Data Networks' Design and Optimization through MPLS VPNs using BGP

Mohammad Junaid Arshad [1], Tauqir Ahmad [2], Amjad Farooq [3]

[1, 2, 3] Department of Computer Science & Engineering, University of Engineering and Technology
Lahore, Pakistan
junaidarshad@uet.edu.pk

Abstract: The key strong points of the Internet have been its vast scalability and flexibility to provide accommodation to the variety of applications. In this context, MPLS (Multi Protocol Label Switching) is the newest technology being employed today's in the Internet core, which is continuously growing to meet the increasing demands of bandwidth and connectivity. In this research work, we provide a survey of MPLS, BGP (Border Gateway Protocol) and both layer-2 and layer-3 VPNs (Virtual Private Networks). We address the issues (such as speed, scalability and security) of traditional IP-based VPNs. Since layer-2 VPNs are efficient but not so intelligent and scalable, while layer-3 VPNs are intelligent and scalable but not so efficient. Thus, we propose a new design scheme for MPLS/BGP-VPNs in such a way that the features of layer-3 as scalability and intelligence are merged with the efficiency of layer-2 to deal with today's evolving demands of speed, scalability and security. The proposed design of optimized data networks through MPLS/BGP-VPNs is implemented in Dynagen simulator for the better understanding the system. This research work will be helpful for adding new security features in core networks in future and provides a guideline for network engineers towards the world of network security. [Journal of American Science. 2010;6(12):88-95]. (ISSN: 1545-1003).

Keywords: BGP-Border Gateway Protocol, MPLS-Multi Protocol Label Switching, QoS-Quality of Service and VPN-Virtual Private Network

1. Introduction

The purpose of this work is to analyze and identify the features and advanced requirements of core networks (i.e., MPLS/BGP-VPNs (Previdi, 2000)). MPLS/BGP-VPNs aim to provide secure, reliable and consistent communication. Some of the aspect of the world most popular core networks design is miserably handled and due to which they are being compromised time after time.

MPLS aim to provide enhanced Traffic Engineering (TE) (Awduche, 1999) mechanisms for IP-based networks to facilitate the ISPs for capably monitoring, assessing and fulfilling a variety of service provisions all through their networks backbone. Like L3-VPN PE-based (Rosen et al., 1999) technology, MPLS/BGP-VPN employs BGP for VPN routes advertisement and utilizes MPLS to send VPN packets over the provider backbone networks. MPLS/BGP-VPN has flexible networking modes, good extensibility and convenient support for MPLS QoS (Lee et al., 2003) and MPLS TE (Swallow, 1999), that's why it is extensively employed.

When building a VPN (Ferguson et al., 1998) based on p-to-p overlays, connection-oriented (like ATM or frame relay, tunneling-on-IP techniques) scalability is a main problem, while VPNs based on MPLS are used to address scalability issues (as they are purely designed on the basis of connection-less, peer-based architecture). Since, a customer-site in a peer-based architecture requires the peer simply within a single provider-edge router in place of the entire customer-edge/provider-edge routers which are associated with the VPN that results in the reduction of large number of VCs. In addition, MPLS-based VPNs naturally use connectionless approach. The Internet is to be obliged its worth to its fundamental approach which is based on connection-less, packet-switching network topology (i.e., TCP/IP). Thus, it does not require any prior act to make association possible in a flexible and useful way among the hosts. In an IP-based connection-less setup the traditional VPNs require initial connection establishment process over p-to-p, connection-oriented overlay networks. When it utilizes under a connection-less environment it still can not get benefit from the connection simplification and service expandability offered by connection-less network. In contrast, if a connection-less VPN is built, to guarantee the network privacy the use of tunnels and encryptions are not required, hence it eliminates the considerable complications.

In this work, the basic goal is also to highlight drawbacks in traditional IP-based VPNs (Callon, 2002) and show how MPLS/BGP VPNs (Alawieh et al., 2008) are used to handle these issues. The conventional IP VPNs in core networks have the following issues:

- **Quality of Service (QoS) Problem**

IP-based applications do not have any straight mechanism to state QoS, as many users and clients are uneasy with independently desirable QoS, because it requires extra charging on behalf of additional QoS category adopted. The regulations for policy managing to create QoS are achievable which are related to customers, servers and associations; however, the dilemma is the volume of the organization tasks. A better policy in simple is to give the matter of QoS headed for the whole VPN (e.g., the working of an ATM/frame-relay network etc). But it is hard to do this through IP-based services, for the reason that the OSPF protocols utilized for constructing routing table cannot share QoS statistics, in other words information concerning resource utilization of the specified trunks or nodes.

- **Scalability Problem**

A very large number of associations can be easily supported by a huge VPN network, and lots of millions can be easily supported by the Internet. So it requires a huge number of VCs which generally makes the process so weak. When every service-link-toward-partner relation is evaluated onto a VC, then the networks having C links of service will generate C(C-1)/2 VCs.

- **Security Problem**

Conventional IP-based Virtual Private Networks (VPNs) have been broadly employed all over the world for remote connectivity; however they are usually vulnerable by multifarious client software and complexities in handling the health position of remote clients. A lot of worms and viruses broadcast through these abandoned VPN endpoints causing destruction of the internal security of the networks. Thus with the Internet, one of the most important issue is the VPN's security, particularly for those which depend upon the publicly designed Internet used for transportation. The IP-based network (unlike ATM/frame relay or private-line services) doesn't allocate the constant logical/physical pipes to the special sites, applications or protocols. To address the Internet security, IPSec (Davis, 2001) is the latest IETF (Internet Engineering Taskforce) solution that was initially proposed for the IPv6 (Deering et al., 1998) protocol; however, it has been used in the current's IPv4 networks. Since, it describes a framework for giving a powerful security in support of network transport over the IP-based environments.

1.1 Contribution and Scope of the Proposed System

To meet high-level demands of security and efficiency in the backbone networks, MPLS aim to offer advanced IP network TE mechanisms these will facilitate the ISPs for easily evaluating, examining and meeting a variety of their service necessities a-cross the backbone. By the use of intelligent routers and speedy switches MPLS provides a technique for mapping IP segments with connection-based transport (such as frame relay or ATM) more efficiently. This supports the QoS definition inside the header of MPLS (Rosen et al., 2001; Rosen et al., 1999) as well. Using routing statistics of layer 3, MPLS distributes resources and builds forwarding tables for routing, while it utilizes layer 2 for switching or forwarding the information through the right link or route. Each IP packet includes a label of MPLS which is subsequently linked with a specific entry inside the forward routing table that identifies the upcoming hop. The network-flows with similar requirements for level of service and routing decisions, commonly keep the same pathway/route across the network resulting in a consistency of service-level for network-flows which having higher priority. MPLS is required to deploy the Label Switching Routers (Das et al., 2003) in the networks that will affect the momentum whereupon MPLS based solution is deployed. At the moment, MPLS is at target in favor of deployment in the backbones first.

We have implemented the MPLS/BGP VPNs in such a way that the features of layer 3 as scalability and intelligence are merged with the efficiency of layer 2 to cope up with almost all modern demands of speed, scalability and security. The proposed MPLS/BGP VPN design is implemented in Dynagen simulator (Dynagen, 2007) for easily understanding the system. Dynagen simulator is easily available and supports variety of network designs. In the proposed system five routers are used in which two routers belong to customer network and the rest belong to MPLS core network. BGP is used for route

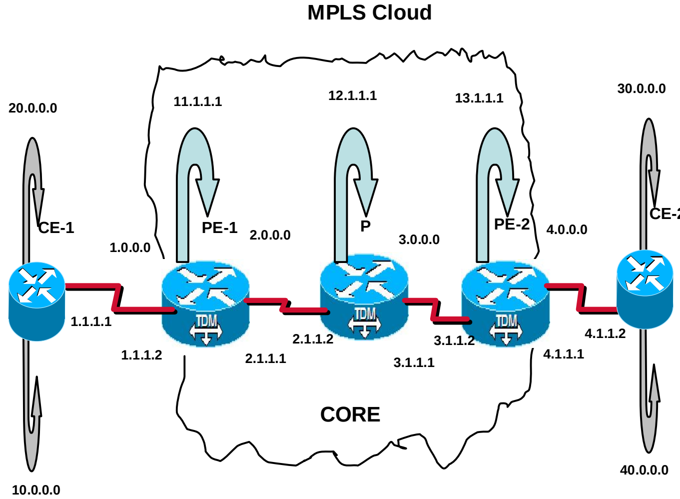


Figure 1. Network Topology

advertisement. After creating MPLS core testing is performed on customer routers which meet stated requirements.

2. MPLS/BGP VPNS Implementation

2.1 Network Topology

The proposed system MPLS/BGP VPN in a network core is implemented using Dynagen simulator in which the network topology consists of five routers that are as follows (also shown in Figure 1):

- CE-1 Customer Edge router at the one end of the network.
- CE-2 Customer Edge router at the other edge of the network.

Table 1. Proposed Network Design Configuration

Customer Edge (CE-1)	Customer Edge (CE-2)	Provider Edge (Core Router P)	Provider Edge (PE-1)	Provider Edge (PE-2)
config t host CE-1 no ip routing ip routing no ip domain-loo no ena sec enable pass cisco int s1/0 ip address 1.1.1.1 255.0.0.0 no shutdown k no en clock rate 128000 int loop 0 ip address 10.1.1.1 255.0.0.0 int loop 1 ip address 20.1.1.1 255.0.0.0 router rip ver 2 no auto network 1.0.0.0 network 10.0.0.0 network 20.0.0.0 line v 0 4 no login privi l 15 line c 0 no login privi l 15	config t host CE-2 no ip routing ip routing no ip domain-loo no ena sec enable pass cisco int s1/1 ip address 4.1.1.2 255.0.0.0 no shutdown k no en clock rate 128000 int loop 0 ip address 30.1.1.1 255.0.0.0 int loop 1 ip address 40.1.1.1 255.0.0.0 router rip ver 2 no auto network 4.0.0.0 network 30.0.0.0 network 40.0.0.0 line v 0 4 no login privi l 15 line c 0 no login privi l 15	config t host P-1 no ip routing ip routing no ip domain-loo no ena sec ena pass cisco ip cef mpls label protocol ldp mpls ldp router-id loop 0 force int s1/0 mpls ip ip address 3.1.1.1 255.0.0.0 no sh k no en clock rate 128000 int s1/1 mpls ip ip address 2.1.1.2 255.0.0.0 no shutdown k no en clock rate 128000 int loop 0 ip address 12.1.1.1 255.0.0.0 router rip ver 2 no auto network 2.0.0.0 network 3.0.0.0 network 12.0.0.0 line v 0 4 no login privi l 15 line c 0 no login privi l 15	config t host PE-1 no ip routing ip routing no ip domain-loo no ena sec ena pass cisco mpls label protocol ldp mpls ldp router-id loop 0 force ip vrf vpn1 rd 1:1 route-target 1:1 int s1/0 ip address 1.1.1.2 255.0.0.0 no shutdown k no en clock rate 128000 ip vrf forwarding vpn1 ip address 1.1.1.2 255.0.0.0 int s1/1 mpls ip ip address 2.1.1.1 255.0.0.0 no sh k no en clock rate 128000 int loop 0 ip address 11.1.1.1 255.0.0.0 router rip ver 2 no auto network 2.0.0.0 network 11.0.0.0 address-family ipv4 vrf vpn1 ver 2 no auto network 1.0.0.0 redistribute bgp 100 metric transparent router bgp 100 no auto -summary no synchronization neighbor 13.1.1.1 remote-as 100 address-family vpnv4 neighbor 13.1.1.1 activate neighbor 13.1.1.1 send-community both neighbor 13.1.1.1 next-hop-self address-family ipv4 vrf vpn1 no auto -summary no synchronization redist rip line v 0 4 no login privi l 15 line c 0 no login privi l 15	config t host PE-2 no ip routing ip routing no ip domain-loo no ena sec ena pass cisco mpls label protocol ldp mpls ldp router-id loop 0 force ip vrf vpn1 rd 1:1 route-target 1:1 int s1/0 mpls ip ip address 3.1.1.2 255.0.0.0 no sh k no en clock rate 128000 int s1/1 ip address 4.1.1.1 255.0.0.0 no shutdown k no en clock rate 128000 ip vrf forwarding vpn1 ip address 4.1.1.1 255.0.0.0 int loop 0 ip address 13.1.1.1 255.0.0.0 router rip ver 2 no auto network 3.0.0.0 network 13.0.0.0 address-family ipv4 vrf vpn1 ver 2 no auto network 4.0.0.0 redistribute bgp 100 metric transparent router bgp 100 no auto -summary no synchronization neighbor 11.1.1.1 remote-as 100 address-family vpnv4 neighbor 11.1.1.1 activate neighbor 11.1.1.1 send-community both neighbor 11.1.1.1 next-hop-self address-family ipv4 vrf vpn1 no auto -summary no synchronization redist rip line v 0 4 no login privi l 15 line c 0 no login privi l 15

- PE-1 Provider Edge router by the side of one end of the MPLS cloud. Interface of this router with IP address 2.1.1.1 is a part of MPLS/BGP VPN while the interface with IP address 1.1.1.2 does not belong to VPN.
- PE-2 Provider Edge router by the side of other end of the MPLS cloud. Interface of this router with IP address 3.1.1.2 is a part of MPLS/BGP VPN while the interface with IP address 4.1.1.1 does not belong to VPN.
- P is a Core router.

2.2 Network Configuration

Following configurations are made on each router in the proposed network design as given in Table 1:

2.3 Simulation Results

2.3.1 Operation 1

The following operation (Figure 2) is to perform that the designed MPLS/BGP VPN has been established and showing the VPNs basic feature of security against the unauthorized access. An attempt to access interface 1.1.1.2 of router PE-1 from CE-1 gets 100 percent success while for the 2.1.1.1 is totally denied. Similarly, all attempts to access router P and 3.1.1.2 interface of PE-2 from CE-1 are refused. But all attempts to access 4.1.1.2 interface of router PE-2 and router CE-2 are again perfectly successful. So, it shows that MPLS BGP VPN exists consisting of three routers.

2.3.1.1 Results

The interfaces of the routers lying within the VPN are inaccessible by any external host but traffic destined through these is communicated properly which is an ultimately key security feature of VPN. As above configuration is of MPLS/BGP VPN so it becomes obvious that MPLS/BGP VPN is a dedicatedly secure channel for traffic transmission.

2.3.2. Operation 2

The following operation shows how labels are assigned to the routes in MPLS based networks (i.e., edge and core routers) and what is the role of these routers in traffic forwarding treat the routes.

2.3.2.1 Router PE-1

Tagging and Label Distribution

The following output (Figure 3) shows the labels being received and forwarded by the provider's edge router PE-1.

MPLS Forwarding & BGP Routing Table

The output displayed in Figure 4 shows the basic operation of provider edge router PE-1. It pops up the tags from all of routes received form P while it tags up the routes properly coming from CE-1 and directly connected to it. It shows the detail of valid and best routs along with their next hops. The presence of VPN named as VPN1 expresses the establishment of Tunnel.

2.3.2.2 Router P

MPLS Forwarding Table

The output displayed in Figure 5 shows the basic operation of provider core, it pops up the tags from all of routes received form PE-1 and PE-2.

Tagging and Label Distribution

Figure 6 and Figure 7 show the labels being received and forwarded by the provider core router P.

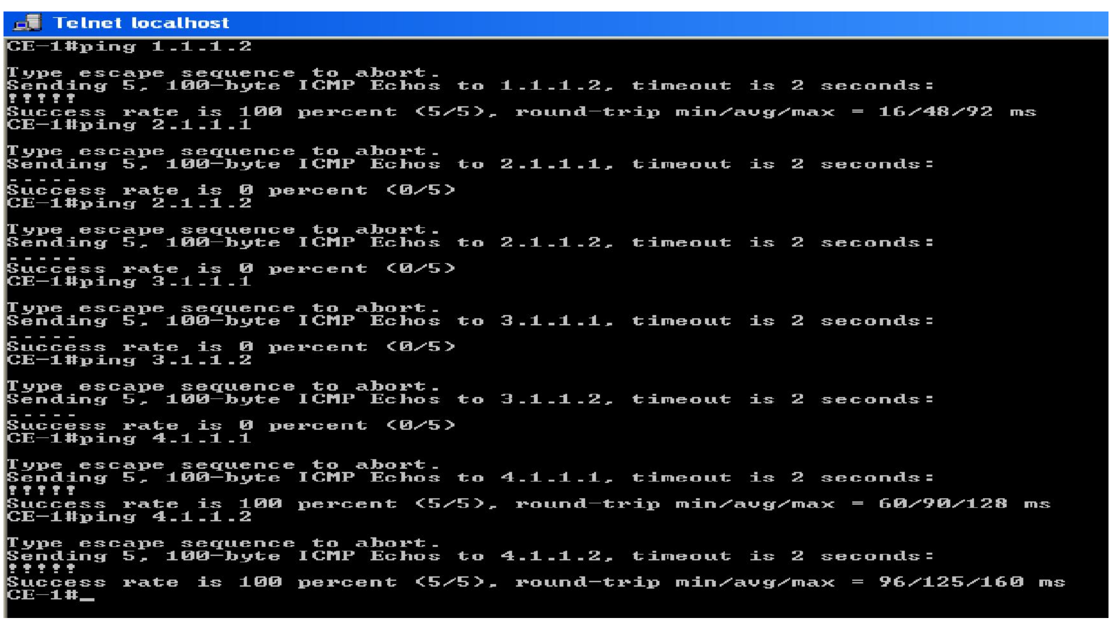
2.3.2.3 Router PE-2

Tagging and Label Distribution

Figure 8 shows the labels being received and forwarded by the provider edge router PE-2.

MPLS Forwarding & BGP Routing

The output displayed in Figure 9 shows the basic operation of provider edge router PE-2, it pops up the tags from all of routes received form P while it tags up the routes properly coming from CE-2 and directly connected to it. It shows the detail of valid and best routes along with their next hops. The presence of VPN named as VPN1 expresses the establishment of tunnel.



```
Telnet localhost
CE-1#ping 1.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/48/92 ms
CE-1#ping 2.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CE-1#ping 2.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.1.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CE-1#ping 3.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CE-1#ping 3.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.1.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CE-1#ping 4.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/90/128 ms
CE-1#ping 4.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/125/160 ms
CE-1#_
```

Figure 2(a). MPLS BGP VPN Test

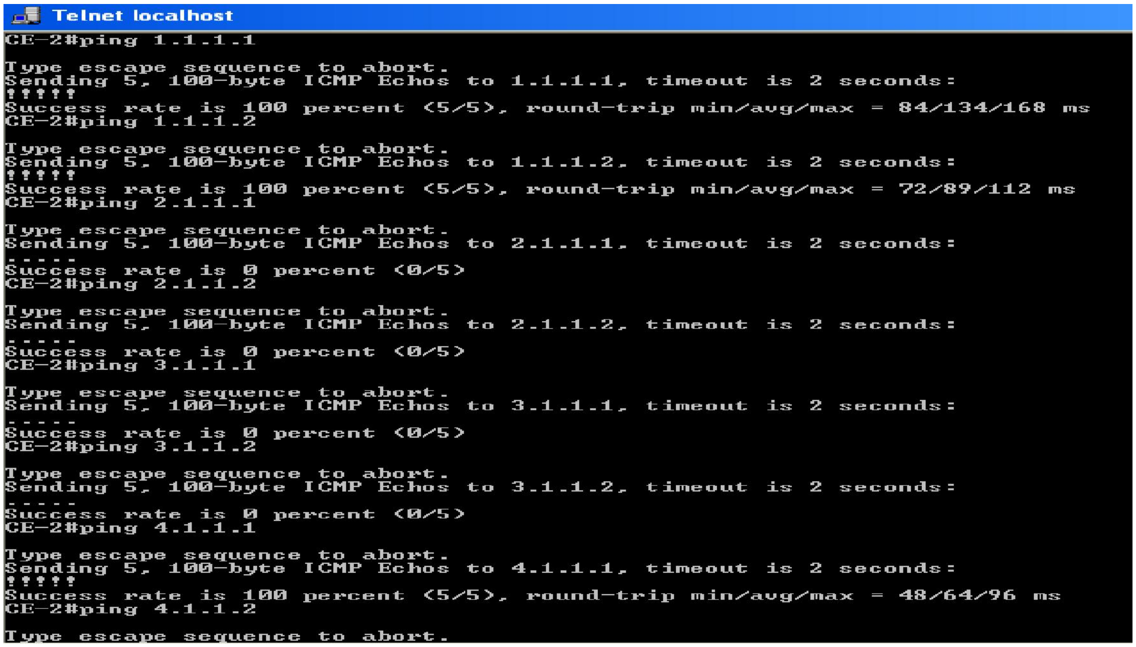


Figure 2(b). MPLS BGP VPN Test

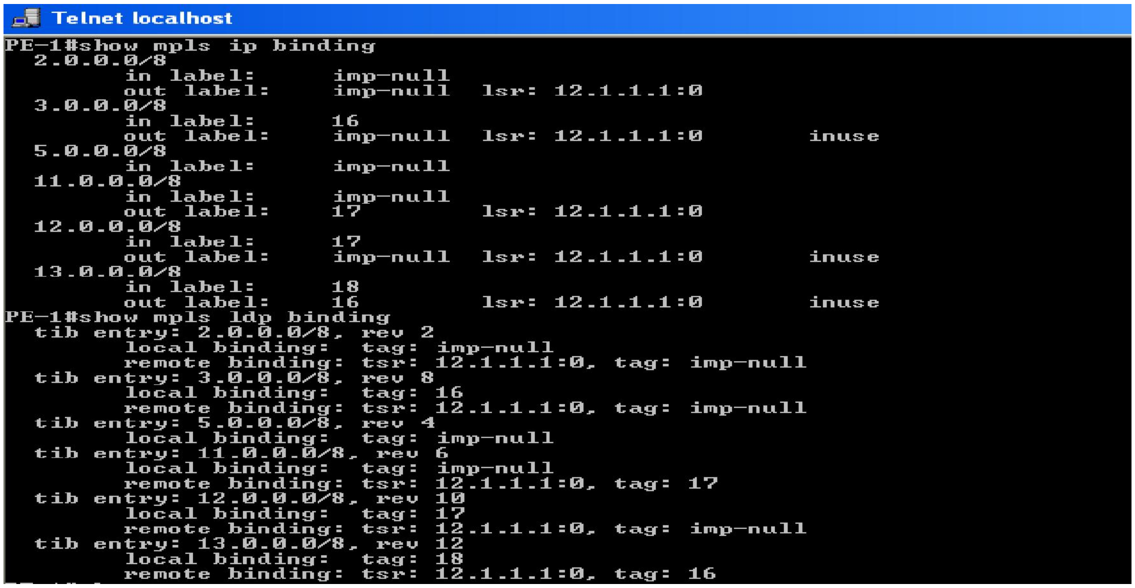


Figure 3. MPLS and LDP bindings at PE-1

2.3.3 Results

- The provider edge router PE-1 assigns labels to its directly connected networks and the traffic coming from CE-1 as starting edge router of MPLS cloud and sends it to core route P. The router which receives the outside traffic at the edge of MPLS VPN and forwards it to the core after labeling is called Ingress Router (IR). Similarly, it pops up the tags of traffic coming from core as ending edge router of MPLS cloud and sends it to C-1.
- The edge router which receives tagged traffic from the core and forwards this traffic after un-tagging is called Egress Router (ER). So PE-1 is ingress for the traffic coming form CE-1 and being forwarded to the core and is egress for the traffic coming from core and being forwarded outside the MPLS cloud.
- The PE-2 (provider edge router) is ingress for the traffic coming from CE-2 while it is egress for the traffic coming from core.
- The core router just switches the tags which causes a huge enhancement in traffic forwarding.

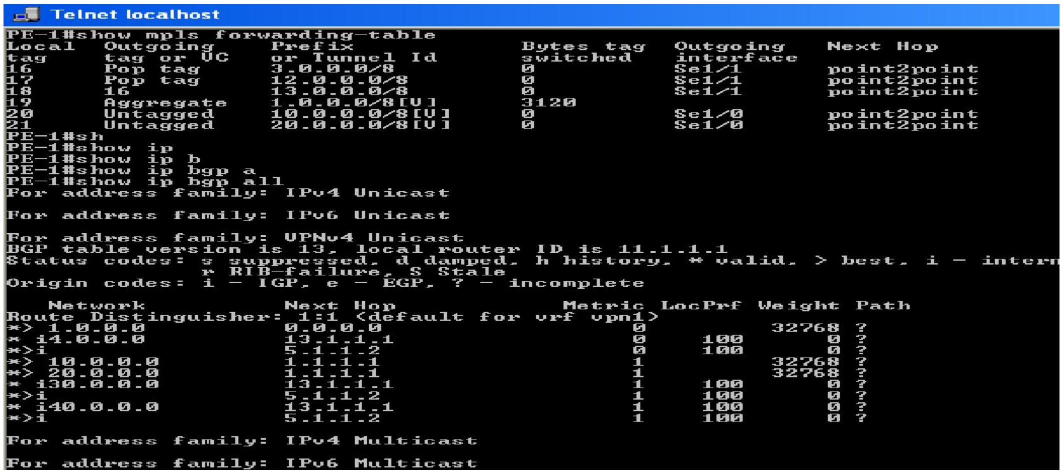


Figure 4. MPLS Forwarding & BGP Routing Table of PE-1

Figure 5. MPLS Forwarding Table of P

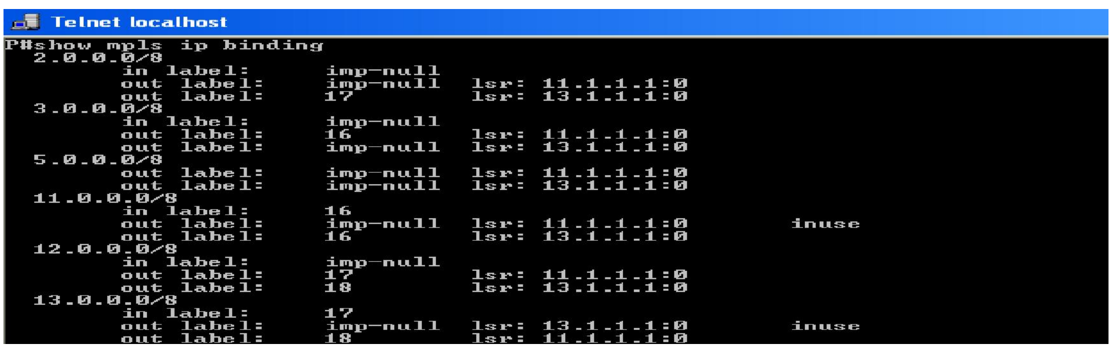


Figure 6. MPLS labeling on core router P

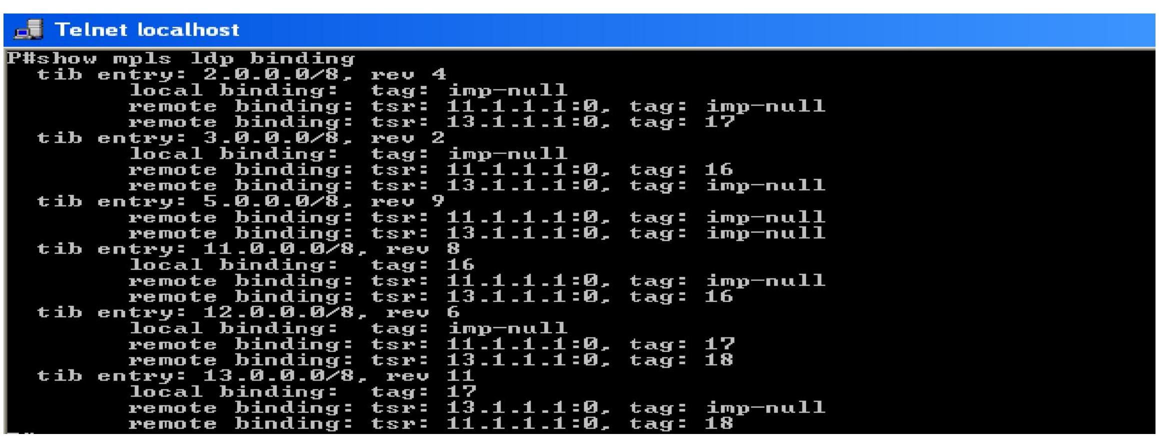
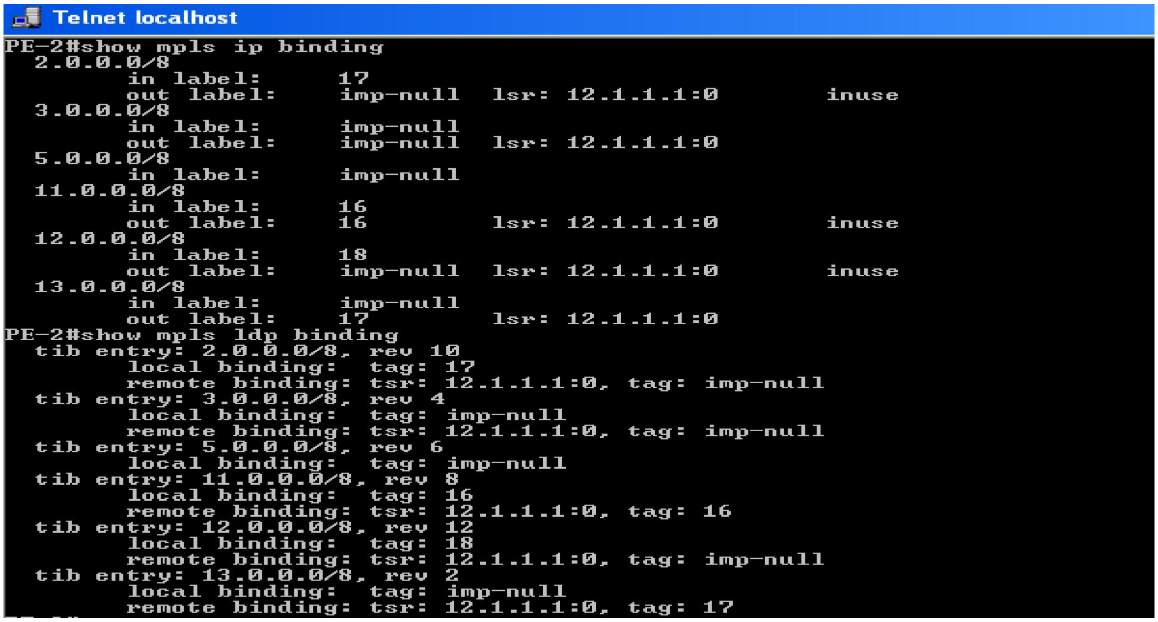
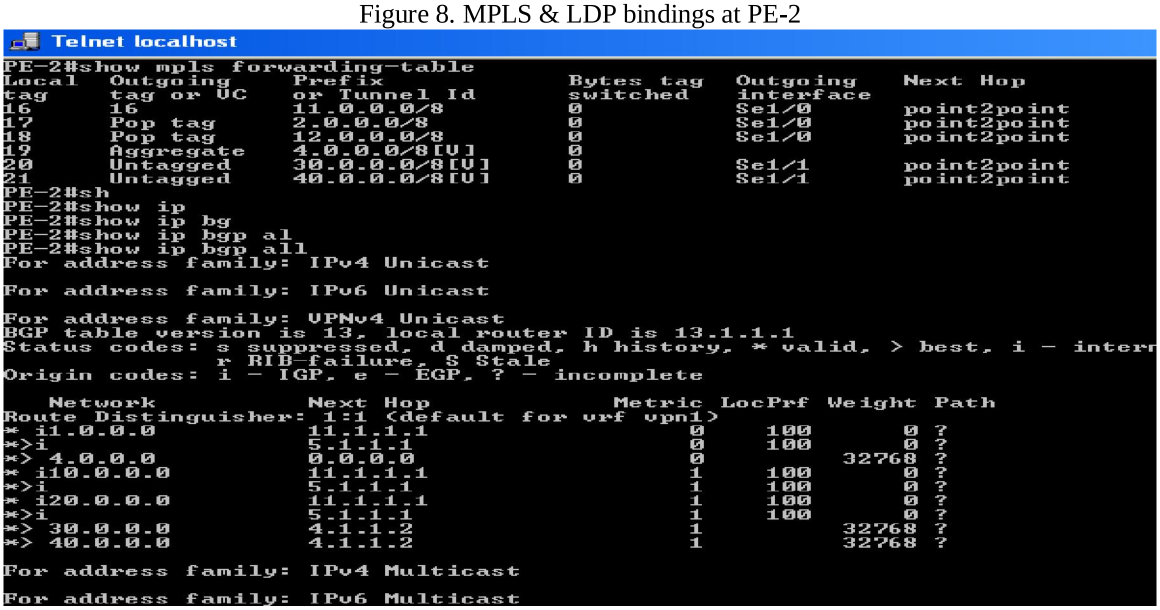


Figure 7. LDP binding on Core router P



```
Telnet localhost
PE-2#show mpls ip binding
  2.0.0.0/8
        in label:     17
        out label:    imp-null  lsr: 12.1.1.1:0       inuse
  3.0.0.0/8
        in label:     imp-null
        out label:    imp-null  lsr: 12.1.1.1:0
  5.0.0.0/8
        in label:     imp-null
  11.0.0.0/8
        in label:     16
        out label:    16        lsr: 12.1.1.1:0       inuse
  12.0.0.0/8
        in label:     18
        out label:    imp-null  lsr: 12.1.1.1:0       inuse
  13.0.0.0/8
        in label:     imp-null
        out label:    17        lsr: 12.1.1.1:0
PE-2#show mpls ldp binding
  tib entry: 2.0.0.0/8, rev 10
        local binding:  tag: 17
        remote binding: tsr: 12.1.1.1:0, tag: imp-null
  tib entry: 3.0.0.0/8, rev 4
        local binding:  tag: imp-null
        remote binding: tsr: 12.1.1.1:0, tag: imp-null
  tib entry: 5.0.0.0/8, rev 6
        local binding:  tag: imp-null
  tib entry: 11.0.0.0/8, rev 8
        local binding:  tag: 16
        remote binding: tsr: 12.1.1.1:0, tag: 16
  tib entry: 12.0.0.0/8, rev 12
        local binding:  tag: 18
        remote binding: tsr: 12.1.1.1:0, tag: imp-null
  tib entry: 13.0.0.0/8, rev 2
        local binding:  tag: imp-null
        remote binding: tsr: 12.1.1.1:0, tag: 17
```

Figure 8. MPLS & LDP bindings at PE-2



```
Telnet localhost
PE-2#show mpls forwarding-table
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     16          11.0.0.0/8        0          Se1/0      point2point
17     Pop tag     2.0.0.0/8         0          Se1/0      point2point
18     Pop tag     12.0.0.0/8        0          Se1/0      point2point
19     Aggregate   4.0.0.0/8[V]      0
20     Untagged    30.0.0.0/8[V]     0          Se1/1      point2point
21     Untagged    40.0.0.0/8[V]     0          Se1/1      point2point
PE-2#sh
PE-2#show ip
PE-2#show ip bg
PE-2#show ip bgp al
PE-2#show ip bgp all
For address family: IPv4 Unicast

For address family: IPv6 Unicast

For address family: VPNv4 Unicast
BGP table version is 13, local router ID is 13.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - intern
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vpn1)
* i1.0.0.0          11.1.1.1                 0    100      0 ?
*>i                 5.1.1.1                  0    100      0 ?
*> 4.0.0.0          0.0.0.0                  0         32768 ?
* i10.0.0.0         11.1.1.1                 1    100      0 ?
*>i                 5.1.1.1                  1    100      0 ?
* i20.0.0.0         11.1.1.1                 1    100      0 ?
*>i                 5.1.1.1                  1    100      0 ?
*> 30.0.0.0         4.1.1.2                  1         32768 ?
*> 40.0.0.0         4.1.1.2                  1         32768 ?

For address family: IPv4 Multicast

For address family: IPv6 Multicast
```

Figure 9. MPLS Forwarding & BGP Routing Table of PE-2

3. Conclusions and Future Work

In this research work firstly, we have comprehensively presented an overview of MPLS, BGP and, both layer 2 and layer 3 VPNs. In particular, IP VPNs issues such as speed, scalability and security are discussed in detail. Secondly, we have proposed a new design scheme for MPLS/BGP-VPNs by merging the features of layer-3 (such as scalability and intelligence) with the features of layer-2 (such as efficiency and simplicity), to deal with the today's evolving demands of network speed, quality of service, scalability and security.

We have discussed in detail the challenges when these two architectures will be merged to provide another infrastructure and we have also provided the solution to some of these challenges to make this new concept worthy and an asset to the current research world. We have presented a network simulation architecture that helps us to assess the security constraints for MPLS/BGP-VPNs.

Further this research can be enhanced to traffic engineering (TE), end-to-end performance, security and path management. Traffic engineering (TE) includes schemes and methods that are applied to force routed traffic to pass through the network on a path, except one which is selected on the basis of standard routing. This system will be helpful for adding new security features in core networks in future and provides a guideline for network engineers towards the world of network security.

In our future work, we will discuss the various issues regarding the implementation of MPLS/BGP-VPNs in multihomed (Junaid and Saleem, 2010; Junaid & Saleem, 2008) environments.

Acknowledgments:

This work was supported by the Directorate of Research Extension and Advisory Services, University of Engineering and Technology (UET), Lahore-Pakistan.

Corresponding Author:
Mohammad Junaid Arshad, PhD
Department of Computer Science & Engineering,
University of Engineering and Technology,
Lahore-Pakistan-54890.
Email: junaidarshad@uet.edu.pk

References

1. Previdi, S. Introduction to MPLS-BGP-VPN, Proceeding of MPLS Forum 2000, Cisco, April, 2000.
2. Awduche, D.O. MPLS and Traffic Engineering in IP Networks, IEEE Communication Magazine, Volume 37, No. 12, pp. 42-47, New Jersey, USA., December, 1999.
3. Rosen, E., and Rekhter, Y. BGP/MPLS VPNs, RFC 2547, IETF (draft-rosen-rfc2547bis-03.txt), March, 1999.
4. Lee, H., Hwang, J., Kang, B., and Jun, K. End-To-End QoS Architecture for VPNs: MPLS VPN Deployment in a backbone Network, Proceedings of IEEE International Workshop on Parallel Processing, Volume 5, No. 1, pp. 479-483, Toronto, Canada, August, 2003.
5. Swallow, G. MPLS Advantages for Traffic Engineering, IEEE Communication Magazine, Volume 37, No. 12, pp. 54-57, New Jersey, USA. December, 1999.
6. Ferguson, P., and Huston, G. What is VPN, The Internet Protocol Journal, Volume 1, No. 2, San Jose, USA., September, 1998,
7. Callon, R. A framework for layer 3 provider provisioned virtual private networks, IETF (draft-ietf-ppvpn-frame-work-06.txt), October, 2002.
8. Alawieh, B., Ahmed, R.E., and Mouftah, HT. Security impacts on establishing MPLS/BGP VPNs, Journal of Security and Communication Networks, Volume 1, No. 4, pp. 269-275, John Wiley & Sons, New Jersey, USA., July, 2008.
9. Davis, C. IPsec: Securing VPNs, McGraw-Hill, Berkley, pp. 1-432, California, USA. April, 2001.
10. Deering, S., and Hinden, R. Internet Protocol Version 6 (IPv6) Specification, RFC 2460, December, 1998.
11. Rosen, E., Viswanathan, A., and Callon, R. Multiprotocol Label Switching Architecture", IETF RFC 3031, January, 2001.
12. Rosen, E., and Rekhter, Y. BGP/MPLS VPNs, RFC 2547, March, 1999.
13. Das, S.K., Venkataram, P., and Biswas, J. MPLS-BGP based LSP Setup Techniques, Proceedings of the 28th Annual IEEE Conference on Local Computer Network (LNC), Volume 17, No. 1, pp. 279-280, Singapore, July, 2003.
14. Dynagen Simulator, http://dynagen.org/ [online, April, 2007].
15. Junaid, M., and Saleem, M. A Simulation-Based Study of FAST TCP Compared to SCTP: Towards Multihoming Implementation Using FAST TCP. Journal of Communications and Networks (JCN), VOL. 12, NO. 3, pp. 275-284, June 2010.
16. Arshad, MJ., and Saleem, M. Issues of Multihoming Implementation Using FAST TCP: A Simulation Based Analysis, IJCSNS International Journal of Computer Science and Network Security, VOL. 8, No. 9, pp.104-114, August 2008.

6/28/2010