# Design of two-layered organizational network using different VPN technologies

Akshay Phalke [1], Gargi Chauhan[2] , Priyanka Shah[3]
*Department of IT, SVIT,GTU[1], Department of IT, SVIT,GTU[2], Department of IT, SVIT,GTU[3]*

akshayphalke429@gmail.com[1]

gargichauhan.it@svitvasad.ac.in[2]

priyankashah.it@svitvasad.ac.in[3]

***Abstract*— This paper focuses on improvement of organizational network in terms of availability, efficiency and security. This paper presents Dynamic multipoint virtual private network (DMVPN) with Multiprotocol label switching virtual private network (MPLS-VPN) to separate internet and intranet traffic. Here separation of both internet and intranet traffic makes network traffic monitoring easy. This paper also focuses on intranet redundancy to ensure availability.**

***Keywords*— VPN, Organizational network, Availability of network, Network security**

## 1. INTRODUCTION

A virtual private network (VPN) extends a private network across a public network. It connects two geographically separated branches of an organization as if their computing devices are directly connected. So that application software used across VPN leverage benefits of private network.

Over the time organizations have become more extensive. An organization may have multiple branches, these branches are required to be connected. To connect different branches of an organization a strong backbone network is required. This network should be efficient and secure. Further it should be available for all the time.

This paper describes two-layered backbone network architecture. First layer consists of DM-VPN and second layer consists of MPLS-VPN for intranet traffic. EIGRP routing protocol is configured in organizational branches. A DMVPN cloud is a collection of routers that is configured either with a multipoint GRE (m GRE) interface or point-to-point (p2p) GRE interface (or combination of the two) that share the same address subnet. [1].

MPLS is an emerging technology. It consists of an important feature known as VPN. MPLS-VPNs provide protection and isolation as traffic travels through the provider network. [2].Here in this paper concepts like MP-BGP, VRF are used to implement MPLS-VPN on layer-2.

## 2. LIMITATIONS OF EXISTING WORK

Existing work consists of two-layered architecture as shown in figure below.

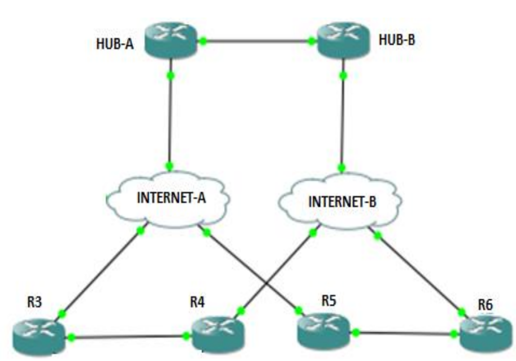

Fig-1:- Two-layered architecture with dm-vpn

Here Hub-A and Hub-B are at headquarters.R3 and R4 are at location-1 and R5 and R6 are at location-2. HUB-A, R3 and R5 are part of layer-1 and HUB-B, R4 and R6 are part of layer-2.

Here DM-VPN is configured on both the layers and EZ-VPN is been introduced for secure remote access [3]. Now here EIGRP routing protocol is been configured on all locations. EIGRP consists of metric, known as composite metric. This composite metric consists of K-Values. The K-Values are as K1= Bandwidth, K2=Load, K3=Delay, K4=Reliability, K5=MTU.

Here natting is been configured on R3, R6 for internet traffic. Because of which internet traffic will travel from R3 for location-1.

Now based on metric value best path is been decided for intranet traffic i.e. the path which has less metric value will be considered as the best path for intranet traffic. Here we are considering device R9 behind location-1 and a server behind headquarter location. Now there are two possible paths for communication between R9 and server. Path-1 is via R3 and path-2 is via R4.

Here Metric calculation for routers R3, R4, R5, and R6 are as follows.

$$Metric = ((10^7 / (Least-bandwidth)) + Cumulative\ delay) * 256$$

$$= ((10^7/9) + 50100) * 256$$

$$= (1161211) * 256$$

$$= 297270016$$

As per EIGRP metric calculation formula metric for both the paths are same. So only one path will be used at a time for internet traffic and another one will be idle. HSRP is being used on R3 and R4 for LAN redundancy. Here path-2 will only be used when path-1 is not available. In this way

This topology provides WAN redundancy for intranet traffic with disadvantage that only one path is used at a time.

## 3. ADVANTAGES AND IMPLIMENTATION OF PROPOSED WORK

Proposed work consist of two-layered architecture as shown in figure below.

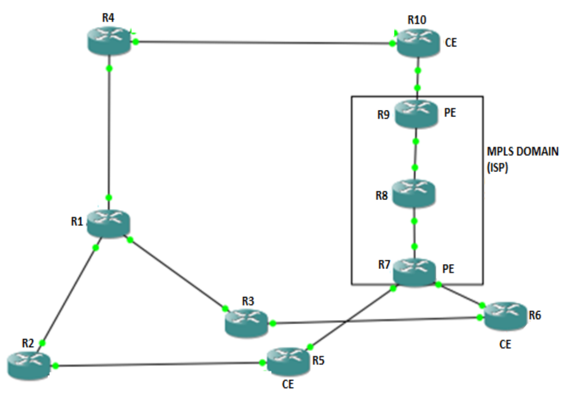


Fig 2:- Two-layered architecture with DM-VPN and MPLS-VPN

Here R4 and R10 are headquarter routers, R2 and R5 are at location-1 and R3 and R6 are at location-2.

Here DM-VPN is configured on layer-1 and MPLS-VPN is configured on layer-2 [5]. R7, R8, R9 are the part of MPLS domain. R5 and R6 are CE (costumer edge) routers. Here MP-BGP is configured on R7 and R9. The concept of VRF [4] is used for R7 and R9. Here we assume device R11 behind location -1 and server R12 behind headquarter location. Here also natting is been configured on R2, R6 for internet traffic. Because of which internet traffic will travel from R2 for location-1.

The EIGRP metric calculation for R2 and R5 is shown below.

EIGRP metric calculation for R2.

$Metric=((10^7/(Least-bandwidth))+Cumulativdelay)*256$

$= ((10^7/100)+5001)*256$

$= (105001) * 256$

$= 26880256$

```
R2#sh ip route 192.168.8.1
Routing entry for 192.168.8.0/24
  Known via "eigrp 100", distance 90, metric 26880256, type internal
  Redistributing via eigrp 100
  Last update from 10.0.0.4 on Tunnel0, 00:00:25 ago
  Routing Descriptor Blocks:
  * 10.0.0.4, from 10.0.0.4, 00:00:25 ago, via Tunnel0
      Route metric is 26880256, traffic share count is 1
      Total delay is 50010 microseconds, minimum bandwidth is 100 Kbit
      Reliability 255/255, minimum MTU 1476 bytes
      Loading 1/255, Hops 1
```

Fig-3:- Metric for R2

EIGRP metric calculation for R5.

$Metric=((10^7/(Least-bandwidth))+Cumulativedelay)*256$

$= ((10^7/10^6)+3)*256$

$= (13) * 256$

$= 3328$

```
R5#sh ip route 192.168.8.1
Routing entry for 192.168.8.0/24
  Known via "eigrp 100", distance 90, metric 3328, type internal
  Redistributing via eigrp 100
  Last update from 75.0.0.7 on GigabitEthernet1/0, 00:19:45 ago
  Routing Descriptor Blocks:
  * 75.0.0.7, from 75.0.0.7, 00:19:45 ago, via GigabitEthernet1/0
      Route metric is 3328, traffic share count is 1
      Total delay is 30 microseconds, minimum bandwidth is 1000000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 2
```

Fig-4:- Metric for R5

As shown in fig 4 and 5 R5 has a less metric value then R2. So that intranet traffic for location-1 will always travel through R5 and internet traffic will travel through R2. In this way internet and intranet traffics are separated. MPLS is more efficient technology for packet forwarding, here we can have more throughput and less latency values for intranet traffic.

Here HSRP is configured on R2 and R5 of location-1 for LAN redundancy. This topology also provides WAN redundancy for intranet traffic. Implementations are shown below.

```
R11#traceroute 192.168.8.1

Type escape sequence to abort.
Tracing the route to 192.168.8.1

  1 192.168.9.3 56 msec 36 msec 40 msec
  2 75.0.0.7 68 msec 88 msec 20 msec
  3 91.0.0.9 [MPLS: Label 32 Exp 0] 200 msec 140 msec 96 msec
  4 91.0.0.10 204 msec 144 msec 200 msec
  5 192.168.8.1 216 msec 228 msec 188 msec
R11#ping 192.168.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.8.1, timeout is 2 seconds:
!!!!!
```

Fig-5:- Trace route and ping information

```
R11#traceroute 192.168.8.1

Type escape sequence to abort.
Tracing the route to 192.168.8.1

  1 192.168.9.2 60 msec 28 msec 56 msec
  2 10.0.0.4 128 msec 124 msec 120 msec
  3 192.168.8.1 156 msec 120 msec 152 msec
R11#ping 192.168.8.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.8.1, timeout is 2 seconds:
!!!!!
```

Fig-6:- New Trace route and ping information after mpls shutdown

```
R11#traceroute 192.168.8.1

Type escape sequence to abort.
Tracing the route to 192.168.8.1

  1 192.168.9.3 44 msec 28 msec 28 msec
  2 75.0.0.7 64 msec 60 msec 60 msec
  3 91.0.0.9 [MPLS: Label 32 Exp 0] 124 msec 112 msec 140 msec
  4 91.0.0.10 124 msec 156 msec 156 msec
  5 192.168.8.1 188 msec 156 msec 204 msec
R11#ping 192.168.8.1 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.8.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.........!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
```

Fig-7:- Intranet redundancy test

In this way we can achieve WAN redundancy with MPLS efficiency and security.

## IV. Conclusions

In today's time multi location organizations want secure, efficient and redundant backbone network. This paper focuses on secure and efficient intranet traffic delivery with the help of DM-VPN and MPLS-VPN. A new topology also provides WAN redundancy for intranet traffic. In future SSL-VPN can be implemented for secure remote access.

# REFERENCES

[1] Gebere Akele Tizazu and Ki-Hyung Kim, “Dynamic Routing Influence on Secure Enterprise Network Based on DMVPN,” IEEE, 2017

[2] Snehal Yadav and Amutha Jeyakumar, “MPLS Multi-VRF Design and Implementation using GNS simulator,” IEEE, March 2016.

[3] Hongru Li, P.W.C. Prasad, Abeer Alsadoon, L. Pham, A. Elchouemi, “An improvement of Backbone Network security using DMVPN over an EZVPN structure,” IEEE, Nov 2016.

[4] Snehal Yadav and Amutha Jeyakumar, “Design of Traffic Engineered MPLS VPN for Protected Traffic using GNS Simulator,” IEEE, 2016.

[5] Ming-Song Sun, Wen-Hao Wu, “Engineering Analysis and Research of MPLS VPN,” IEEE, 2013.

[6]. Yusuf Bhaiji " Network Security Technologies and Solutions".

**1.Akshay P Phalke** has received Bachelor's (2014) in Information Technology. At present he is student in Information Technology Department. at Sardar Vallabhbhai Patel Institute of Technology – Vasad.

**2.Gargi K Chauhan** has received Bachelor's (2006) in Information Technology and Master's (2012) in Computer Science & Technology from LDCE - Ahmedabad, Gujarat, India. At present she is working as an Assistant Professor in the IT Dept., at Sardar Vallabhbhai Patel Institute of Technology – Vasad, Gujarat – India.She has more than 12 years of experience as an academician. She authored many papers at national/international conferences/journals of repute and worked on many students' projects. She is also life member of IETE and ISTE professional societies.

**3.Mrs Priyanka Shah** Bechlor in information Technology and Master in Computer engineering from Gujarat technological university currently working as an asst prof. in department of information technology at SVIT, Vasad. She has 10 years teaching experience. Her area of specialization are Wireless communication, mobile computing, cloud computing, computer organization.