عدد خاص
بالمؤتمر الليبي الدولي للعلوم التطبيقية
و الهندسية
27-28- سبتمبر 2022

Multiprotocol Label Switching Layer 3 VPN Solution for Libyan Oil Company

Khawlah Alqamoudi [1] , Mawada Alqamoudi [1]
Mohamed Ghretli [1] , Bashir Khamoudi [2]
bkhamoudi2014@hotmail.com
1 College of Computer Technology, 2 Appled Research and Devlopment Org.

الملخص

قامت تقنية MPLS بتحسين العيوب الموجودة فى الشبكة التقليدية, و ذلك لأن تقنية MPLS لا تقوم بتوجيه الحزمة اعتمادا على عنوان الجهاز المستقبل (Destination ip address) بل تقوم بتوجيه الحزمة اعتمادا على المصلقات (Labels).

طريقة الاتصال التى تستخدمها تقنية (MPLS L3 VPNs) هي النظير الى النظير (Peer–to–peer) و بروتوكول التوجيه (BGP) الذي ينشر المعلومات المتعلقة با الشبكة الخاصة الافتراضية (VPN). ان ميزة استخدام اتصال (النظير الى النظير) هي الحفاظ على التكلفة (Cost saving) و التقليل من المشاركة مع حلول قابلية التوسع العالية.

يقدم هذا البحث محاكاة (MPLS L3 VPN) لشبكة حقيقية لشركة نفطية فى ليبيا , باستخدام برنامج (GNS3). تظهر نتائج المحاكاة القدرة على استخدام نفس عنوان (IP Address) و نفس (Subnet mask) لواجهتين (Interfaces) على نفس جهاز التوجيه (Router) بدون تداخل بينهم.

Abstract

Multiprotocol Label Switching (MPLS) technology has improved the weaknesses of traditional IP networking. This is because MPLS does not route packets based on destination IP address but rather forward packets based on their labels. MPLS L3 VPNs use a peer to peer connection that uses Border Gateway Protocol (BGP). The distribution is based on Virtual Private Network (VPN) related information. Cost saving and engagement reduction with highly scalability solutions are accomplished using this peer-to-peer enterprise model.
This paper presents the simulation of MPLS Layer 3 VPNs for real network of Oil Company in Libya using GNS3 software. The simulated results show the capability to use two interfaces on the same router with the same IP address and sub netmask without overlap between them.

Keywords: Multiprotocol Label Switching, IP networking, Company in Libya, GNS3 software

I. Introduction

Multiprotocol Label Switching (MPLS) technology is based on forwarding data in relation to its label which increases the speed and controls of network traffic. MPLS data is directed through a specific path based on labels instead of routing through large routing table at every step.[1]

The MPLS has many applications, which are MPLS LAYER 3 VPN (MPLS L3 VPN), MPLS Traffic Engineer (TE), and Quality of Service (QoS). These applications are very important.

MPLS L3 VPNs use a peer-to-peer model which uses Border Gateway Protocol (BGP). The distribution is based on Virtual Private Network (VPN) related information. Cost saving and management reduction with highly scalability solutions are accomplished using this peer-to-peer enterprise model.[2]

In this paper the simulation of MPLS L3 VPN of real network will be carried out using GNS3 software.

The paper will be organized as, the first part will cover the theoretical part related to MPLS overview, MPLS L3 VPN, MPLS VPN Architecture Layer three MPLS VPN operation, and Benefits of a MPLS L3 VPN, whereas the second part will present the simulation of MPLS L3 VPN.

II. MPLS Overview

A. MPLS and the OSI Reference Model

MPLS technology operates at an OSI Reference Model layer that is essentially considered to be in between traditional definitions of Layer two (Data Link layer) and Layer three (internet layer), and for this reason it is often referred to as a "Layer 2.5" protocol [3], as shown in Figure 1. MPLS is named multiprotocol because it works with any protocols such as the IP, ATM, and frame relay network protocols [4].

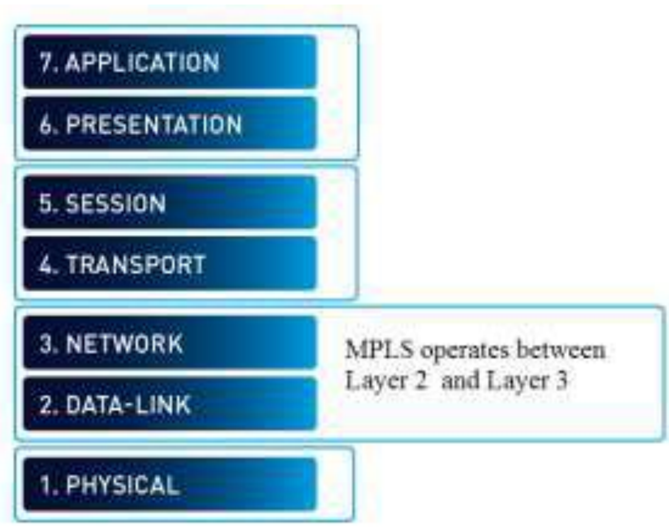


Figure 1. MPLS in OSI model.

B. Label Distribution Protocols

Label Distribution requires a different protocol to distribute the labels and the dynamic routing protocol is used to distribute prefixes. In this method, the routing protocol is independent, and it is an advantage that a new protocol is required in each Label Switch Routers. There are many selections of protocols that allocate labels including:
1) Tag Distribution Protocol.
2) Label Distribution Protocol.
3) Resource Reservation Protocol.

C. Label Distribution Protocol (LDP)

LDP is a protocol which is used between routers in a MPLS cloud to give labels to network and exchange label info with other routers. MPLS encompasses head-to-head routers forming LDP session; local labels are assigned to prefixes and these labels are switched over recognized LDP.
sessions. After completion of label interchange between neighboring LSRs, the control and data structures of MPLS, namely FIB, LIB, and LFIB are populated with data, and the router is prepared to forward data in data plane based on label values [5].
There are four types of C. Label Distribution Protocol messages:
1) Discovery messages: Declare and maintain LSR existence in the network.
2) Session messages: Launch, preserve, and close sessions between LSRs.
3) Advertisement messages: declare label mappings to FECs.
4) Notification messages: Signal errors.

III. MPLS L3 VPN

A. Defined VPN

Virtual Private Network is a collection of networks that may interconnect with each other privately over the public Internet or other public or private clouds [6].

B. Layer Two and Layer Three VPNs

1) Layer two (Data Link Layer) VPN technology managed at layer two are defined as Layer 2 VPNs (ATM, MPLS, Frame Relay).
2) VPNs based on tunneling at Layer Three (Network Layer) are Layer 3 VPNs, BGP/MPLS, IPSec)[7].

IV. MPLS VPN Architecture

There are three fundamental building blocks on PE routers. They are as follows:-
1) Virtual Routing Forwarding (VRF).
2) Route Distinguisher (RD).
3) Route Targets (RT).

A. Virtual Routing (Forwarding)

Virtual routing and forwarding tables instances (VRFs) achieve customer isolation on the PE router and this is accomplished by the use of virtual routing tables. The purpose of a VRF is

analogous to a routing table, except that it has all routes relating to a definite VPN versus routing table. The VRF must support Cisco Express Forwarding (CEF).
A physical or logical interface can be linked with only one VRF. Total number of interfaces on the router only limits the number of interfaces that can be linked to a VRF, and
The VRF compromised from an IP routing table similar to the IP routing table, a Cisco Express Forwarding table, all VRF interfaces, and a set of orders defining routing protocol exchange with attached Customer Edge routers (routing frameworks). The VRF also encompasses VPN identifiers as well as VPN association information [8].

B. Route Distinguisher

Route Distinguisher (RD) is an identifier which makes the IPv4 address unique across different VPNs. A Route Distinguisher is a 64bit unique identifier that is pended to the 32-bit customer prefix route obtained from a customer edge router, which makes it a unique 96 bit address which can be transported between the PE routers in the MPLS cloud. Thus, a unique RD is formed for every VRF on the Provider Edge router. The resulting 96 bits address total (32bit prefix for customer + 64-bit RD unique identifier), is called a VPN version 4 (VPNv4) address. VPN addresses are swapped between Provider Edge routers in the provider network as well as IPv4 (32-bit) addresses [8].

C. Route Target (RT)

VPN route target (RT) communities control the distribution of VPNv4 information, implemented by BGP extended communities [8].
The introduction of RT was to overcome the drawbacks of the RD because RD can only communicate with one VPN;
whereas RT can communicate with complex VPN topologies [8].
The values for RT; imported or exported may match the RD value for the VRF even though they don't need to be exactly the same. The RD uniquely classifies customer IPv4 routes and the route-targets define import export policies for routes into and out of the Virtual Routing Forwarding. By using the same RT and RD values make straightforward the configuration and management of it. Figure 2. shows RT and RD mechanism [8].

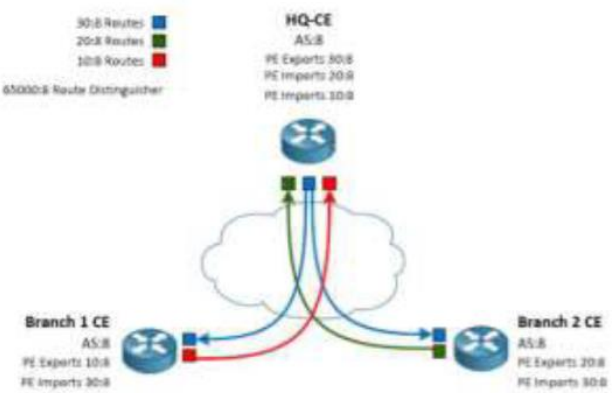


Figure 2. Mechanism of RT and RD [8]

V. Layer Three MPLS VPN Operation

The distribution steps of the operation as pointed in Figure 3. are as follows:

1) Customer routes are inserted into VRF table at PE using static or dynamic routing protocols i.e. RIPv2, OSPF, or BGP between PE and the CE. Customer routes are handed as IPv4 prefixes .
2) The PE route spends a 64bit RD in order to give the ipv4 routing update, resulting in a globally 96bits VPNv4 prefix.
3) The VPN prefix is circulated via MP-BGP session to other PE routers.
4) Receiving PE router strips the Route Distinguisher from the VPNv4 prefix, resulting in an ipv4 prefix. RT is used to match the proper VRF routing table.
5) The prefix is promoted to other CE routers within an ipv4 routing update [9].

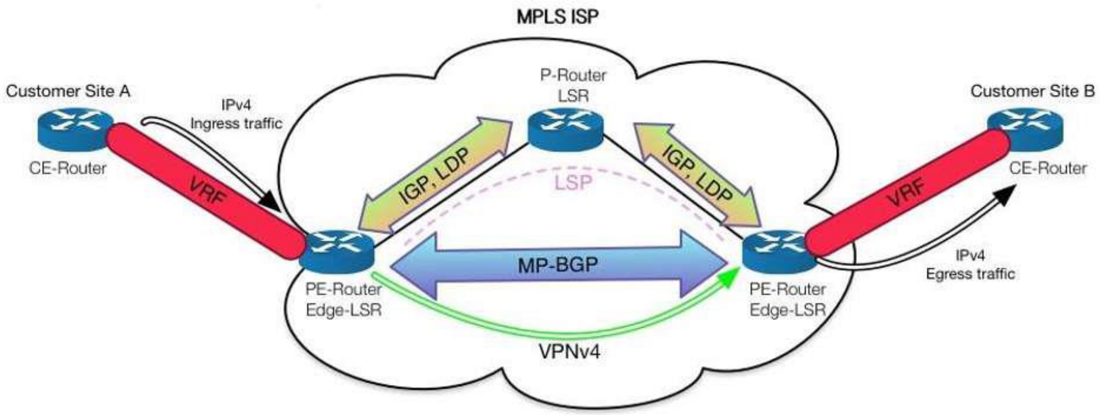


Figure 3. Layer 3 VPN [9]

VI. Benefits of a MPLS L3 VPN

The MPLS L3VPN has the following benefits: -

1) Scalability.
2) Security.
3) Ease of Creation.
4) Flexible Addressing.

VII. Implementation of MPLS L3 VPN

The scenario in this network will have two connected sites, Headquarters (HQ) and Branch-2. Each site has two switches which are connected to the router. While the first switch is connected to the IT department, second switch is connected to Communication Department. The two interfaces have the same IP address and subnet mask on the same router.

This scenario is emulated in GNS3 software, then the configuration set up will be carried out and the results will be displayed.

The whole scenario has been divided into two separate sections, which are described below.

A. Basic Configuration

In this section all interfaces in each router are assigned with IP address, then IP Routing (OSPF) Protocol is configured on all routers (Core Providers and Provider Edge). Also

MPLS is configured on all routers (Core Providers and Provider Edge).

B. MPLS L3 VPN

This section presents four configurations, which are, MPBGP configuration on two PEs (HQ-PE,BR-2-PE), create of two VRFs on HQ-PE and BR-2-PE, then configuring of OSPF as the Routing Protocol Between internal switches departments and provider edge, and followed by redistribution process. The network is shown in Figure 4.a, which uses MPLS L3 VPN configuration during this Lab.

This configuration will be repeated except the names and numbers in order to create second VRF as Table 1 displays that.

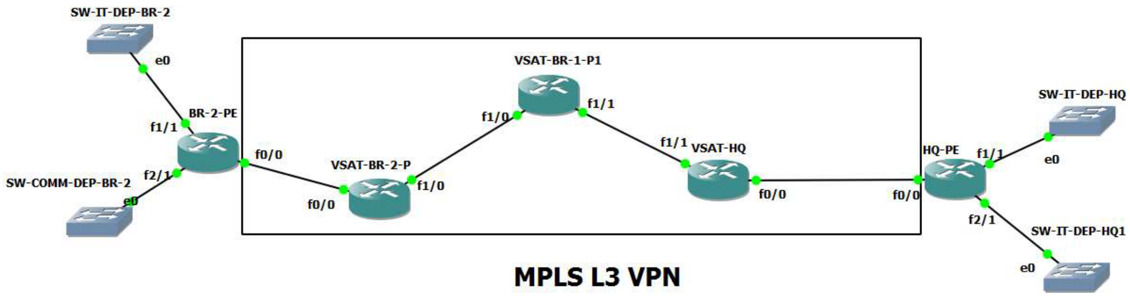


Figure 4 MPLS L3 VPN

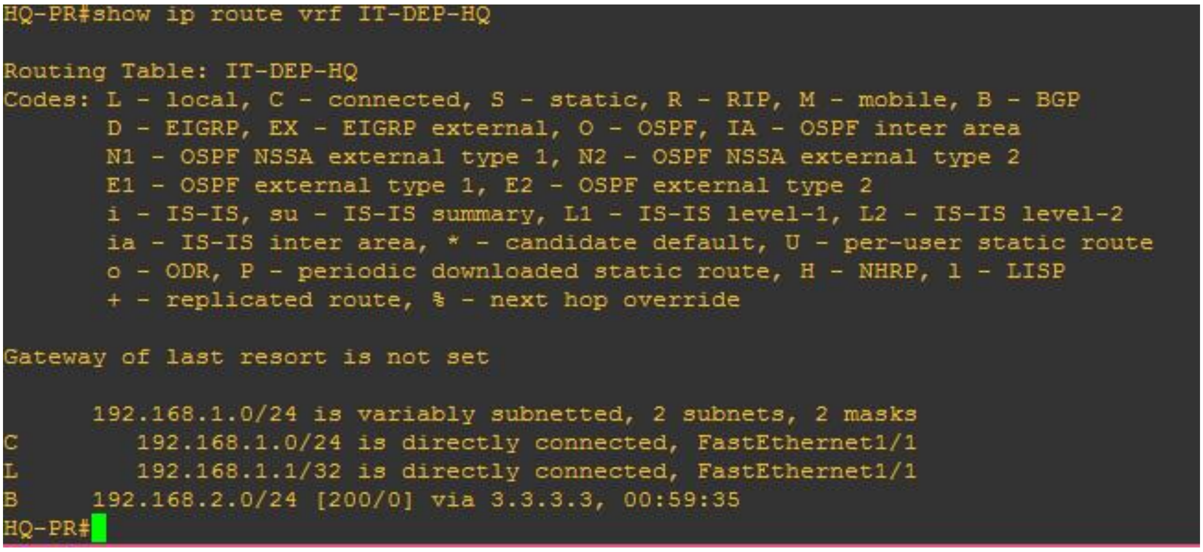
TABLE 1 Configuration of MPLS L3 VPN

HQ-PE	BR-2-PE
HQ-PE (config) #router bgp 64000	**BR-2-PE (config)#router bgp 64000**
HQ-PE (config-router)# neighbor 3.3.3.3 remote-as 64000	**BR-2-PE (config-router)# neighbor 1.1.1.1 remote-as 64000**
HQ-PE (config-router) # neighbor 3.3.3.3 update-source loopback 0	**BR-2-PE (config-router)# neighbor 1.1.1.1 update-source loopback 0**
HQ-PE (config-router)# address-family vpnv4	**BR-2-PE (config-router)# address-family vpnv4**
HQ-PE (config-router-af)# #neighbor 3.3.3.3 activate	**BR-2-PE(config-router-af)# #neighbor 1.1.1.1 activate**
HQ-PE (config-router-af)# #neighbor 3.3.3.3 send-community extende	**BR-2-PE (config-router-af)# #neighbor 1.1.1.1 send-community extended**
HQ-PE (config)# vrf definition IT- DEP-HQ	**BR-2-PE (config)# vrf definition IT- DEP-BR-2**
HQ-PE (config-vrf)# rd 64000:1	**BR-2-PE (config-vrf)# rd 64000:1**
HQ-PE (config-vrf)#address-family ipv4	**BR-2-PE (config-vrf)# address-family ipv4**
HQ-PE (config-vrf-af)#route-target export 64000:1	**BR-2-PE (config-vrf-af)#route-target export 64000:1**
HQ-PE (config-vrf-af)#route-target import 64000:1	**BR-2-PE (config-vrf-af)#route-target import 64000:1**
HQ-PE (config)# interface FA1/1	**BR-2-PE (config)# interface FA1/1**

HQ-PE (config-if)#description connected to IT- DEP-HQ	**BR-2-PE (config-if)# description connected to IT- DEP-BR-2**
HQ-PE (config-if)#ip vrf forwarding IT- DEP-HQ	**BR-2-PE (config-if)#ip vrf forwarding IT- DEP- BR-2**
HQ-PE (config-if)#ip add 192.168.1.1 255.255.255.0	**BR-2-PE (config-if)#ip add 192.168.2.1 255.255.255.0**
HQ-PE (config-if)#no shut	**BR-2-PE (config-if)#no shut**
HQ-PE (config)#router ospf 100 vrf IT-DEP-HQ-PE	**BR-2-PE (config)#router ospf 100 vrf IT-DEP-HQ-PE**
HQ-PE (config-router)#network 192.168.1.0 0.0.0.255 area 0	**BR-2-PE (config-router)#network 192.168.2.0 0.0.0.255 area 0**
HQ-PE (config-router)#router-id 100.100.100.100	**BR-2-PE (config-router)#router-id 101.101.101.101**
HQ-PE (config)# interface FA1/1	**BR-2-PE (config)# interface FA1/1**
HQ-PE (config-if)#ip ospf 100 area 0	**BR-2-PE (config-if)#ip ospf 100 area 0**
HQ-PE (config)# router bgp 64000	**BR-2-PE (config)# router bgp 64000**

VIII. Simulation Results

The results of the simulated scenario of the network are illustrated in Figures 5 to 8, which are obtained from HQ-PE and BR-2-PE



```
HQ-PR#show ip route vrf IT-DEP-HQ

Routing Table: IT-DEP-HQ
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet1/1
L        192.168.1.1/32 is directly connected, FastEthernet1/1
B     192.168.2.0/24 [200/0] via 3.3.3.3, 00:59:35
HQ-PR#
```

Figure 5. Verify of (IT-DEP-HQ VRF Route Table) on HQ-PE

```
HQ-PR#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.1.1.1        YES manual up                    up
FastEthernet1/0        100.100.100.1   YES manual up                    up
FastEthernet1/1        192.168.1.1     YES manual up                    up
FastEthernet2/0        unassigned      YES unset  administratively down down
FastEthernet2/1        192.168.1.1     YES manual up                    up
Loopback0              1.1.1.1         YES manual up                    up
```

Figure 6. Verify of ip address for interfaces on HQ-PE

```
BR-2-PE#show ip route vrf IT-DEP-BR-2

Routing Table: IT-DEP-BR-2
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B      192.168.1.0/24 [200/0] via 1.1.1.1, 01:02:13
       192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.168.2.0/24 is directly connected, FastEthernet1/1
L         192.168.2.1/32 is directly connected, FastEthernet1/1
BR-2-PE#
```

Figure 7. Verification of IT-DEP-BR-2 VRF Route Table on BR-2-PE

```
BR-2-PE#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.3.3.1        YES manual up                    up
FastEthernet1/0        100.100.100.3   YES manual up                    up
FastEthernet1/1        192.168.2.1     YES manual up                    up
FastEthernet2/0        unassigned      YES unset  administratively down down
FastEthernet2/1        192.168.2.1     YES manual up                    up
Loopback0              3.3.3.3         YES manual up                    up
BR-2-PE#
```

Figure 8. Verification of ip addresses for BR-2-PE interfaces

IX. Conclusion

MPLS L3 VPN is applied between two sites which are HQ and Branch-2. Creation of two VRFs in each provider edge router with same IPs and subnet mask without any overlap between these interfaces, when connected to switches. The use of VRF in MPLS networks causes the PE routers to create a virtual routing table for each customer and route the traffic for each VRF separately. Simulated topology shows that VRFs are routed between PE routers by the MP-BGP protocol.

References

[1] Steven Smith, “Introduction to Multiple Protocol Label Switching”, Cisco Networking symposium, 2003.
[2] Luc De Ghein, “MPLS Fundaments”, Cisco Press, 2007.
[3] Russ White, Danny McPherson, Srihari Sangli, “Practical BGP”, Published Jul6, 2004, Addison Wesley Professional.
[4] Luc De Ghein, “MPLS Fundaments”, Cisco Press, 2007.
[5] Cisco IOS XR Virtual Private Network Configuration Guide for the Cisco CRS Router, Release 6.1.x. First Published: 2016-11-01.
[6] MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS Release 15M&T First Published: 2012-11-21 Last Modified: 2013-03-15.
[7] Narbik Kocharians, Peter Paluch, “ CCIE Routing and Switching v5.0”, Official Cert Guide, Volume 1, 5th Edition, 2014 by Cisco Press.
[8] Jim Guichard, Ivan Pepelnjak and Jeff Apcar, "MPLS and VPN Architectures", Cisco Press, Volume 2, 2003
[9] MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS XE Release 3S, 2018.