

Traffic Engineering, QoS and MP-BGP VPNs in MPLS Networks

M. Zeeshan Gondal¹, M. Junaid Arshad² and Husnain Ahmad³

^{1,2}Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan

³Virtual University (VU), Lahore, Pakistan

Abstract– In the recent past there have been an enormous growth in the use of Internet, and new real time connection oriented services like streaming technologies, transaction based services are in use and a lot of new ones are currently rising. As these new areas of services are becoming more and more important in field of networks, to ensure QoS in these fields has become more important than ever MPLS, which combine the Layer 2 and Layer 3 technologies, provide the ability to best control over traffic engineering, fast recovery in case of network failure, VPNs and tight QoS, offer guarantee service for all type of applications. The MPLS is most prominent back bone protocol adopted by most of the service providers. Our main goal of research work is to thoroughly understand MPLS with industry prospective and analyze its different applications, with emphasis on MPLS VPNs, and aspects with help of simulations in state of the art CISCO simulator GNS3.

Keywords– MPLS (Multi Protocol Label Switching), TE (Traffic Engineering), MP-BGP (Multi Protocol Border Gateway Protocol), CEF (Cisco Express Forwarding), VRF (Virtual Routing and Forwarding), RD (Route Distinguisher) and RT (Route Target)

I. INTRODUCTION AND PROBLEM STATEMENT

The initial and basic purpose of our research work is to provide a platform that will discuss MPLS applications particularly Traffic Engineering and MPLS VPNs. We are intended to gather all these areas on one platform. Before our work, different fields are discussed but at different places. And regarding Implementations, We will implement MPLS and explore its behavior and see label forwarding between nodes. MPBGP MPLS VPNs would be implemented supported with in depth configuration details and their corresponding outputs. Also the inter area problem in VPNs will be defined and eliminated using sham link. Complete study, discussion and implementation on Traffic Engineering would be provided. By keeping in mind industry scope we will implement major MPLS application on one platform.

A) Traffic Engineering

In Traditional IP network routing protocols follow SPF (Shortest path First algorithms) to converge their routing table. Furthermore all traffic will follow these paths. Routing protocol's robustness made end users transparent to any fault

occur. For example TCP/IP network adjusts its traffic flow after re-calculations and adjusting its routing table. Congestion occurs because all traffic will follow through the shortest path computed by routing protocols while other link which is available will be under used. In case of delay sensitive and high reliability demanding traffic like VoIP and streaming follow the same congested (because this is shortest) path will severely damage overall quality of service of network.

This can be seen from Fig. 1 that short path from R1 to R5 is (R1-R3-R5). Whole traffic destined to R5 will follow this path even an alternate route (R1-R2-R4-R5) is available which can be used for load balancing. The process of how traffic flow in network in controlled fashion and provide optimal use of resources hence increase network efficiency is called Traffic Engineering. MPLS can provide better resource usage and increase performance as compare to IP network. Paths can be reserve for delay sensitive and critical traffic and those nodes or links can be assigned to such traffic which is more reliable. In this way traffic can be routed in more controlled way and hence cause performance upgrade. Previously most of the works define theoretical concepts of MPLS Traffic Engineering. On the basic of concepts defined about TE we will also implement the Traffic Engineering in MPLS domain and highlight its working characteristics using providing outputs in different scenarios.

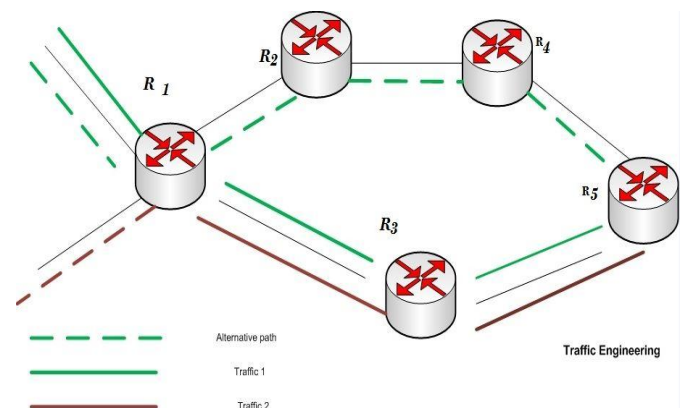


Fig. 1: MPLS Traffic Engineering

B) MPBGP MPLS VPNs

Drawback of Over Lay type of VPN was that, service provider was unaware of customer ip schemes and whole service provider network was transparent to customers. This is called overlay because customer need to establish another network, which can be of any layer, over service provider network. For example in L1 Customer borrows lease lines from SPs (Service providers) and over those lines customer can build L2, L3 network of their own choice. In L2 SP provide L2 cloud for example Frame-Relay, PVC's etc.

In L3 Customer build L3 network over SP's L3 network using GRE Tunnels. In this type of VPN Customer address space would not overlap and SP does not know what information is exchanging in above customer overlay network. Over Lay VPNs were easy to implement but suffer

sub-optimal routing issue. In peer to peer type of VPN now SP have complete information about customer networks so routing was optimal. But managing customer routes and avoiding overlapping of same ip schemes from different customers was very much difficult and complicated. MPLS VPNS combine positive aspects of both techniques that are optimal routing and ease to implement. MPLS VPNs are by peer to peer by nature. On basis of these evolutions we decide to implement MPBGP MPLS VPNs. During implementation we identify few problems and provide successful solutions to them. First was inability of simple BGP to carry VPNv4 routes and second was Inter Area OSPF issue as shown in Fig. 2. We successfully provide solutions to both of problems and implement them.

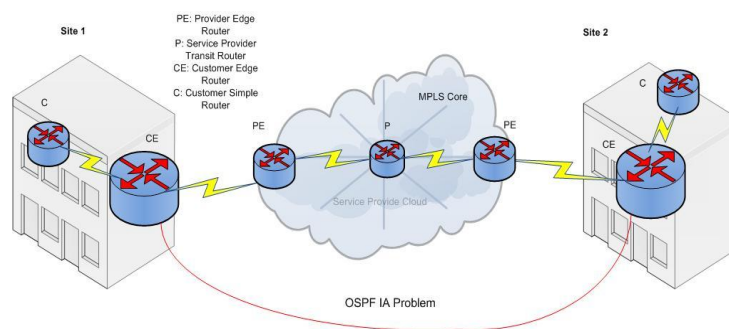


Fig. 2: MPLS VPNs

Previously most of the works define theoretical concepts of MPLS Traffic Engineering. On the basic of concepts defined about TE we will also implement the Traffic Engineering in MPLS domain and highlight its working characteristics using providing outputs in different scenarios. We will implement MPBGP MPLS VPNs. During implementation we identify few problems and provide successful solutions to them. First was inability of simple BGP to carry VPNv4 routes and second was Inter Area OSPF issue. We will provide solutions to both of problems and implement them. Rules and different model for implementing Qos for MPLS will also be discussed.

II. PROPOSED WORK

A) Simulations Environments

We choose GNS3 for our work because it is open source and supports real Cisco routers operating systems. It's a process intense simulator and can support emulate topologies. It supports almost most of the commands. GNS is robustly

connected with:

- Dynamips (Cisco IOS emulator)
- Dynagen (Front end for Dynamips, text-based)
- Qemu (open source ,generic and machine virtualizer & emulator)
- VirtualBox (Free and Strong virtualization software)

And provide precise simulations.

B) MPLS Design

First of all we made simple MPLS operational topology as shown in Fig. 3 in GNS3. After basic configurations like IP addresses on interfaces, loop backs as mentioned in topology we run OSPF as IGP for our scenario. MPLS core cloud identifies the MPLS capable nodes. Now MPLS will run on interfaces those are present within the MPLS core region. CEF (Cisco Express Forwarding) is a Cisco proprietary switching technique for MPLS. By default CEF is in running state but it's better to hardcoded it using command:

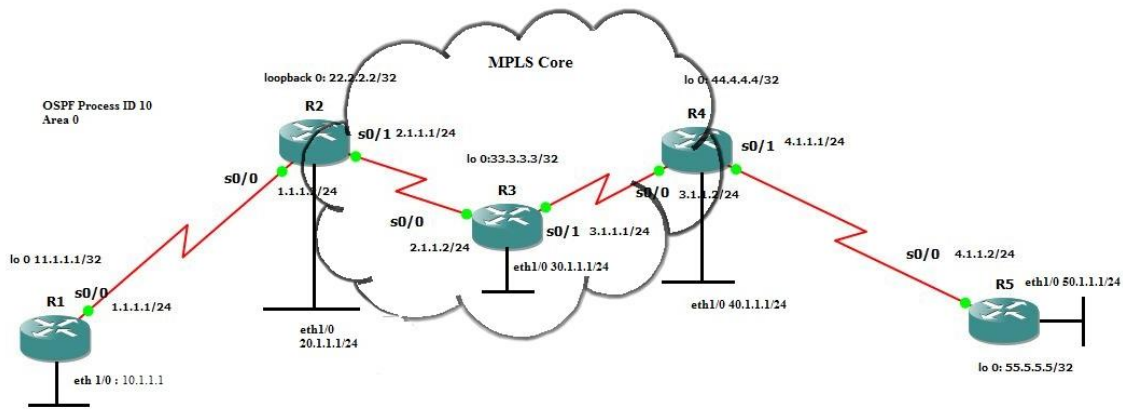


Fig. 3: GNS3 MPLS Topology

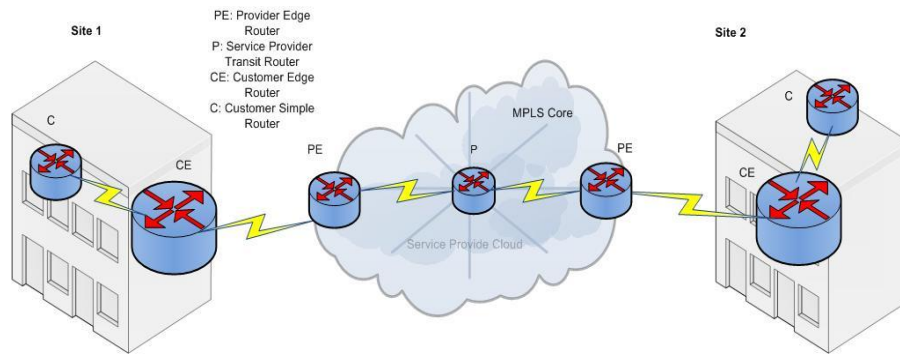


Fig. 5: MPLS VPNs

#ip cef

We used LDP as Label Distribution protocol and enable it using command

mpls label protocol ldp

Loopbacks are used as mpls router ids. To enable MPLS on all the desired interfaces we use following command

#mpls ip

With these configurations MPLS will start working in our described topology and all the concepts regarding label distribution, label swapping and packets forwarding can be observed.

C) MPBGP MPLS VPNS Implementations

MPLS VPNS combine positive aspects of both techniques that are optimal routing and ease to implement. MPLS VPNs are by peer to peer by nature shown in Fig. 5.

There are four important concepts used to separate customer routes:

- VRF Virtual Routing and Forwarding
- RD Route Distinguisher
- RT Route Target
- VPN Label Attribute

VRF Virtual Routing and Forwarding

Suppose similar IP schemes are being use in two different customer sites and they are using same service provider network. It's SP responsibility to keep them separate. For this purpose VRFs are used. Each Customer has its own VRF in adjacent PE router. Service provider keeps its own routing information in Global Routing Table while assign different VRFs to each customer. An interface cannot be a part of multiple VRFs while multiple interfaces can be part of one VRF. For each VRF there is separate routing table.

Route Distinguisher

When PE need to advertise these VRFs routes there is again threat that these routes can be intermixed. To prevent this 3rd concepts is used which is Route Distinguisher (RD). 64 bit value attached to network id so address will be now of

32+64= 96 Bits. PE assigns unique RD to each VRF in unique pattern given below for example 1:1 where first 1 is service provider Autonomous System Number while second 1 is customer number.

BGP (IBGP) as IGP. Huge Routing information is coming on PE router in that case simple IGP protocols could not carry this much load of routing traffic so in such case BGP is used which can support heavy traffic. Only Edge Routers need to implement BGP. This is why core is called BGP Free Core because Transit core routers have no need to implement BGP. New 96 bits value is called VPNv4 Route for MPLS special version of BGP is used which is called MPBGP (Multi Protocol BGP). Because simple BGP can only carry IPv4 traffic While MPBGP can carry IPv4, IPv6, and VPNv4, VPNv6 traffic.

Route Target

RT is an extended community attribute for BGP attach with VPNv4 routes, used to assign routes to their specific VRFs on Receiving PE side. RTs are assigned as 1:1, 1:2. Multiple RTs can be used. There are two types of RTs: i) IMPORT RT, ii) Export RT. Export RT must be configured on receiving side as export RT. Generally both are same.

VPN Label attributes

This is another extended community attribute use to carry VPN label information. PE will advertise it too along with RT. There will be two labels in use now. One is Simple MPLS Label second VPN label through the core.

Implementation of MPLS VPNs

According to topology Basic, OSPF and MPLS in Core Configurations are already been made. Now we will configure VPNs. Since configurations are complicated, for better understanding we will divide these configurations into following 4 steps:

- Step#1 VRF Related Configurations
- Step#2 MPBGP Related Configurations
- Step#3 PE to CE Routing Configurations
- Step#4 Re-Distributions

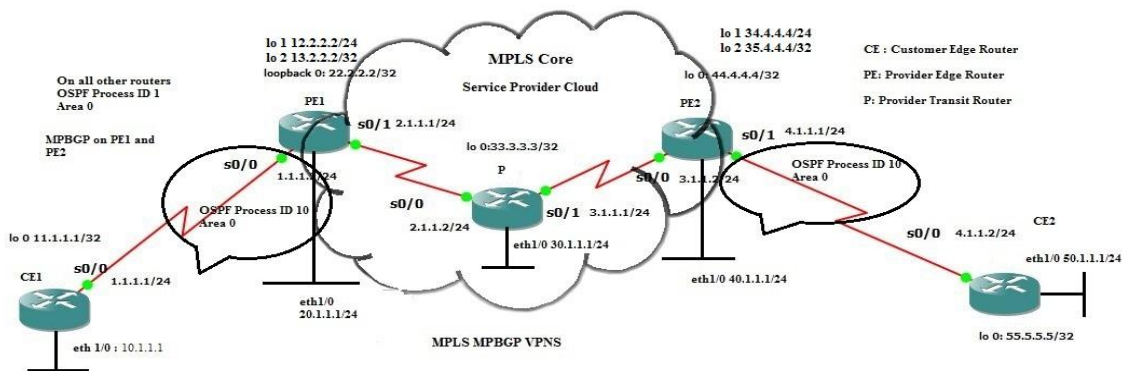


Fig. 6: MPLS VPNs GNS3 Topology

Step 1 VRF Related Configurations

VRF Related Configurations will be implemented on both PEs routers i.e., PE1 and PE2 as shown in Fig. 6. In these configurations we will define VRFs, Route Distinguishers (RDs) and Route Targets (RTs). After these configurations, the interfaces adjacent to customers’ sites will be assigned to defined VRF.

Step 2 MPBGP Related Configurations

In this step of configurations again our focused nodes will be PE1 and PE2. Initially we will run simple BGP. Since BGP couldn’t carry VPNv4 routes so we have to modify simple BGP to MPBGP. Which require additional steps of address

family definition and sending of community attributes. Also the neighbor which is PE2 for PE1 and vice versa will be activated. In BGP configurations mode

```
#address-family vpnv4
```

Above command is used to make BGP capable of carrying VPNv4 routes.

```
#neighbor 44.4.4.4 active
(Neighbor for PE1)
```

Above command is used to activate neighbor.

```
#neighbor 44.4.4.4 send-community both (RT and VPN Label)
```

Above Command is used to enable forwarding of community attributes. Same Configurations will implement on both PE1 and PE2.

Step 3 PE to CE Routing Configurations

PE1 to CE1 Configurations

We have to run ospf between customer and service provider with different process id keep them isolated with each other.

```
#router ospf 10 vrf uet
```

Will be used for different process OSPF and also make this part of VRF, we have defined. Same configurations on both PE1 and PE2

Step 4 Re-Distributions

Same Re-distributions steps will be followed on PE1 and PE2. PE2 configurations are given below.

To Re-distribute OSPF routes on MPBGP we have to use another address family i.e., IPv4. Following command will be used for this purpose, in the configuration mode for BGP:

```
#address-family ipv4 vrf uet
#redistribute ospf 10 match internal external
```

After Re-distribution we will see in below figures that routes are successfully transferring between PEs but still not forwarding to CEs. To solve this issue we have to invert that process that now BGP will converge in to OSPF so that routes can forward to CEs Routers. Following commands will be used on both PEs Routers.

PE1 Router

```
Router(config)#router ospf 10
Router(config-router)#redistribute bgp1 subnets
```

PE2 Router

```
Router(config)#router ospf 10
Router(config-router)#redistribute bgp1 subnets
```

After these commands routes will converge between CEs. Outputs are given below in Fig. 7 and Fig. 8.

```

CE1 - SecureCRT
File Edit View Options Transfer Script Tools Help
| CE1 | PE1 | P | PE2 | CE2
Router#
Router#
Router#
Router#
Router#
Router#sh ip route
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

      1.0.0.0/24 is subnetted, 1 subnets
        C       1.1.1.0 is directly connected, Serial0/0
      50.0.0.0/24 is subnetted, 1 subnets
        O IA    50.1.1.0 [110/138] via 1.1.1.2, 00:01:44, Serial0/0
      4.0.0.0/24 is subnetted, 1 subnets
        O IA    4.1.1.0 [110/65] via 1.1.1.2, 00:01:44, Serial0/0
      55.0.0.0/32 is subnetted, 1 subnets
        O IA    55.5.5.5 [110/129] via 1.1.1.2, 00:01:44, Serial0/0
      10.0.0.0/24 is subnetted, 1 subnets
        C       10.1.1.0 is directly connected, Ethernet1/0
      11.0.0.0/32 is subnetted, 1 subnets
        C       11.1.1.1 is directly connected, Loopback0
Router#

```

Fig. 7: CE1 Routing Table

```

CE2 - SecureCRT
File Edit View Options Transfer Script Tools Help
| CE1 | PE1 | P | PE2 | CE2

Router>
Router>
Router>
Router>en
Router#
Router#sh ip ro
Router#sh ip route
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

CE1 Routes start converging in
CE2 showing as IA

O IA 1.0.0.0/24 is subnetted, 1 subnets
    11.1.1.0 [110/65] via 4.1.1.1, 00:01:51, Serial0/0
C   50.0.0.0/24 is subnetted, 1 subnets
    50.1.1.0 is directly connected, Ethernet1/0
C   4.0.0.0/24 is subnetted, 1 subnets
    4.1.1.0 is directly connected, Serial0/0
C   55.0.0.0/32 is subnetted, 1 subnets
    55.5.5.5 is directly connected, Loopback0
O IA 10.0.0.0/24 is subnetted, 1 subnets
    10.1.1.0 [110/138] via 4.1.1.1, 00:01:51, Serial0/0
O IA 11.0.0.0/32 is subnetted, 1 subnets
    11.1.1.1 [110/129] via 4.1.1.1, 00:01:51, Serial0/0
Router#
Router#
Router#

```

Fig. 8: CE2 Routing Table

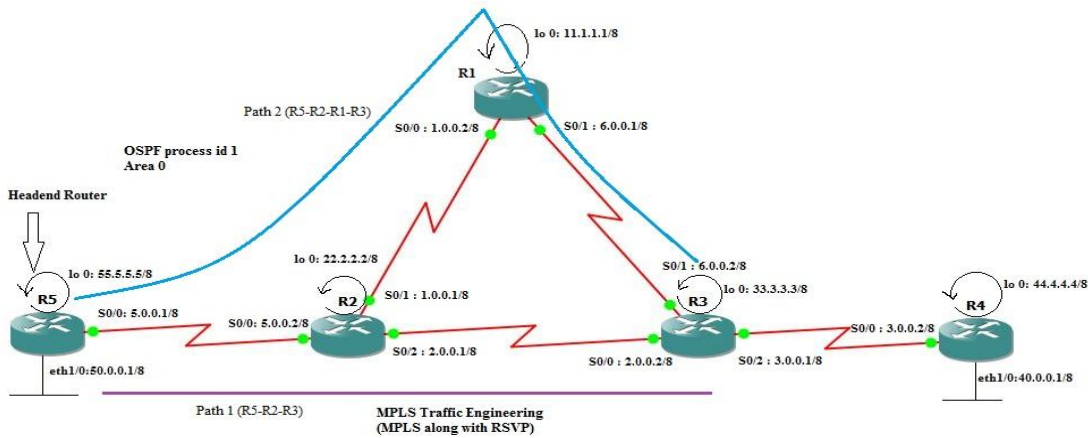


Fig. 9: Traffic Engineering Topology

```

R5 - SecureCRT
File Edit View Options Transfer Script Tools Help
| R5 | R2 | R1 | R3 | R4

Router#
Router#
Router#mpls tra
Router#mpls traffic-eng re
Router#mpls traffic-eng reoptimize
Router#sh mpls traffic-eng tunnels tunnel 1
We have to re-optimize to activate path defined.

Name: Router_t1
Status: up (Tunnel1) Destination: 33.3.3.3
Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit uet (Basis for Setup, path weight 192)
path option 20, type dynamic explicit tunnel is up now

Config Parameters:
Bandwidth: 256 kbps (Global) Priority: 4 3 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: disabled Lockdown: disabled Loadshare: 256 bw-based
auto-bw: disabled

InLabel : serial0/0, 17
OutLabel :
RSVP Signalling Info:
src 55.5.5.5, dst 33.3.3.3, Tun_Id 1, Tun_Instance 5
RSVP Path Info:
My Address: 55.5.5.5
Explicit Route: 5.0.0.2 1.0.0.2 6.0.0.2 33.3.3.3 Path followed
Record Route: NONE
TSpec: ave rate=256 kbits, burst=1000 bytes, peak rate=256 kbits
RSVP Res: Info:
Record Route: NONE
Espec: ave rate=256 kbits, burst=1000 bytes, peak rate=256 kbits
Shortest unconstrained Path Info:
Path weight: 128 (TE)
Explicit Route: 5.0.0.2 2.0.0.2 33.3.3.3
History:
Tunnels:
Time since created: 19 minutes, 50 seconds
Current LSP:
Uptime: 13 seconds
Selection: reoptimization
Priority:
ID: path option 20 [2]
Removal Trigger: reoptimization completed
Router#
Ready

```

Fig. 10: Tunnel View

Traffic Engineering Implementations

In Traffic Engineering we have to change default routing protocol behavior and directs it to follow path we defined as shown in Fig. 9. Five steps to be followed implementing TE.

1. Generally routing protocol take routing decision on based of its metric, cost for example in case of OSPF. Here we will direct routing protocol to carry some other attributes as well along with its metric and now the routing decision will be based upon all of these attributes. So in first step will define these attributes.
2. We will make routing protocol capable to carry these attributes.
3. On each router now the path selection will be based upon these attributes.
4. Ensure that candidate path provide end to end bandwidth provisioning. We will use RSVP here instead of LDP because RSVP supports TE. RSVP request message follow through each router and its reply with resv message will reserve path where attributes conditions meet.
5. We will decide which traffic will follow from different paths.

Results

Fig. 10 shows the re-optimization process and related output as well.

Although Tunnel is created and up now but still it would not appear in routing table in R5. For that we have to announce that tunnel in tunnel configuration mode i.e.,

```
Router(config)#int tu 1
```

```
Router(config-if)#tunnel mpls traffic-eng autoroute announce
```

Tunnel creation and Traffic Engineering configurations completed. Now we will explore this by using traceroute command and view routing table as well in Fig. 11 and Fig. 12.

D) MPLS QoS Implementation Rules

There are 5 rules for MPLS QoS default behavior:

Rule # 1

Precedence bits of incoming packet are copied to the experimental bits of MPLS label being imposed.

Rule# 2

Experimental bits of incoming label packet are copied to the experimental bits of the swapped or imposed label.

Rule # 3

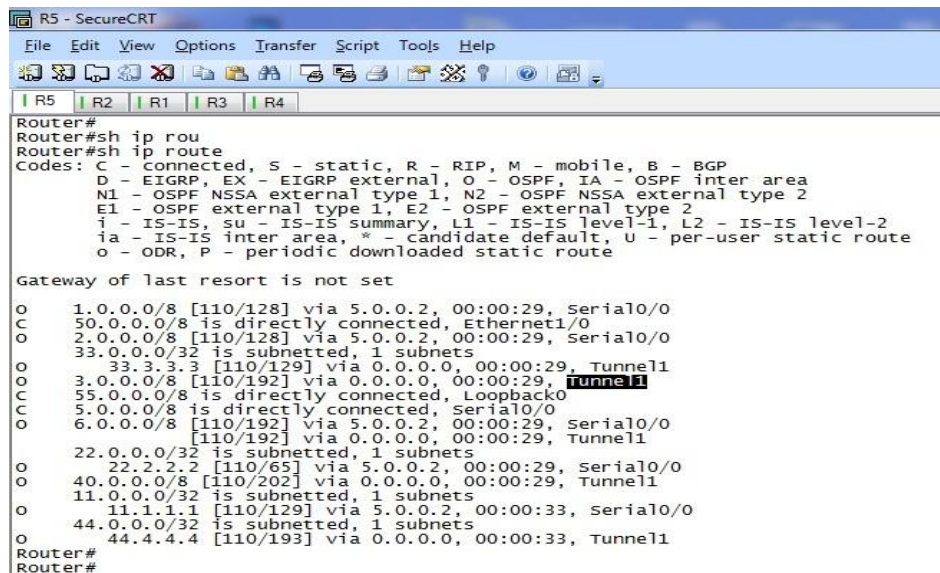
Experimental bits of the incoming label are not copied to the experimental bits of outgoing label when the label is being popped or disposed.

Rule # 4

Experimental bits of incoming label are not copied to the precedence bits of outgoing ip packet

Rule # 5

If the value of experimental bits is changed during transition through mpls domain only the top most label value is changed.



```

R5 - SecureCRT
File Edit View Options Transfer Script Tools Help
R5 R2 R1 R3 R4
Router#
Router#sh ip rou
Router#sh ip route
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

O    1.0.0.0/8 [110/128] via 5.0.0.2, 00:00:29, Serial0/0
C    50.0.0.0/8 is directly connected, Ethernet1/0
O    2.0.0.0/8 [110/128] via 5.0.0.2, 00:00:29, Serial0/0
O    33.0.0.0/32 is subnetted, 1 subnets
O    33.3.3.3 [110/129] via 0.0.0.0, 00:00:29, Tunnel1
O    3.0.0.0/8 [110/192] via 0.0.0.0, 00:00:29, Tunnel1
C    55.0.0.0/8 is directly connected, Loopback0
C    5.0.0.0/8 is directly connected, Serial0/0
O    6.0.0.0/8 [110/192] via 5.0.0.2, 00:00:29, Serial0/0
O    [110/192] via 0.0.0.0, 00:00:29, Tunnel1
O    22.0.0.0/32 is subnetted, 1 subnets
O    22.2.2.2 [110/65] via 5.0.0.2, 00:00:29, Serial0/0
O    40.0.0.0/8 [110/202] via 0.0.0.0, 00:00:29, Tunnel1
O    11.0.0.0/32 is subnetted, 1 subnets
O    11.1.1.1 [110/129] via 5.0.0.2, 00:00:33, Serial0/0
O    44.0.0.0/32 is subnetted, 1 subnets
O    44.4.4.4 [110/193] via 0.0.0.0, 00:00:33, Tunnel1
Router#
Router#

```

Fig. 11: Routing Table with Tunnel interface

```

R5 - SecureCRT
File Edit View Options Transfer Script Tools Help
R5 | R2 | R1 | R3 | R4
Router#
Router#
Router#
Router#
Router#trace
Router#traceroute 2.0.0.2
Type escape sequence to abort.
Tracing the route to 2.0.0.2
  1 5.0.0.2 40 msec 68 msec 44 msec
  2 2.0.0.2 28 msec 72 msec *
Router#
Router#
Router#
Router#
Router#
Router#traceroute 44.4.4.4
Type escape sequence to abort.
Tracing the route to 44.4.4.4
  1 5.0.0.2 [MPLS: Label 17 Exp 0] 68 msec 56 msec 92 msec
  2 1.0.0.2 [MPLS: Label 16 Exp 0] 36 msec 104 msec 40 msec
  3 6.0.0.2 84 msec 68 msec 60 msec
  4 3.0.0.2 84 msec 84 msec *
Router#
Router#
Router#

```

Since 2.0.0.2 is before tunnel terminate point so for this path no need to follow explicit tunnel. Dynamic path will be followe

Tough for this destination Explicit Tunnel will be followed. We can see the Path followed.

Fig. 12: Traceroute

MPLS QoS Models

There are 3 MPLS QoS models that can be implemented using above 5 rules.

1. Pipe Model
2. Short Pipe Model
3. Uniform Model

Pipe Model

- i. At ingress router incoming ip packet's precedence value may or may not be copied.
- ii. At Transit P router value will be copied (default behavior).
- iii. QoS decision will be based on experimental bits of label.

Short Pipe Model

- i. At ingress router incoming ip packet's precedence value may or may not be copied.
- ii. At Transit P router value will be copied (default behavior).
- iii. QoS decision will be based on precedence bits of ip packet.

Uniform Model

- i. At ingress router incoming ip packet's precedence value must be copied.
- ii. At Transit P router value will be copied (default behavior).
- iii. At Egress router incoming labeled packet's experimental value must be copied to outgoing ip precedence field. If value changed, the change will forward out.

IV. CONCLUSIONS

We successfully implemented MPLS and explore its behavior and see label forwarding between nodes. MPBGP MPLS VPNs are successfully implemented supported with in depth configuration details and their corresponding outputs. Traffic Engineering is also being studied, discussed and implemented to best of possible effort. QoS Rules and models have been discussed. There are lot of areas when still work can be proceed for example regarding implementations in our thesis we have defined QoS default behavior which can be implanted. Also the recovery models we have discussed can also be implemented using traffic engineering but for that may require original equipment. Because there was no fast re-route configuration option in GNS3. Regarding research SDN is hot topic now a day.

REFERENCES

- [1] Winter, R., "The coming of age of MPLS," Communications Magazine, IEEE , vol.49, no.4, pp.78,81, April 2011
- [2] Chang Cao; Yongjun Zhang; Jie Zhang; Xiaofei Cheng; Wanyi Gu, "Packet-Level Optimization for Transmission Performance Improvement of Internet-Bound Traffic in a MPLS-TP Network," Optical Communications and Networking, IEEE/OSA Journal of , vol.2, no.11, pp.991,999, November 2010.
- [3] Alarcon-Aquino, V.; Minero-Munoz, M., "Path Restoration Schemes for MPLS Networks," Potentials, IEEE , vol.30, no.2, pp.22,28, March-April 2011
- [4] Anjali, T.; Scoglio, C.; de Oliveira, J.C., "New MPLS network management techniques based on adaptive learning," Neural Networks, IEEE Transactions on , vol.16, no.5, pp.1242,1255, Sept. 2005
- [5] Dongmei Wang; Guangzhi Li, "Efficient Distributed Bandwidth Management for MPLS Fast Reroute," Networking, IEEE/ACM Transactions on , vol.16, no.2,

- pp.486,495, April 2008
- [6] Cohen, R.; Nakibly, G., "Maximizing Restorable Throughput in MPLS Networks," *Networking, IEEE/ACM Transactions on* , vol.18, no.2, pp.568,581, April 2010
 - [7] Kompella, R.R.; Yates, J.; Greenberg, Albert; Snoeren, A.C., "Fault Localization via Risk Modeling," *Dependable and Secure Computing, IEEE Transactions on* , vol.7, no.4, pp.396,409, Oct.-Dec. 2010
 - [8] Oommen, B.J.; Misra, S.; Granmo, O.-C., "Routing Bandwidth-Guaranteed Paths in MPLS Traffic Engineering: A Multiple Race Track Learning Approach," *Computers, IEEE Transactions on* , vol.56, no.7, pp.959,976, July 2007
 - [9] Salam, S.; Sajassi, A., "Provider backbone bridging and MPLS: complementary technologies for next-generation carrier ethernet transport," *Communications Magazine, IEEE* , vol.46, no.3, pp.77,83, March 2008
 - [10] Lillian Goleniewski "Telecommunications Essentials" ISBN 978-81-317-1192-7
 - [11] E. Rosen, A. Viswanathan, R.Callon "Multiprotocol Label Switching Architecture (RFC 3031)" <http://www.ietf.org/rfc/rfc3031.txt> January 2001
 - [12] Fenglin Li; Jianxun Chen, "MPLS Traffic Engineering Load Balance Algorithm Using Deviation Path," *Computer Science & Service System (CSSS), 2012 International Conference on* , vol., no., pp.601,604, 11-13 Aug. 2012