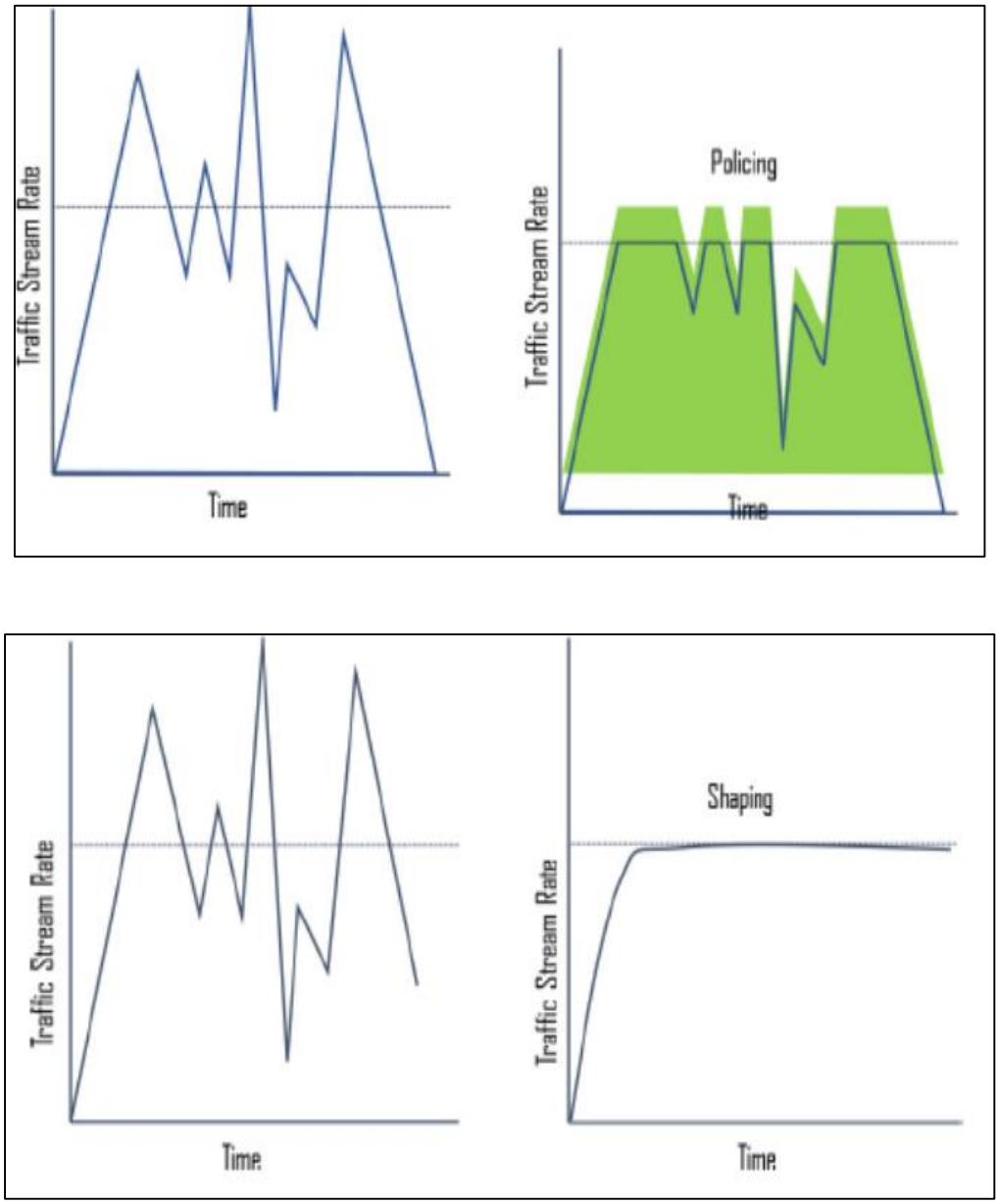


Figure 3.19: Policing Versus Shaping.

III.5.3 Congestion Management

Congestion management techniques provide some control of the order of transmission, and they are a set of QoS features that handle the queuing and scheduling of the traffic. Queuing (also called buffering in QoS) is the temporary storage of excess packets. By enabling queuing, the buffer is divided into blocks. For example, one of the data and another for voice.

Scheduling is to prioritize sending the data. For example, sending one packet from the first queue then sending two packets from the second queue. Or, sending all packets from the first queue then start sending packets from the second queue [18].

Congestion can occur for one of these two reasons:

- The input interface is faster than the output interface.
- The output interface is receiving packets from multiple input interfaces.

There are many queuing algorithms, but most of them are not suitable for modern multimedia networks that deliver high-definition voice and video traffic, as they were designed before these types of traffic appeared. Legacy queuing algorithms that precede the MQC architecture include the following:

- **First-in, first-out queuing (FIFO):** A single queue with packets sent in the exact order they arrived. (first come, first served). In FIFO queuing, all traffic belongs to the same class.
- **Priority queuing (PQ):** Using PQ, a set of four queues (high, medium, normal and low) are presented in strict priority order. One of the main obstacles is the possibility of starving low-priority traffic.
- **Custom queuing (CQ):** A round-robin scheduler is used to manage 16 queues. It assures bandwidth and prevents starvation, but does not provide the strict priority required by delay, and real-time flows
- **Weighted round robin:** WRR has been developed to provide priority-setting possibilities for round-robin. It allows weight to be assigned to each queue, and based on this weight, each queue effectively receives a portion of the bandwidth of the interface that is not necessarily equal to other queues portions.

- **Weighted fair queuing (WFQ):** The algorithm divides the interface's bandwidth by the number of flows (weighted by IP precedence, or IPP) ensuring an equitable distribution of bandwidth for all applications. This method provides better service for high-priority real-time flows, but lacks a bandwidth guarantee for any particular flow.

The recommended queuing algorithms include the following:

- **Class-based weighted fair queuing:** CBWFQ allows for the creation of up to 256 queues, each of which can serve up to 256 traffic classes. The amount of bandwidth allotted to each class dictates how each queue is handled. CBWFQ is a more advanced form of WFQ.
- **Low-latency queuing (LLQ):** This method is CBWFQ combined with priority queueing (PQ) and is therefore suitable for mixes of real-time and non-real-time traffic, like voice. Traffic assigned to the strict-priority queue is serviced up to its assigned bandwidth before other CBWFQ queues are serviced. [18].

III.6 MPLS VPN QoS

Because MPLS labels include three experimental bits that are often used for QoS marking, it is feasible to "tunnel DiffServ," that is, maintain Layer 3 DiffServ markings while re-marking (through MPLS EXP bits) within the cloud to signal in- and out-of-contract traffic. there are three distinct modes of MPLS DiffServ tunneling:

III.6.1 Uniform Mode

When a client and a service provider share the same DiffServ domain, such as when a business deploys its own MPLS VPN core, Uniform Mode is employed. The tunneled information must be used to produce LSP DiffServ information for the ingress LSR, and the egress LSP DiffServ information must be propagated to the Tunneled DiffServ information in the Uniform model. The QoS information is always present in the top label or in the IP header if the packet is not labeled. The MPLS does not affect QoS information but switches packets via the MPLS network. To change the EXP bits of the top label(s) we use the MQC, this only changes the outer QoS

information, or the LSP DiffServ information, and this change in the LSP DiffServ information is propagated on the egress LSR because the EXP bits are mapped to IP Precedence values. Figure 3.20 shows the behavior of Uniform Model [19].

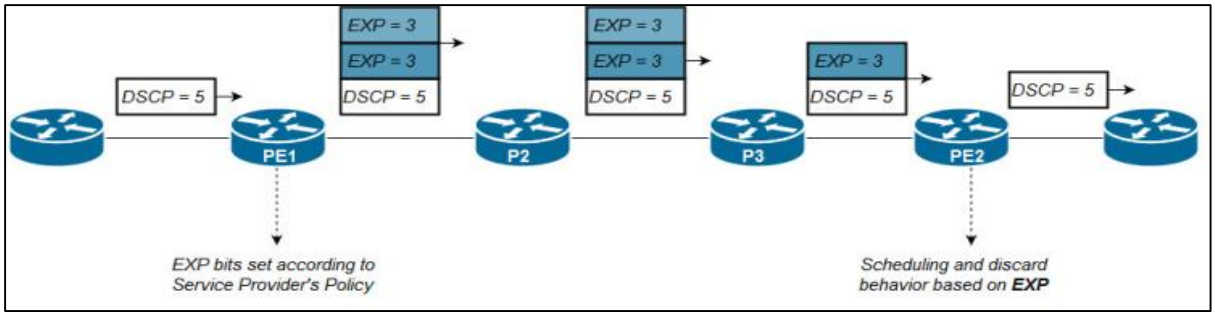


Figure 3.20: uniform model.

III.6.2 Pipe Mode

In the pipe mode the LSP DiffServ is not derived from the Tunneled DiffServ Information on the ingress LSR. on the egress LSR the forwarding treatment (classifying the packet for scheduling and discarding behavior at the output interface) of the packet is based on MPLS PHB (EXP bits), and the LSP DiffServ Information is not propagated to the tunneled DifferServ Information. Figure 3.21 illustrates the Pipe Mode MPLS DiffServ tunneling operation.

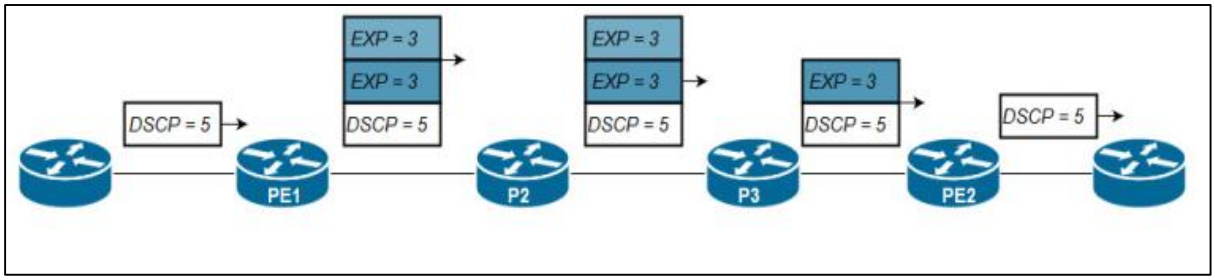


Figure 3.21: Pipe model.

Pipe Mode operation is identical to Short Pipe operation (as depicted in Figure 3.21), with the exception that the final PE egress queuing policies are based on the SP's marks (rather than the customer's) [19].

III.6.3 Short Pipe Mode

The Short Pipe model uses the same rules and techniques of the Pipe model across the core. The difference is that you classify recently exposed IP packets for outbound queuing at the egress PE router based on the IP PHB from the DSCP value of this IP packet. Figure 3.22 depicts the operation of MPLS DiffServ tunneling in Short Pipe Mode [19].

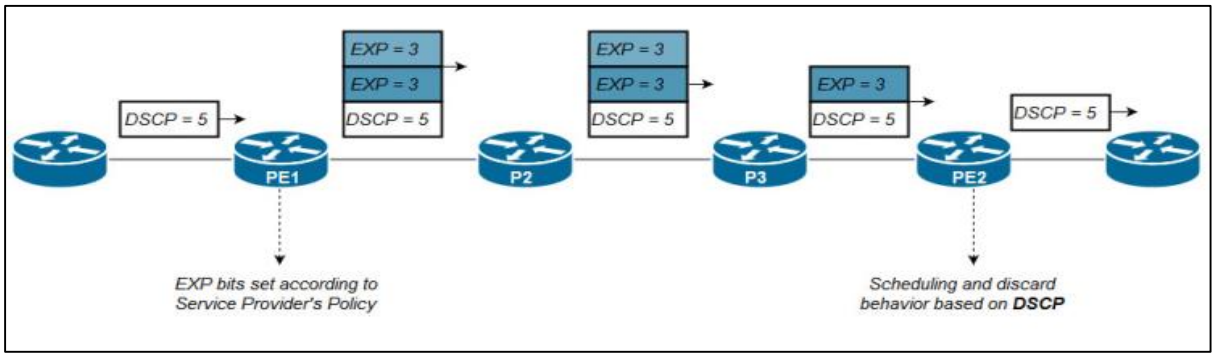


Figure 3.22: Short Pipe Model.

I.7 Conclusion

The usage of quality of service (QoS) has become widespread, in this chapter, we have seen that the MPLS network can use QoS on three MPLS DifferServ Models and the difference between the three models is only at the edge LSRs.

IV.1 Introduction

Nowadays, companies are using digital transformation more rapidly. work Remotely and video conferences are now standards. Many applications are moved either to the public cloud or private cloud and many services are now available over the Internet. Enterprises want to reduce costs and manage their infrastructure more effectively and easily. The classic wide-area network (WAN), on the other hand, was designed to connect users at remote locations to applications stored in the data center. To offer secure and dependable access to the Data Center, dedicated leased lines and MPLS were deployed.

This traditional WAN design does not work anymore in a digital transformation world where applications are moved out of the data center, and the users consuming those applications. As companies are rapidly adopting Software-as-a-service (SaaS) and Infrastructure-as-a-service (IaaS) models. Information Technologies realizes that the user experience of the application is poor. That's because WANs built for a particular purpose aren't equipped to handle the tremendous surge in WAN traffic that cloud adoption brings. That traffic results in management complexity, the unpredictability of application performance, and data vulnerability. SD-WAN solutions have evolved to meet these challenges.

IV.2 SD-WAN Overview

Software-defined wide area networks (SD-WAN) are a combination of two technology areas. the one traditional, and one relatively new. It takes the new concept of software-defined networking (SDN) and applies it to traditional enterprise-wide area network architecture. SD-WAN is an overlay architecture that applies the concept of SDN to the traditional WAN. It's designed to meet the needs of modern enterprise applications and rapidly increasing safety requirements.

The management plane, control plane, and data plane are all separated in SD-WAN. This enables each component to operate independently and efficiently, as well as facilitating the scaling of the various components in accordance with network requirements.

IV.3 Benefits of SD-WAN

Many companies and technical researchers agree that the next-generation networks would be deployed and operated As-a-System and not as a collection of individual network devices. SD-WAN is a centralized approach to managing and operating large WAN networks.

1. **Single Management Plane:** One of the best ideas of SD-WAN is to administrate and monitoring the WAN via a single centralized management plane using controllers to manage the underlying network devices. This provides a better overall user experience.
2. **Affordable Bandwidth:** One of the main ideas for the benefits of SD-WAN is cost reduction. Because SD-WAN uses many Internet connections, which means a significant reduction in the cost of the service. Both 4G/5G and broadband are less expensive than MPLS.
3. **Unified Security:** Companies that have integrated policy, security, and orchestration are well suited to modern business. This is something that the SD-WAN network is well equipped to handle. Because of the unified, secure connectivity and end-to-end encryption that runs across the network, your organization will be safe. Cloud-based apps are being used by a large number of businesses.
4. **Scalability:** The deployment of software-defined networking technologies does not necessitate a capital outlay. Because SD-WAN is a cloud-based solution, adding a new location is less expensive, quicker, and easier. The solution improves worldwide availability and reduces manual configurations on-site.
5. **Flexibility:** With MPLS, you must utilize the same internet service provider (ISP) across all sites, whereas SD-WAN allows you to work with a variety of ISPs. You may also easily switch to a backup connection, such as LTE, if necessary. This ensures that your most critical applications are always accessible [20]**.**

IV.4 Components of SD-WAN

Cisco Viptela SD-WAN solution is made up of four planes - Orchestration plane, Management Plane, Control Plane, and Data Plane. Each plane has its functions and responsibilities and is abstracted away from the other planes. For example, if you replace or add a device in the data plane, that does not affect the control/management or orchestration plane.

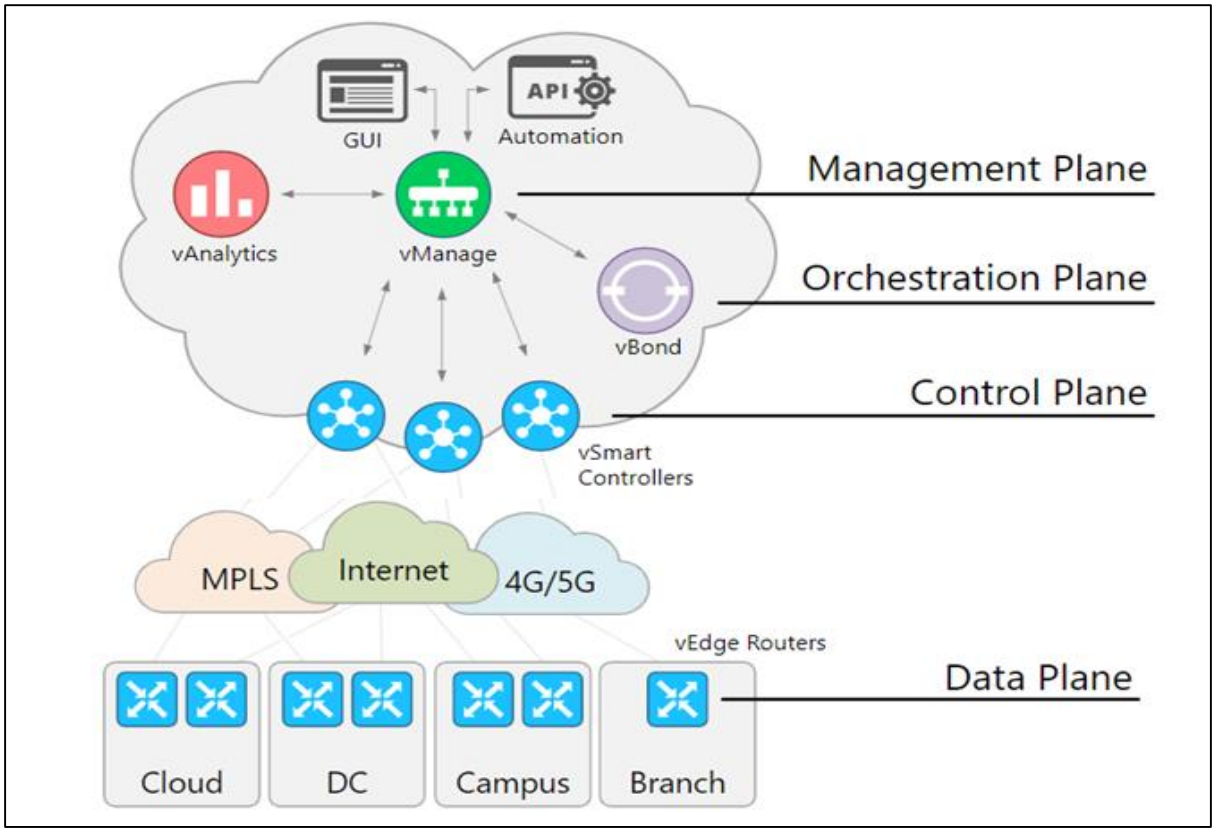


Figure 4.23: Cisco SD-WAN Components.

IV.4.1 vManage NMS

Cisco vMange is a Network Management System NMS (Management Plane) of the SD-WAN system. It provides a GUI interface to facilitates monitoring, configuration, and maintain all Cisco SD-WAN devices and links in the underlay and overlay network. It is responsible for collecting network telemetry data, and alert on events in the SD-WAN fabric. It is also the tool that administrators use to create templates, push configurations, and perform overlay traffic. Cisco vManage can be deployed on-prem, in the public cloud (such as AWS, Microsoft Azure ...), or in the Cisco cloud environment. [21]**.**

IV.4.2 vSmart Controller

The vSmart controller is the SD-WAN solution's centralized control plane, and it manages the overlay network fabric using the Overlay Management Protocol (OMP). As shown in figure 4.24, each vEdge router creates a permanent secure connection to the vSmart controller through each possible transport. The vEdges then use these connections, which are usually DTLS, to provide control plane information to the controller, such as crypto keys and policy information.

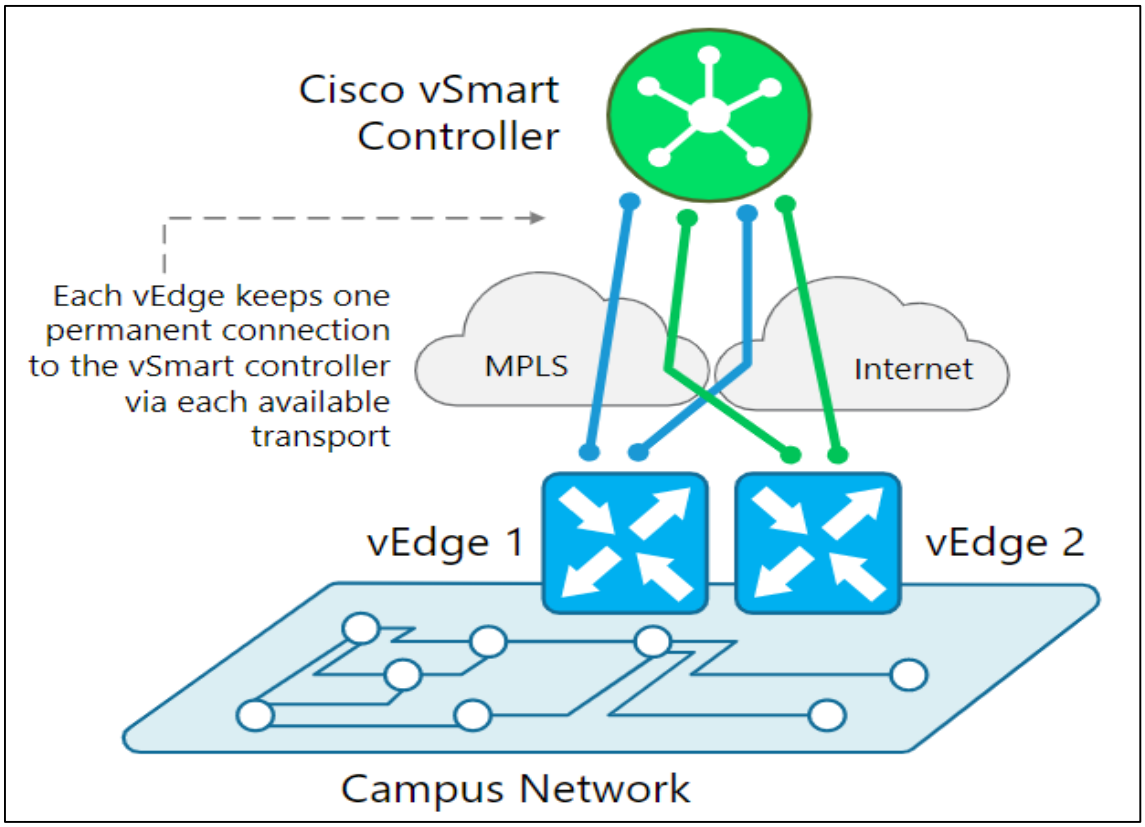


Figure 4.24: Cisco vEdges OMP peering.

Due to the separation of the control plan and data plan in the SD-WAN architecture, the OMP peering will never be performed between vEdge routers on site.

Three types of routes are advertised with OMP:

IV.4.3 vBond Orchestrator

Cisco vBond is the Orchestrator that resides in the orchestration Plane of the SD-WAN system. Its role is to orchestrate the process of onboarding new unconfigured devices to the SD-WAN fabric.

It is responsible for the authentication of vEdge devices and control/management information distribution. The vBond is the only Cisco vEdge device that is located in a public address space. It also has the ability to enable the communication of access devices that sit behind Network Address Translation (NAT) [21].

IV.4.4 vEdge Routers

Cisco vEdge routers (Data Plane) are available as either a hardware device or software-based router. It sits at the WAN edge and establishes the network fabric and joins the SD-WAN overlay. Is in charge of traffic forwarding across the network, as well as security, encryption, Quality of Service (QoS), and routing protocols like BGP and OSPF. When a vEdge router is added to an existing network, it appears to be a regular router. Everything southbound of the vEdge routers is normally traditional networking, such as offices, data centers, and branches, and everything northbound of the vEdge routers is the SD-WAN Overlay network, as depicted in figure 4.25. The Overlay Management Protocol is used to communicate routing information between vEdge routers and vSmart controllers (OMP). Let's say we have a modest company network that uses OSPF. The OSPF routes are redistributed into the SD-WAN network through OMP at the vEdge devices, and the vSmart controllers then pass this routing information to other vEdge routers if the WAN topology requires it.

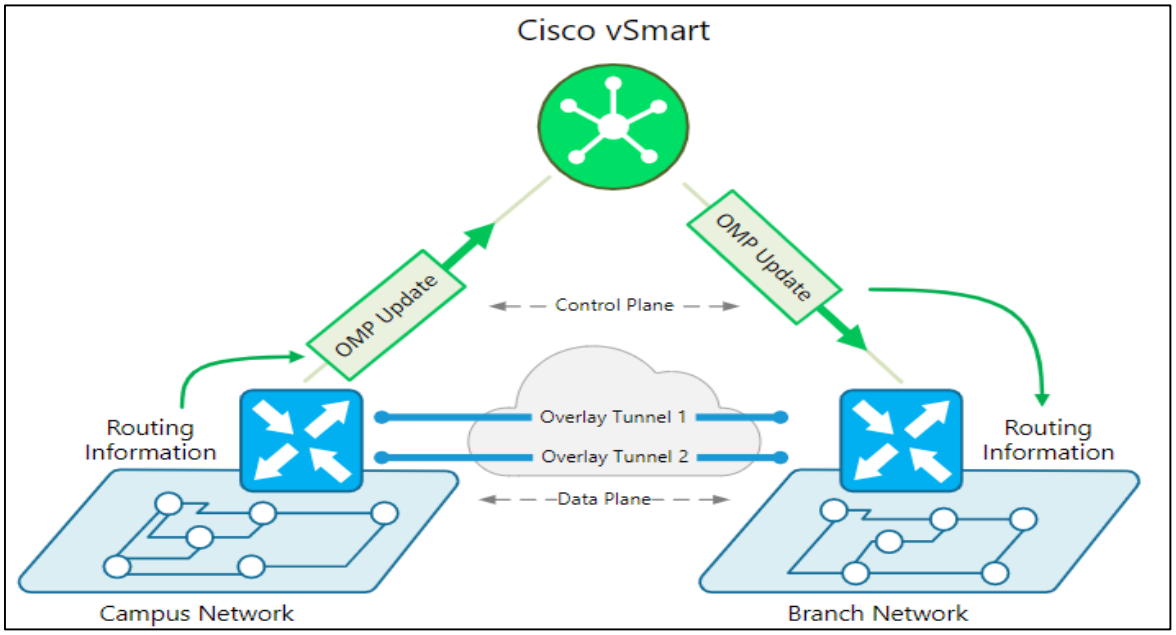


Figure 4.25: Cisco SD-WAN OMP Protocol.

The WAN Edge routers could be either a Viptela software or Cisco IOS-XE devices. They can be virtual or physical devices. The system configures vEdges automatically. This procedure was known as Zero-Touch Provisioning (ZTP) in Viptela, and it is now known as Cisco Plug-and-Play in Cisco devices (PnP). Both names have the same meaning. [21].

IV.5 SD-WAN Deployment

In this part, we'll try to explain how everything works together in this part to construct an operational overlay structure capable of transferring user data more securely and intelligently than traditional WAN. When an enterprise decides to migrate its traditional WAN architecture to Software-Defined WAN, the thing that always comes first is to deploy the controllers. The next step is to migrate the major data centers and finally the remote sites such as campuses and branches.

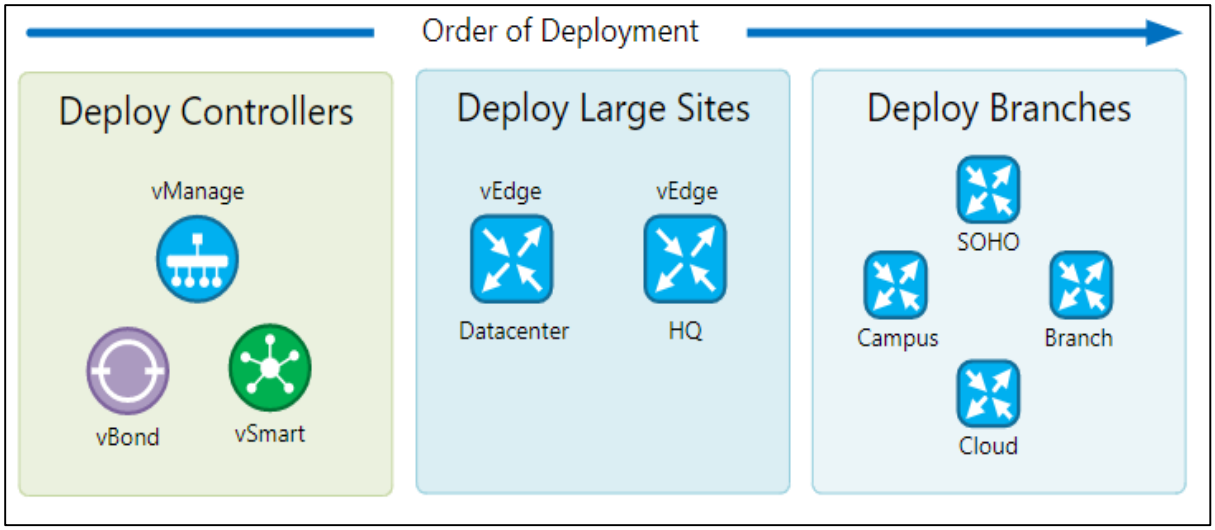


Figure 4.26: Cisco SD-WAN Order of Deployment.

IV.5.1 Controllers Deployment Options

The controllers of a Software-Defined WAN can be installed in the public cloud, which is one of the key benefits. This can drastically cut CAPEX/OPEX expenditures while also improving the management plane/control plane's overall availability and redundancy. Compare this model to the scenario in which you have all controllers deployed on-premises. You need to accommodate rack space, power, cooling, physical servers, hypervisor, and virtual machines or containers. You have to manage redundancy and backups on your own. Using the cloud options, you can consume the management/control plane as IaaS (Infrastructure-as-a-Service) or even SaaS (Software-as-a-Service).

Customers can choose from the following choices provided by Cisco:

- **Cisco-hosted cloud -** According on the data I've gathered on current deployments, the majority of customers (over 90%) prefer this method. This is also the vendor's recommended architecture because Cisco handles all controller provisioning, backup, and disaster recovery. The customer is basically consuming the SD-WAN control plane as a Software-as-a-Service (SaaS) by using the vManage to create custom configuration templates for their device and administer the overlay fabric.
- **Public cloud -** The customer could decide to host the controllers in the public clouds such as Azure and AWS. In this scenario, the controllers could be managed by a service provider or by the customer.
- **On-prem -** Of course, the controllers can be deployed in the company's data centers or private clouds. The client is responsible for backups and disaster recovery in this circumstance. This is common in banking and government institutions that are required to comply with regional regulators.

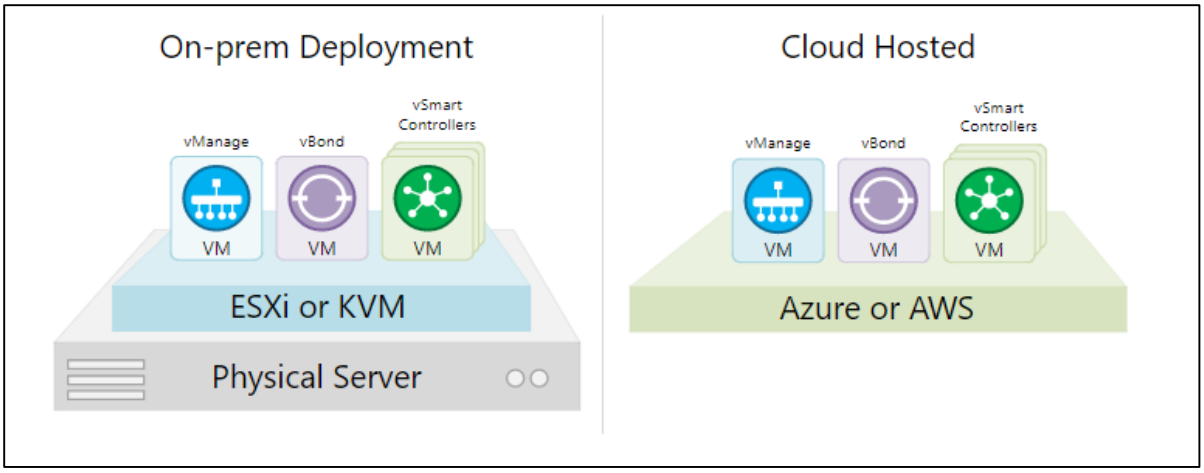


Figure 4.27: Cisco SD-WAN Deployment Options.

Once the controllers are up and operating, they must link in a secure manner. When it comes to the underlying secure protocol, there are two options: TLS, which utilizes TCP transport, and DTLS, which uses UDP transport. All controllers use the DTLS option by default. Figure 4.28 displays the Layer four information for all permanent connections between the controllers if the SD-WAN is deployed in a zero-trust environment Manage and vSmart each have a persistent DTLS connection to the vBond, resulting in four vManage and vBond connections and two vSmart and vBond connections [22].

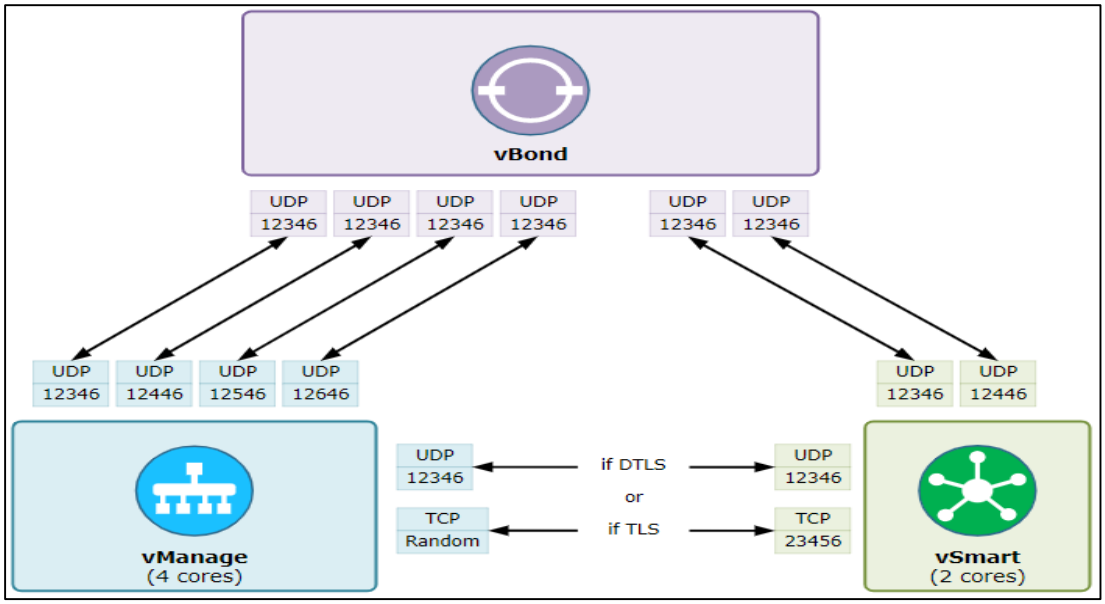


Figure 4.28: Cisco SD-WAN Control Connections.

IV.5.2 Communication in Cisco SD-WAN

Every device needs to be authenticated before becoming part of the system which makes complete sense of security and certificate authentication is used for thatTo obtain a full configuration, a vEdge router must establish a secure connection with the vManage, as well as a secure connection with the vSmart controller to participate in the overlay network. The discovery of the vManage and vSmart occurs automatically and is performed by first establishing a secure connection to the vBond orchestrator, as shown in Figure 4.29. When a new vEdge router joins a network, the following processes occur:

- Over a secure channel, the vEdge router authenticates with the vBond orchestrator and retrieves the IP addresses of vSmart and vManage. The new vEdge is also communicated to vManage and vSmart via the vBond.
- The vEdge router establishes secure DTLS or TLS sessions with the vManage and vSmart controllers before terminating the connection with the vBond orchestrator. If the vEdge router successfully authenticates with the vManage NMS, the vManage will push the whole configuration to the vEdge router.
- Over each transport link, the vEdge router attempts to establish DTLS/TLS connections with the vSmart controllers. It will establish an OMP session after being authenticated by

the vSmart controller and then learn the routes, including prefixes, TLOCs, service routes, encryption keys, and policies.

- Lastly, the vEdge establishes IPsec tunnels with other vEdge routers.

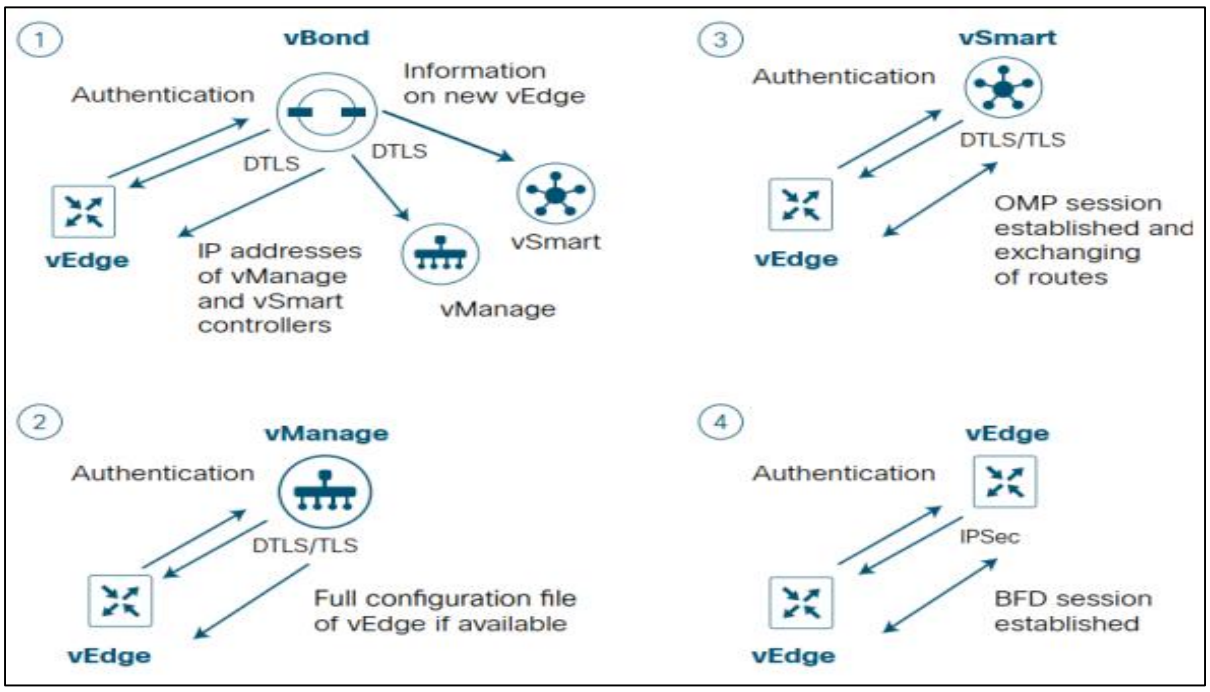


Figure 4.29: Cisco SD-WAN Bring Up Process.

IV.6 Overlay Management Protocol

Route prefixes, crypto keys, and policy information are exchanged through a secure connection by Cisco SD-WAN, which runs between the vSmart controllers and WAN Edge routers (DTLS or TLS). If no policy is established, OMP will allow a full mesh topology, which means each WAN Edge router can connect directly to other WAN Edge routers. Three types of routes are advertised by OMP:

1. **OMP routes (**also known as **vRouter)** Between the vSmart controllers and vEdge routers in the overlay network, OMP is the control protocol that is used to exchange policy, management, and routing information (which could be OSPF or BGP routes). OMP is a protocol similar to iBGP that allows vSmart to operate as a route reflector.

2. **TLOC routes (Transport locations)** Is the tunnel endpoints on the WAN Edge routers that connect to the transport networks are known as Transport Locations (TLOCs). The system IP, circuit interface color, and encapsulation Protocol are used to represent these routes.
3. **Service routes** Are a method to use the router control plane to provide and exchange services such as firewall, IPS, load-balancers [23]**.**

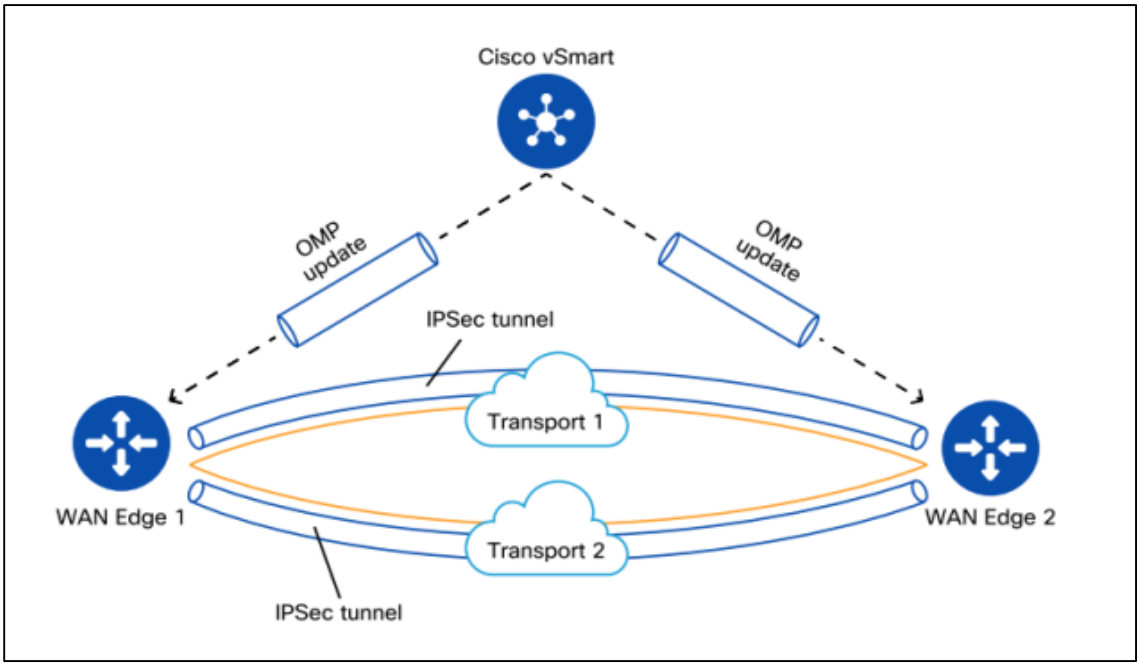
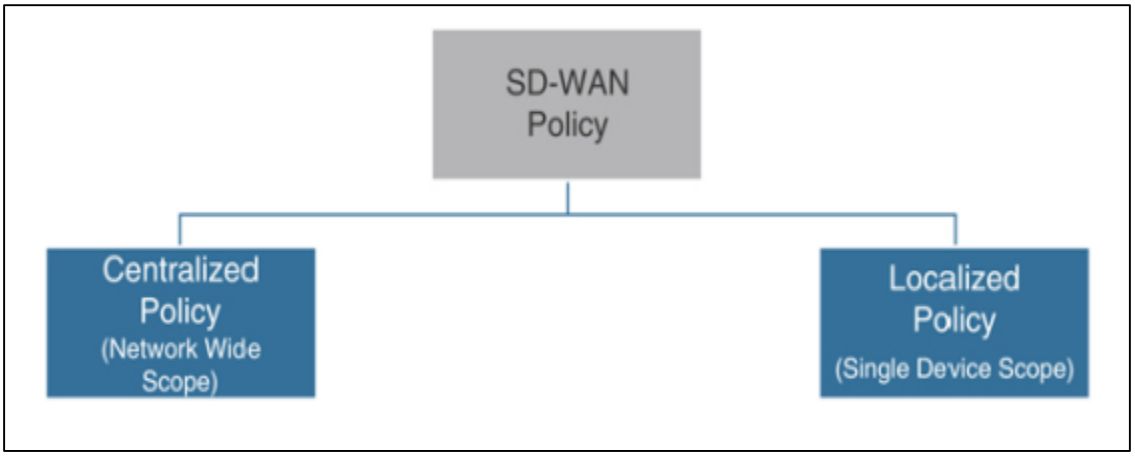


Figure 4.30: OMP Protocol.

IV.7 Cisco SD-WAN Policies

Network administrators use several types of policies to achieve their business objectives. Policies can be categorized as either centralized policies or localized policies. In general, centralized policies control routing information and data that is transmitted through the Cisco SD-WAN fabric. Localized policies control routing and traffic forwarding at the perimeter of the Cisco SDWAN fabric where WAN Edge routers interface with traditional routers. Figure 4.31 illustrates the relationships between these types of policies.



. **Figure 4.31:** Types of Cisco SD-WAN Policies.

IV.7.1 Centralized policy

Figure 4.32 shows that centralized policies can be further classified as either control policies (called topology policies in the vManage GUI) or data policies (called traffic policies in the vManage GUI). Control policies are used to manage the structure of the Cisco SD-WAN fabric by changing the control plane information exchanged through the Overlay Management Protocol (OMP). Data policies are used to change the traffic forwarding using the Cisco SD-WAN fabric to directly manage the data plan.

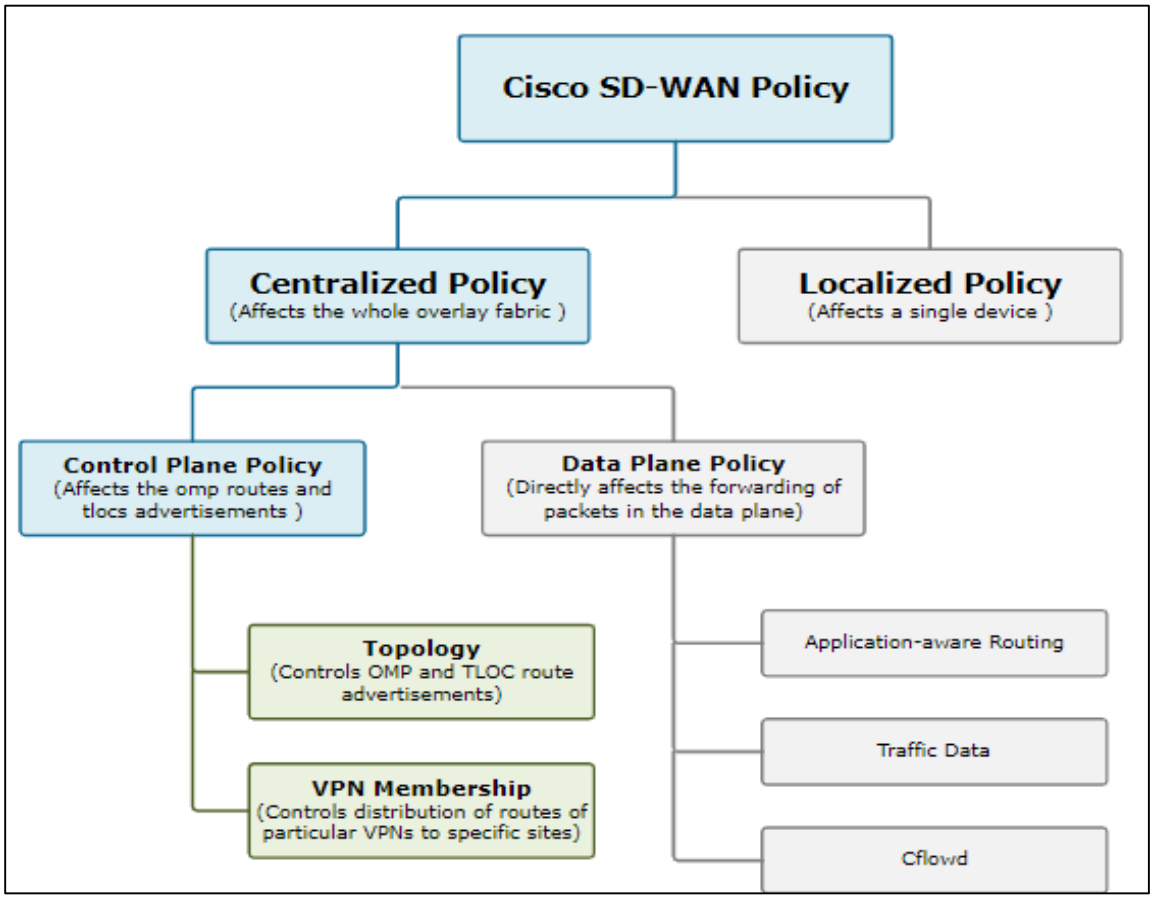


Figure 4.32: Types of Centralized Policies.

- There are two types of Centralized Control Policies in Cisco SD-WAN, each with a different objective:
- **Topology -** Route information like OMP, TLOC, and service routes are redistributed to a list of sites using topology policies. They are used to manage the overlay topology and limit the number of overlay tunnels between locations.
- **VPN Membership** - VPN Membership policies are used to manage how routing information for specific VPNs is distributed to a group of sites. Creating guest networks with Internet access is a common use-case, although site-to-site communication is limited.

IV.7.2 Localized policy

Similar to centralized policies, localized policies can be used to manipulate both the control plane and the data plane. Figure 4.33 illustrates the two main types of localized policy: traditional localized policy and security policy. Route policies, quality of service, and access control lists are all examples of traditional localized policies (ACLs). The security policy feature set supports guest access, Direct Cloud Access (DCA), and Direct Internet Access (DIA). Route policies, or localized control plane policies, can be used to filter or update routes exchanged or learned outside of the SD-WAN fabric using protocols like BGP, OSPF, and EIGRP. Route policies can also be used to filter routes as they are redistributed across protocols, such as between OMP and other protocols. Route policies are the sole means to have a localized policy impact on the control plane.

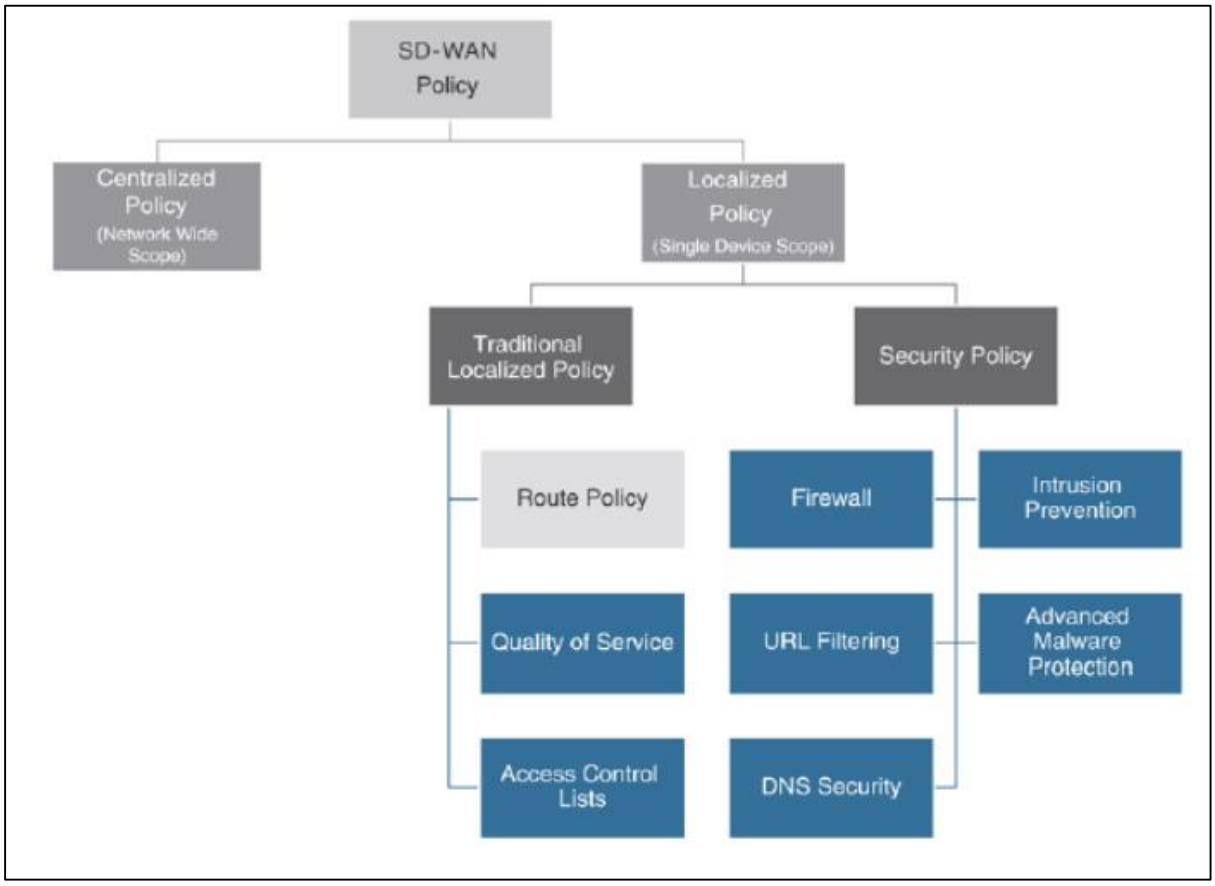


Figure 4.33: Types of Localized Policies.

Localized policies that affect the data plane include the following:

- **Quality of Service:** Quality of Service (QoS) can be configured on the WAN Edge routers to perform queueing, shaping, policing, congestion avoidance, and congestion management.
- **Access Control Lists:** The localized policy can be used to establish access control lists (ACLs) to filter traffic at the interface level. For QoS purposes, ACLs can also be used to mark or remark traffic.
- **Security Policy:** Security Policy feature set actually supports IPS, URL Filtering, Advanced Malware Protection (AMP), and DNS Security. These Characteristics are used to affect traffic in the data plane [24].

IV.8 Conclusion

In this chapter, we explained the need for SD-WAN in networking, the Components and the Communication in Cisco SD-WAN and we discussed the functionality of Overlay Management Protocol (OMP), and finally the policies in cisco SD-WAN.

V.1 Introduction

In this chapter, we will deploy the previously seen MPLS applications, (MPLS VPN and MPLS QoS) and SD-WAN by using EVE-NG emulator. Each lab will be detailed on both the configuration and verification levels in the following pages, we tried to cover all the points covered in the previous chapters. Each lab will have a few configurations and verification captures for demonstration purposes.

V1.1 Work tools

EVE-NG

EVE-NG is a network administration tool similar to GNS3 that allows network managers to simulate routers, switches, and other network appliances such as firewalls, intrusion prevention systems, and so on. You may build a network lab using Cisco, Juniper, Citrix, Arista, A10, Alcatel, Checkpoint, F5, Palo Alto, PFSense, SonicWALL, Trend Micro Tipping Point vTPS, and many other brands. If the network vendor has a virtual device, it can more than likely run in an EVE-NG environment. You can even add Linux and Windows server images. Supporting a huge network/security/system migration or upgrade.

V.2 First LAB: QoS, MPLS VPN L3

V.2.1 Objective of the LAB

The main objective of this LAB is connecting GICA company (Alger) with SCIBS BENI-SAF using MPLS VPN L3, and assigning 2Mgb bandwidth to TFTP traffic using QoS MPLS.

V.2.2 Description of the LAB

We have used eight routers in our LAB. Six routers are in the service provider domain, and two are customer edge routers shown in figure 5.34. Four provider routers in the service provider core are P-R3, P-R4, P-R5, and P6. The functionality of these routers is providing an MPLS backbone. The two other edge routers are PE-R2 and PE-R7, PE-R2 is facing the Customer site1 and PE-R7 is facing Customer site2. PE-R2 and PE-R7 routers are providing connectivity to the customer routers and also providing the functionality of MPLS VPNs. Customer Edge routers will only run

the normal routing protocols, and they are isolated from the provider network. Service Provider core routers are running OSPF as an interior routing protocol. Customer's edge routers are running RIPv2 as a routing protocol. Virtual routing and forwarding (VRF) have been configured on the provider's edge routers that are only handling customer's routes separately. BGP peering is being configured between the provider's edge routers to carry all the customer's routes from one site to another site. And finally, we have added QoS to our LAB, we have used a uniform DiffServ QoS model and created a TFTP class. The DiffServ QoS model is configured on the customer's edge routers and also at the service provider. Classification and Marking are done at the customer's routers. Provider's router is matching traffic on the basis of IP Precedence value and assigning 2Mgb bandwidth to TFTP traffic.

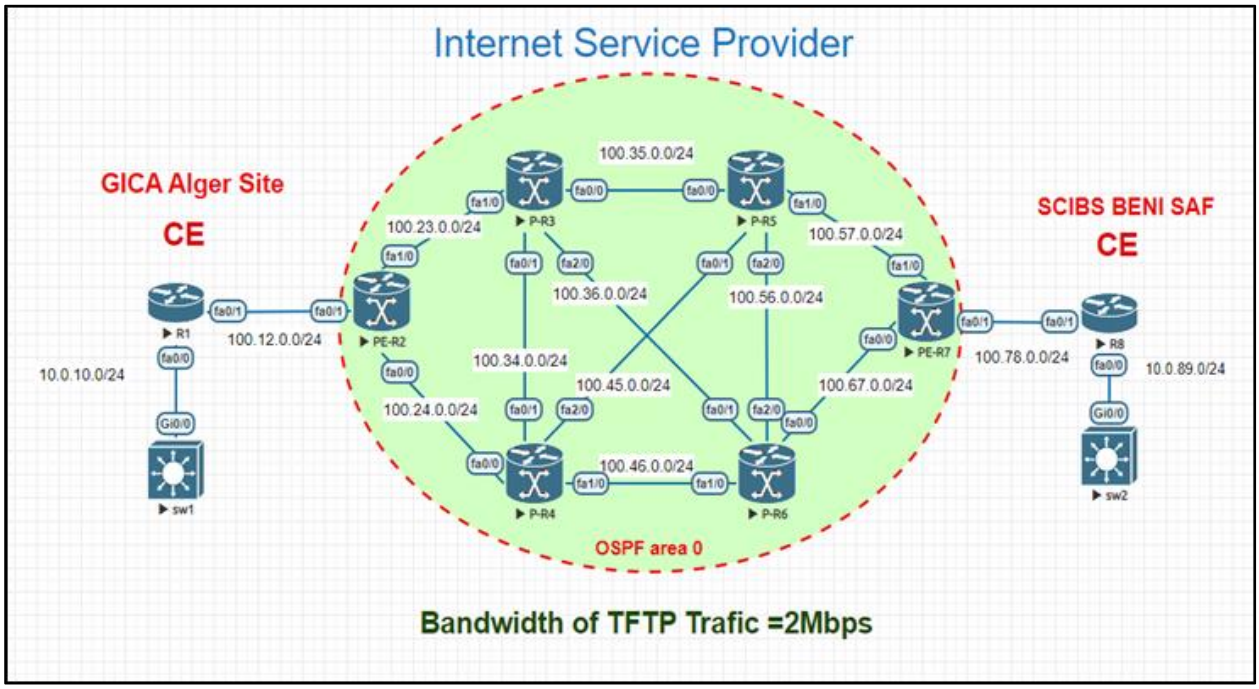


Figure 5.34: QoS MPLS VPN L3.

V.2.3 Configuration and verification

IGP and LDP

To start, all of our Provider and Provider-Edge routers will be configured to use the Label Distribution Protocol (LDP). This is performed by enabling LDP at the global level, then per-

interface on each MPLS domain interface, and finally implementing OSPF as an IGP in the ISP core.

Enable LDP

```
mpls ip
interface FastEthernet x/x
mpls ip
```

OSPF Configuration

```
router ospf 1
network 7.7.7.7 0.0.0.0 area 0
network 100.57.0.7 0.0.0.0 area 0
network 100.67.0.7 0.0.0.0 area 0
```

Verification:

There are two commands that may be used to verify this configuration.

First, we'll use **show mpls interfaces** to see which interfaces LDP is enabled on, and then we'll use **show mpls ldp neighbor** to ensure successful LDP neighbor finding.

```
PE-R2#show mpls interfaces
Interface              IP         Tunnel   Operational
FastEthernet0/0        Yes (ldp)  No       Yes
FastEthernet1/0        Yes (ldp)  No       Yes
```

Figure 5.35: Verification of mpls ldp interfaces.

```
PE-R2#sh mpls ldp neighbor
    Peer LDP Ident: 100.36.0.3:0; Local LDP Ident 2.2.2.2:0
TCP connection: 100.36.0.3.33427 - 2.2.2.2.646
State: Oper; Msgs sent/rcvd: 77/75; Downstream
Up time: 00:54:09
LDP discovery sources:
  FastEthernet1/0, Src IP addr: 100.23.0.3
        Addresses bound to peer LDP Ident:
          100.35.0.3      100.34.0.3      100.23.0.3      100.36.0.3
    Peer LDP Ident: 100.46.0.4:0; Local LDP Ident 2.2.2.2:0
TCP connection: 100.46.0.4.57688 - 2.2.2.2.646
State: Oper; Msgs sent/rcvd: 72/72; Downstream
Up time: 00:50:18
LDP discovery sources:
  FastEthernet0/0, Src IP addr: 100.24.0.4
        Addresses bound to peer LDP Ident:
          100.24.0.4      100.34.0.4      100.46.0.4      100.45.0.4
```

Figure 5.36: Verification of mpls ldp neighbor.

VRFs on the PE Routers

The VRFs will be configured next in the configuration process. We'll utilize a VRF named ″GICA″, with route distinguishers of 170:170 and 120:120 on PE-R7 and PE-R2, respectively, and route-target of 20:30 on the opposite side.

PE-R7 Configuration

```
vrf definition GICA
rd 170:170
!
address-family ipv4
route-target export 30:30
route-target import 20:20
exit-address-family
!
interface FastEthernet4/0
vrf forwarding GICA
ip address 100.78.0.7 255.255.255.0
```

PE-R2 Configuration

```
vrf definition GICA
rd 120:120
!
address-family ipv4
route-target export 20:20
route-target import 30:30
exit-address-family
!
interface FastEthernet4/0
vrf forwarding GICA
ip address 100.12.0.2 255.255.255.0
```

Verification

To verify, we'll use **show ip vrf** to see if the VRFs have been created.

```
PE-R2#show ip vrf
  Name                 Default RD          Interfaces
  GICA                 120:120             Fa0/1
```

Figure 5.37: Verification of VRF.

Configure MP-BGP

To exchange VPNv4 routes, our two provider edge routers (the ingress and egress LSR) require iBGP.

PE-R7 Configuration

```
router bgp 27
 no synchronization
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 27
 neighbor 2.2.2.2 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
 exit-address-family
```

PE-R2 Configuration

```
router bgp 27
 no synchronization
 bgp log-neighbor-changes
 neighbor 7.7.7.7 remote-as 27
 neighbor 7.7.7.7 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 7.7.7.7 activate
  neighbor 7.7.7.7 send-community extended
 exit-address-family
```

Verification

To test our configuration, we'll use **show ip bgp summary** to examine the adjacency.

```
PE-R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 27
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
7.7.7.7         4    27     558     565        1    0    0 08:06:49        0
```

Figure 5.38: IBGP adjacency.

Configure CE-PE Routing

The edge routers of Customers GICA and SCIBS , as well as ISP edge routers, are configured with RIPv2 to exchange routes.

Costumer R1 Configuration

```
router rip
version 2
network 1.0.0.0
network 10.0.0.0
network 100.0.0.0
no auto-summary
```

Costumer R8 Configuration

```
router rip
version 2
network 8.0.0.0
network 9.0.0.0
network 10.0.0.0
network 100.0.0.0
no auto-summary
```

We must configure RIP, not for the global routing table, but for this specific VRF, because the customer is in the VRF. The address family is used for this. With the redistribution command, we can now get this RIP information into BGP so that we may broadcast it to the other PE router. And finally, we have to redistribute these VPNv4 routes back into RIP so that the CE routers can learn the networks.

PE-R7 Configuration

```
router rip
!
address-family ipv4 vrf GICA
redistribute bgp 27 metric 2
network 100.0.0.0
no auto-summary
version 2
!
router bgp 27
address-family ipv4 vrf GICA
redistribute rip
```

PE-R2 Configuration

```
router rip
!
address-family ipv4 GICA
redistribute bgp 27 metric 2
network 100.0.0.0
no auto-summary
version 2
!
router bgp 27
address-family ipv4 vrf GICA
redistribute rip
```

Verification

We use **show ip route vrf** to check that the routes are being distributed correctly.

```
PE-R2#show ip route vrf GICA

Routing Table: GICA
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
R       1.1.1.1 [120/1] via 100.12.0.1, 00:00:07, FastEthernet0/1
     100.0.0.0/24 is subnetted, 1 subnets
C       100.12.0.0 is directly connected, FastEthernet0/1
     10.0.0.0/24 is subnetted, 1 subnets
R       10.0.10.0 [120/1] via 100.12.0.1, 00:00:07, FastEthernet0/1
```

Figure 5.39: Verification of routes distribution.

Configuration of Quality of Service

We established a class-map for TFTP traffic with an IP precedence value of 4, then assigned TFTP traffic **2MB** bandwidth using policy-map, which we then deployed to the interface.

PE-R2 Configuration

```
class-map match-all MPLS_EXPERIMETAL_4
match mpls experimental topmost 4
!
policy-map OUT_TO_P
class MPLS_EXPERIMETAL_4
bandwidth 2000
!
interface FastEthernet2/0
service-policy output OUT_TO_P
```

Verification

To test the functionality of QoS we have forwarded a file from switch1 to switch2, and to confirm that QoS works as well, we observed that the number of packets has increased after running TFTP and the bandwidth assign to it is 2Mb.

```
PE-R2#show policy-map interface fastEthernet 1/0
 FastEthernet1/0

  Service-policy output: OUT_TO_P

    Class-map: MPLS_EXPERIMETAL_4 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: mpls experimental topmost 4
      Queueing
        Output Queue: Conversation 265
        Bandwidth 2000 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      1040 packets, 91727 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Figure 5.40: Before running TFTP.

```
PE-R2#show policy-map interface fastEthernet 1/0
 FastEthernet1/0

  Service-policy output: OUT_TO_P

    Class-map: MPLS_EXPERIMETAL_4 (match-all)
      49953 packets, 28273398 bytes
      5 minute offered rate 46000 bps, drop rate 0 bps
      Match: mpls experimental topmost 4
      Queueing
        Output Queue: Conversation 265
        Bandwidth 2000 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 3/1698
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      6464 packets, 546357 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Figure 5.41: After running TFTP.

Final Validation

Ping and traceroute will be used as a final check to confirm connectivity from the headquarter company (GICA) to its branch (SCIBS) and to indicate the traffic path is going through the MPLS core.

```
SW1#ping 10.0.89.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.89.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 55/62/71 ms
```

Figure 5.42: Ping output SW1-to-SW2.

```
SW1#tracerout 10.0.89.10
Type escape sequence to abort.
Tracing the route to 10.0.89.10
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.10.1 11 msec 3 msec 8 msec
  2 100.12.0.2 23 msec 21 msec 23 msec
  3 100.23.0.3 [MPLS: Labels 22/29 Exp 0] 240 msec 61 msec 70 msec
  4 100.36.0.6 [MPLS: Labels 21/29 Exp 0] 117 msec 50 msec 55 msec
  5 100.56.0.5 [MPLS: Labels 19/29 Exp 0] 87 msec 60 msec 55 msec
  6 100.78.0.7 [MPLS: Label 29 Exp 0] 47 msec 55 msec 55 msec
  7 100.78.0.8 179 msec 57 msec 50 msec
  8 10.0.89.10 81 msec 79 msec *
```

Figure 5.43: Traceroute Output SW1-to-SW2.

V.3 Second LAB: SD-WAN

V.3.1 Objective of the LAB

The main objective of the LAB is:

- connect the headquarters (GICA) with its branches using SD-WAN technology.
- enable the company to bring network operations and management into one console, centralized management.
- configure Centralized Policy to block Facebook for all branches.
- Improve network security: SD-WAN comes with built-in security mechanisms and encryption, guaranteeing that only authorized users may access and view assets connected to a business network.
- reducing time and cost of deployment by using templates.
- reducing the mistakes of deployment due to the Graphical User Interface (GUI) rather than producing lines of code.

V3.2 Description of the LAB

There is a headquarter and two remote sites in this architecture, with one MPLS (only for simulation) and one Internet service provider SD-WAN controllers hosted in the cloud and accessible through the Internet; one vManage, one vSmart controller, and one vBond orchestrator are present. Each vEdge router tries to connect to the controllers through the Internet.

Hardware and Software

Cisco SD-WAN Software:

• Version 19.2.0

Cisco SD-WAN Devices:

• 1x vManage

• 1x vSmart

• 1x vBond

• 3x vEdge

Infrastructure Devices:

• 3x Windows 8.1 Desktop

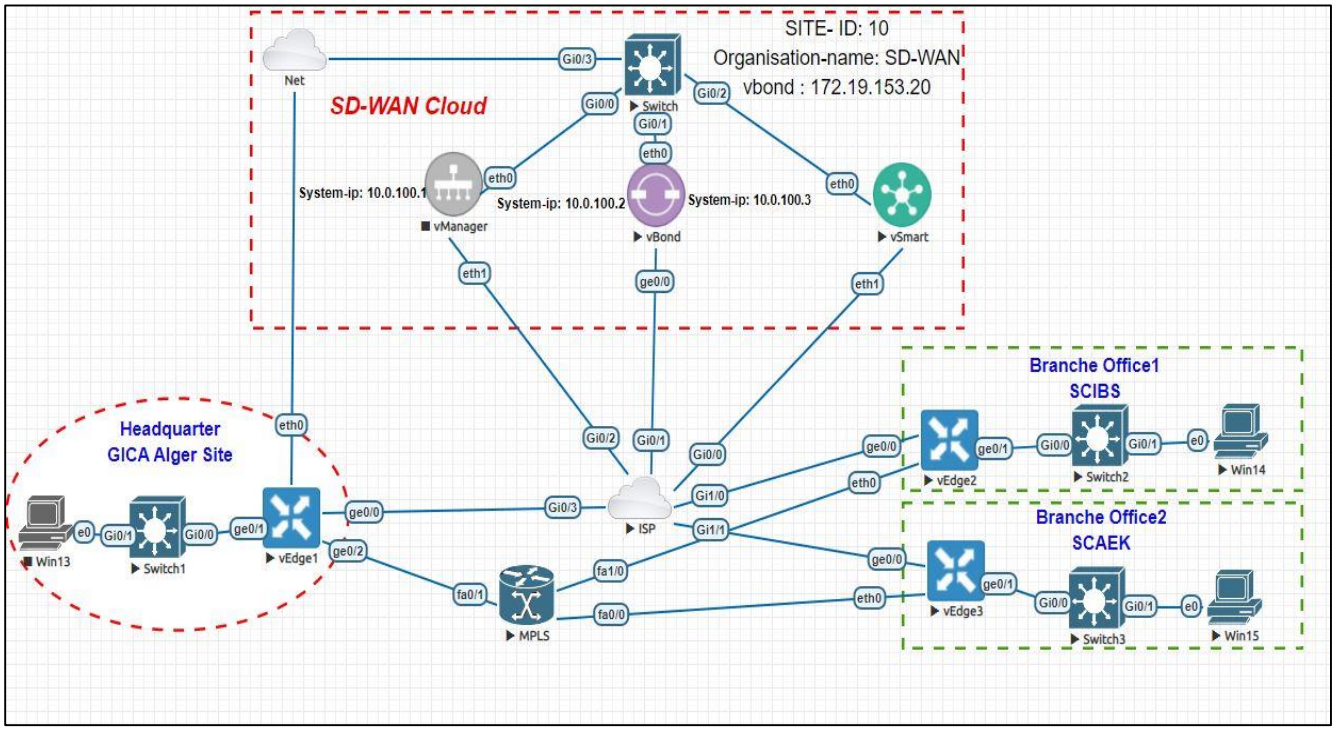


Figure 5.44: SD-WAN Topology.

V.3.3 Configuration and verification

Set up the vBond

All SD-WAN devices in the fabric must have the same organization-name. A vBond must be accessible to every device in the fabric.

In Cisco SD-WAN terms, a VPN is similar to a VRF, and VPN0 is the transport VPN used by all SD-WAN devices. The static route selected affects only VPN0. VPN0 will be used to create IPsec and/or GRE tunnels as well.

vBond Configuration

```
System
host-name vBond
system-ip 10.0.100.2
site-id 10
admin-tech-on-failure
no route-consistency-check
sp-organization-name SD-WAN
organization-name SD-WAN
vbond 172.19.153.20 local vbond-only
!
vpn 0
interface ge0/0
ip address 172.19.153.20/24
tunnel-interface
encapsulation ipsec
allow-service all
no shutdown
!
ip route 0.0.0.0/0 172.19.153.1
!
vpn 512
interface eth0
ip address 192.168.153.20/24
no shutdown
ip route 0.0.0.0/0 192.168.153.1

!
```

```
vBond# show control local-properties
personality                     vedge
sp-organization-name            SD-WAN
organization-name               SD-WAN
root-ca-chain-status            Installed

certificate-status              Installed
certificate-validity            Valid
certificate-not-valid-before    Jun 11 16:44:45 2021 GMT
certificate-not-valid-after     Dec 02 16:44:45 2026 GMT

dns-name                        172.19.153.20
site-id                         10
domain-id                       1
protocol                        dtls
tls-port                        0
system-ip                       10.0.100.2
chassis-num/unique-id           76152565-501b-4754-9ddd-cb9cb512e497
serial-num                      EDB3A5F392E14616
token                           Invalid
keygen-interval                 1:00:00:00
retry-interval                  0:00:00:18
no-activity-exp-interval        0:00:00:20
dns-cache-ttl                   0:00:02:00
port-hopped                     FALSE
time-since-last-port-hop        0:00:00:00
pairwise-keying                 Disabled
embargo-check                   success
number-vbond-peers              0
```

Figure 5.45: Display local properties related to the control plane.

```
vBond# show orchestrator connections
                                                                                      PEER                     PEER
         PEER     PEER     PEER                SITE         DOMAIN       PEER              PRIVATE  PEER               PUBLIC
                 ORGANIZATION
INSTANCE TYPE     PROTOCOL SYSTEM IP            ID           ID           PRIVATE IP        PORT     PUBLIC IP          PORT    REMOTE COLOR
 STATE           NAME                       UPTIME
------------------------------------------------------------------------------------------------------------------------------------
-----------------------------------------------------
0        vsmart   dtls     10.0.100.3           10          1            172.19.153.30     12346    172.19.153.30      12346   default
 up              SD-WAN                     0:00:15:09
0        vsmart   dtls     10.0.100.3           10          1            172.19.153.30     12446    172.19.153.30      12446   default
 up              SD-WAN                     0:00:15:08
0        vmanage  dtls     10.0.100.1           10          0            172.19.153.10     12346    172.19.153.10      12346   default
 up              SD-WAN                     0:01:43:47
0        vmanage  dtls     10.0.100.1           10          0            172.19.153.10     12446    172.19.153.10      12446   default
 up              SD-WAN                     0:01:43:48

(END)
```

Figure 5.46: Verification the active DTLS connections to the vBond orchestrator.

Set up the vSmart

Except for policy, the vSmart's initial configuration is virtually similar to that of the vBond.

vSmart Configuration

```
System
host-name vSmart
system-ip 10.0.100.3
site-id 10
admin-tech-on-failure
sp-organization-name SD-WAN
organization-name SD-WAN
vbond 172.19.153.20
!
vpn 0
interface eth1
ip address 172.19.153.30/24
tunnel-interface
  allow-service all
no shutdown
!
ip route 0.0.0.0/0 172.19.153.1
!
vpn 512
!
policy
data-policy _service_vpn20_DIA
vpn-list service_vpn20
sequence 1
match
source-data-prefix-list VPN20_supernet
app-list Facebook
!
action drop
log
!
```

Set up the vManage

vManage Configuration

```
System
host-name vManage
system-ip 10.0.100.1
site-id 10
admin-tech-on-failure
sp-organization-name SD-WAN
organization-name SD-WAN
vbond 172.19.15.20
!
vpn 0
interface eth1
ip address 172.19.153.10/24
no shutdown
!
ip route 0.0.0.0/0 172.19.153.1
!
vpn 512
interface eth0
ip address 192.168.153.10/24
no shutdown
!
```

```
vManage# show control local-properties
personality                         vmanage
sp-organization-name                SD-WAN
organization-name                   SD-WAN
root-ca-chain-status                Installed

certificate-status                  Installed
certificate-validity                Valid
certificate-not-valid-before        Jun 11 09:55:35 2021 GMT
certificate-not-valid-after         Dec 02 09:55:35 2026 GMT

dns-name                            172.19.153.20
site-id                             10
domain-id                           0
protocol                            dtls
tls-port                            23456
system-ip                           10.0.100.1
chassis-num/unique-id               77ed6405-e962-4c3e-8a98-e06e9349a55f
serial-num                          EDB3A5F392E14614
cloud-hosted                        no
token                               -NA-
retry-interval                      0:00:00:19
no-activity-exp-interval            0:00:00:20
dns-cache-ttl                       0:00:02:00
port-hopped                         FALSE
time-since-last-port-hop            0:00:00:00
number-vbond-peers                  1
```

Set up the vEdge

Finally, the vEdge will be connected to the SD-WAN fabric. It's a fairly similar procedure.

vEdge Configuration

```
System
host-name vEdge-1
system-ip 4.4.4.4
site-id 101
admin-tech-on-failure
no route-consistency-check
sp-organization-name SD-WAN
organization-name SD-WAN
vbond 172.19.153.20
!
vpn 0
interface ge0/0
description "vpn0 interface"
ip address 172.19.153.15/24
no shutdown
!
interface ge0/1
description MPLS
ip address 1.1.101.2/30
no shutdown
!
vpn 20
router
ospf
timers spf 200 1000 10000
redistribute omp
area 0
interface ge0/2
exit
!
interface ge0/2
description "LAN INTERFACE"
ip address 172.16.1.1/24
no shutdown
```

Monitoring and visibility

SD WAN promises to create greater visibility of the network. Visibility on the utilization of your connectivity and applications across the network can give insight to what’s actually happening, and also monitoring the state and resources of the devices.

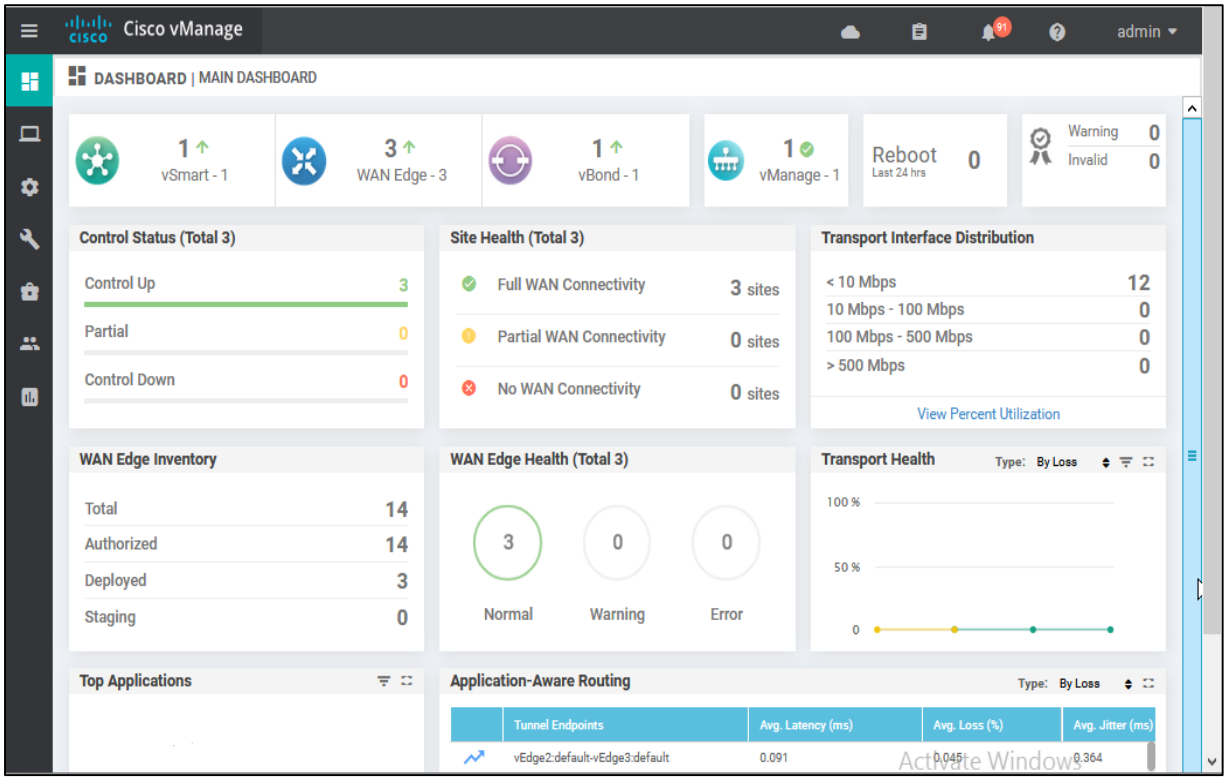


Figure 5.47: vManage dashboard.

OSPF Template

To connect our branches together we have used OSPF, we have done the OSPF template in the vManage, then attached it to each vEdge with changing the IP address corresponding to each site.

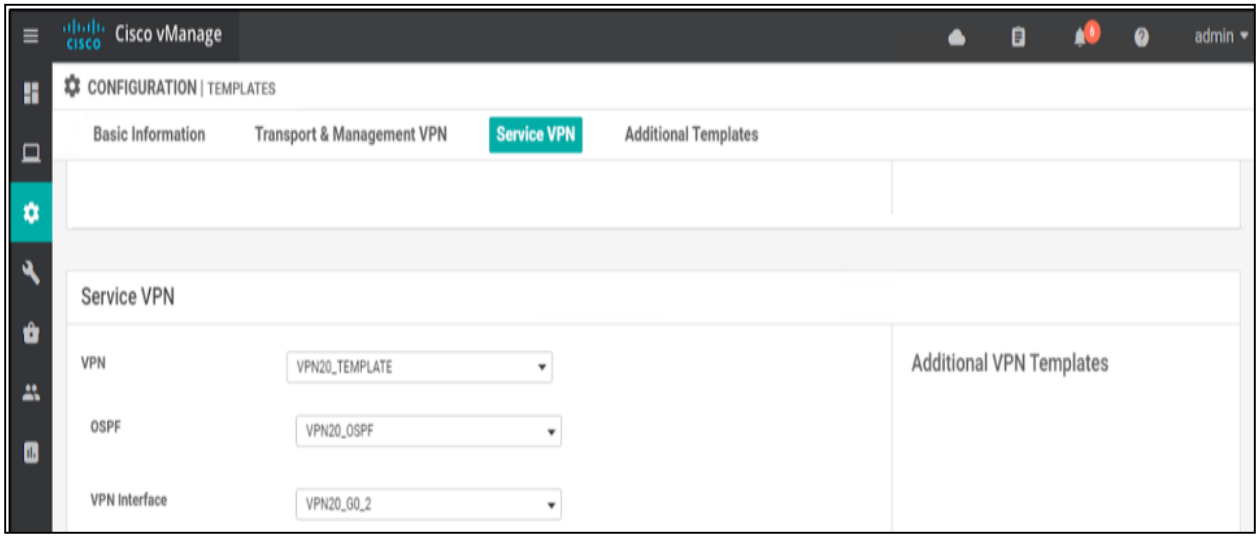


Figure 5.48: OSPF Template.

V.4 Conclusion:

In this chapter, we proceed to configure two labs, the first one to connect headquarter (GICA) with its branch (SCIBS) over a leased line connexion MPLS and limit the bandwidth of TFTP traffic at 2Mbps by QoS mechanism, and in the second lab, we implemented a cisco SD-WAN solution (Viptela SD-WAN) to improve the management of the traditional WAN design by using smart services for centralized management of all devices in the fabric.

General Conclusion

We have divided our project into two main parts, in the first part we have seen that MPLS has a multitude of applications, among them are VPN and QoS, we confirmed that enterprises need MPLS and its applications, we examined the MPLS technology and found out that MPLS benefits include better performance, delivers packets providing high Quality of service, and proficiently manages and avoids packet loss.

In the second part, we talked about SD-WAN and confirmed that it came to solve many problems of MPLS which are: Complexity, time-consuming to manage, and so expensive to upgrade and scale. We examined the SD-WAN and found out that SD-WAN benefits include Boosts security, Lowers complexity, Reduces costs, and Enables cloud usage. Finally, we concluded that SD-WAN provides many benefits for organizations of all sizes, that is not to mean, however, that it is always the greatest option for businesses. Private networks such as MPLS will always be in demand, especially in companies or institutions that have specific connectivity needs. Companies must spend time weighing the benefits and drawbacks of each solution before deciding if MPLS or SDWAN is the best option for their future.

.

Bibliography

Books

[1] Ghein, D. L. (2006). MPLS Fundamentals: CCIE N°. 1897 (1st ed.). Cisco Systems, (p.5)

[2] Ghein, D. L. (2006). MPLS Fundamentals: CCIE N°. 1897 (1st ed.). Cisco Systems, (p.7 & 8)

[3] Ghein, D. L. (2006). MPLS Fundamentals: CCIE N°. 1897 (1st ed.). Cisco Systems, (p. 10)

[4] Ghein, D. L. (2006). MPLS Fundamentals: CCIE N°. 1897 (1st ed.). Cisco Systems, (p.17)

[5] Ghein, D. L. (2006). MPLS Fundamentals: CCIE N°. 1897 (1st ed.). Cisco Systems, (p.25)

[7] Reagan, J. (2021). CCIP-MPLS Study Guide (Vol.466). USA: Sybex, Hardcover (2002), (p.9)

[8] Barker. K & Morris. S. (2012). CCNA Security 640–554 Official Cert Guide (Vol. 741). Cisco Press, USA: MICHAEL WATKINS (p. 426)

[10] Kocharians, N. (2017). CCIE Routing and Switching v5.1 Foundations. Cisco Press.

[11] Black, Uyless D. (2001). MPLS and Label Switching Networks. Upper Saddly River, New Jersey: Prentice Hall PTR

[12] MPLS Fundamentals Video Course by Keith Barker (CBT nuggets)

[13] MPLS Layer 3 VPNs Published by Alexandrina Cain

[14] Ram Balakrishnan. (2008). Advanced QoS for multi-service IP MPLS networks, Wiley Publishing, Inc, USA. (p.5)

[16] Brad Edgeworth et al. (2020). CCNP and CCIE Enterprise Core ENCOR 300-401 Official Cert Guide, Cisco press, USA. (p.782-794)

[17] Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA. Cisco IOS Quality of Service Solutions Configuration Guide. Release 12.2SR

[18] Brad Edgeworth et al. (2020). CCNP and CCIE Enterprise Core ENCOR 300-401 Official Cert Guide, Cisco press, USA. (p .835)

[19] Luc De Ghein. MPLS Fundamentals Cisco CCIE NO.* 1897 (p. 467)

[23] Cisco SD-WAN Design Guide. (2020).

[24] Gooley. J. (2020). Cisco Software-Defined Wide-Area Networks, Cisco press, USA, (p. 208)

Web Sites

[6] url: https://networklessons.com/mpls/mpls-ldp-label-distributionprotocol/

(visited on 03/22/2021).

[9]url: https://ipcisco.com/lesson/l3-vpn-control-plane-activities/

(visited on 04/01/2021)

[15] url: https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/introduction-qos-quality-service

(visited on 03/31/2021).

[14] https://www.extnoc.com/blog/sd-wan-vs-mpls/

(visited on 04/03/2021).

[21] url: https://www.networkacademy.io/ccie-enterprise/sdwan/what-is-sd-wan

(visited on 04/03/2021).

[22] url: https://www.networkacademy.io/ccie-enterprise/sdwan/how-cisco-sd-wan-works

(visited on 04/03/2021)