

Virtual Routing and Forwarding-lite Traffic Management over Multi-protocol Layer Switching-Virtual Private Network

Ruhani Ab Rahman, Nur Asikin Zahari, Murizah Kassim, Mat Ikram Yusof
Faculty of Electrical Engineering, Universiti Teknologi MARA,
UiTM Shah Alam, Selangor, Malaysia.
ruhani467@salam.uitm.edu.my

Abstract— Quality of Services in Multi-protocol layer switching for Virtual Private Network (MPLS-VPN) is one of important matter today. These networks experienced an increase of bandwidth size for enterprises LAN which are faster than the increased of bandwidth at WAN link. Thus, line speed is disparity and bottleneck is occurred at the link between WAN and LAN due to the unparalleled increase of bandwidth between these links. This paper presents a study of MPLS-VPN architecture and how to encounter the congestions problem by simulating traffic management on the path diversity and load balance using VRF-lite technique at enterprises MPLS-VPN. A test bed is set up and real enterprise MPLS-VPN network for traffic management is simulated. VRF-Lite traffic management is applied at identified two WAN headquarters and three branch network. WAN and LAN link is identified on primary and secondary network link. VRF-lite is used to overcome the bottle neck at the Branch WAN-LAN link and also to fully utilize all available links at the other sites. Adaptive traffic management is set where if it is identified that other link is not congested than traffic will pass through the link. Result presents analyzed of throughput and bandwidth utilization percentage on all identified links using ftp and http applications. Successful results present that all links at HQ and Branch is being utilized and the congestion at the Branch WAN-LAN link is avoided.

Index Terms— Quality of services; Multi-protocol layer switching; Virtual private network; Virtual routing.

I. INTRODUCTION

Multi-protocol layer switching -Virtual Private Network (MPLS-VPN) are the ideal solution for medium and large enterprises that currently deploy site-to-site VPN services. MPLS provides sophisticated traffic engineering capabilities that, coupled with IP QoS, enable multiple classes of service so business critical applications are treated with higher priority than less important applications and best effort services. The popularity of MPLS VPNs as an alternative to private Wide Area Network (WAN) introduces a number of considerations with regard to QoS [1,2]. MPLS VPN also experienced on QoS issues where all the WAN-LAN links of the multi-homed sites at any given instant are not being fully utilized [3]. Research presented that one WAN-LAN links will be fully utilized but one is underutilized. Thus, load balancing is virtualized as the traffic management that balances the lightly loaded link to be fully utilized. The result achieved from this

prototype shows the improvements in bandwidth utilization once the load balancing techniques is applied to the network [4]. Others study presented traffic diversity is implemented where traffic from LAN (Local Area Network) to backbone network are divided through the different disjoint routes [5].

A Virtual Routing and Forwarding (VRF) table is a way to make multiple routing tables that are completely separate from each other. VRF-lite is used to isolate each of these networks from interfering with each other and it also enables the CEs to have separate VRF tables for each of the networks [6]. Using VRF-lite, the packets of each customer is routed based on their individual routing table. It also make used of same and overlapping IP address on the same physical device when the device is using VRF-lite. The input interfaces of the CE are used by the VRF-lite to match the routes from the different VPN. The virtual packet forwarding table is formed based on the associated layer 3 interfaces which are physical or logical layers with all VRF. Traffic segregation is using VRF-lite replacing policy-based routing when it is normally being opted. It is one of a load balance technique to route traffic to identified unutilized route for bandwidth utilization.

This research presents a study of MPLS VPN architecture and simulating traffic management on the path diversity and load balance using VRF-lite technique at enterprises MPLS VPN WAN-LAN network. Real enterprise MPLS VPN network for traffic management is simulated and data collected from the test bed. VRF Lite traffic management is applied at two HQ WAN and three branch LAN network. WAN and LAN link is identified on primary and secondary network link. VRF-lite is used to overcome the bottle neck at the Branch WAN-LAN link and also to fully utilize all the available links at the other sites. Load balance is applied on identified congested link where traffic is passing through the uncongested link. Result presents an analyzed of throughput and bandwidth utilization on all links using ftp and http applications. Successful results present that all links at HQ and Branch is being utilized and the congestion at the Branch WAN-LAN link is avoided.

II. MPLS VPN LOAD BALANCE

MPLS VPN network which consist of many HQ and client routers experienced with congestions traffic that focus to one

route especially if it not monitored for QoS. Thus, a diverse path method for the core link might be achieved by using Multi-Topology Routing (MTR) topologies or VRF lite technology to overcome congestion link problem. This gives diverse path within the core for IP transport [7]. Figure 1 shows how MPLS VPN architecture works [8]. The MPLS VPN consists of three important components which are customer edge (CE), provider edge (PE) and provider router (P) [9]. Each of the customer's remote sites in the MPLS VPN is connected to the CE and it is connecting the backbone sites via PE router. The routers used in the MPLS VPN are the P router that responsible only for high speed forwarding and it is operating using Multi-Protocol Label Switching (MPLS) [10]. Bandwidth size for enterprises VPN WAN-LAN is increasing rapidly. MPS experience with increased of bandwidth at the WAN link is slower than the LAN link. A study on implementation of dynamically auto configured multiservice multipoint VPN has been done. The study implemented VRF-Lite approach to isolate client traffic at levels 2 and 3 using isolated routing tables and ARP without virtualizing the network stack. Different VPN services use virtual interfaces to route the VPN client traffic. Redirecting traffic to different VRFs allows to isolates traffic within the same server but different VPN protocols. At the CPE side, separated routing instances, named Virtual Routing Function (VRF) Lite which is a logical way of segregating network traffic handle voice and data traffic and also QoS is applied accordingly [11, 12].

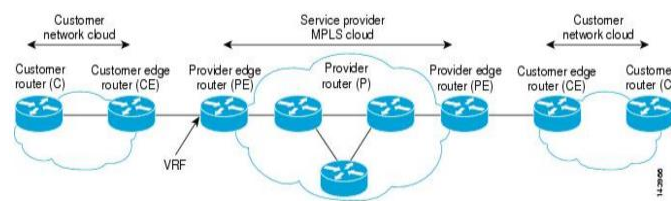


Figure 1: MPLS VPN architectural model

III. METHODOLOGY

This study comprise of three phase which are firstly is test bed simulation, monitoring setup and last phase is data collection and analyzed.

A. Test Bed Setup

Figure 2 and Figure 3 shows the diagram and actual test bed setup of the project. Four routers are being used to construct the WAN network and one router with the Ethernet cards are being used as the switch at the Branch site. Three computers are being used as FTP server, HTTP server and Client in the test bed setup. Five sites are set up which are HQ WAN, HQ LAN, Primary Branch, Secondary Branch and Branch Switch. All sites used Cisco 2811, Cisco 1841 model and C2800NM-adventerprisek9-M and C1841-adventerprisek9-M OIS image. The bandwidth for each of the links is configured as HQ Primary and Secondary WAN link for 20 Mb, Branch Primary and Secondary WAN link with 1 Mb and Branch LAN link for 100 Mb.

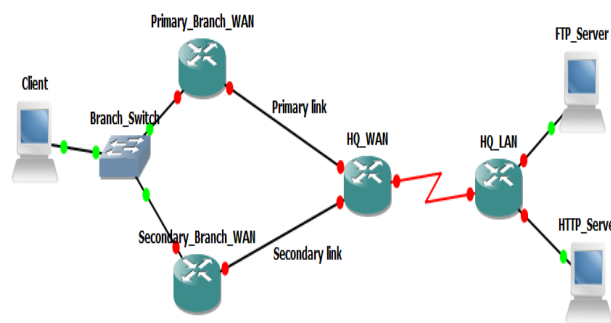


Figure 2: Diagram of the test bed setup



Figure 3: Actual test bed setup

Systems are operated with Microsoft Windows XP, 8 and 7 Professional Operating Software for each Client and FTP server. Type of applications use are Torch Web browser, FileZilla Client 3.8.0, FileZilla Server version 0.9.40 Beta in transferring the file across the network. The experiment has tested setup two different scenarios which are the network setup without applying VRF-lite at the HQ and the scenario where VRF-lite is being applied to the HQ.

B. Bandwidth Monitoring Setup

Specification and requirement in setting up bandwidth monitoring tool of the simulated network is important. Bandwidths of all links are monitored using the Solar wind Bandwidth real-time monitoring software. SNMP v2 is used by the monitoring software to monitor the desired links [13]. The Solar Wind real-time monitoring software is able to monitor the entire 5 different link simultaneously during the file transfer [14]. The Client PC which is located at the Branch is being used at the SNMP-server. All routers such as HQ WAN, HQ LAN, Primary Branch WAN and Secondary Branch WAN are configured with the SNMP community string cisco and the SNMP server IP address which is the Client PC IP address 10.3.3.10.

i. Traffic Management (VRF-lite) Setup

Figure 4 shows process flow of the packets from Client to Application Server without VRF-lite. Traffic flows of packets from Branch to HQ when Client at Branch starts downloading 100 Mb files via FTP and HTTP. TCP connection between Client PC and the application server at the HQ is established at this moment. All packets travel from Client PC to the Branch

WAN router. If the Primary Branch WAN router is up, the packet flows to the Primary Branch WAN router to the Primary Branch WAN link. From the Primary Branch WAN link the packets is routed to the Primary HQ WAN link to the HQ WAN router, HQ LAN router and finally arriving at the application server. During the outage of the Primary Branch WAN router, the Secondary Branch WAN router is routed the packets to the Secondary Branch WAN link. The packets then is routed to the Secondary HQ WAN link, HQ WAN router, HQ LAN router and finally to the application server.

Figure 5 shows the flows of the packets routed from the application server at the HQ to the client at the Branch. The packets are routed from the application server to the HQ LAN router and to the HQ WAN router. The return traffic from the HQ WAN router to the Branch router followed the same links where the packets arrived. If the packets from Branch arrived at HQ router from the Primary HQ WAN link, the return traffic from the HQ to the Branch flows through the Primary HQ WAN link to the Primary Branch WAN link and finally arriving to the client at the Branch.

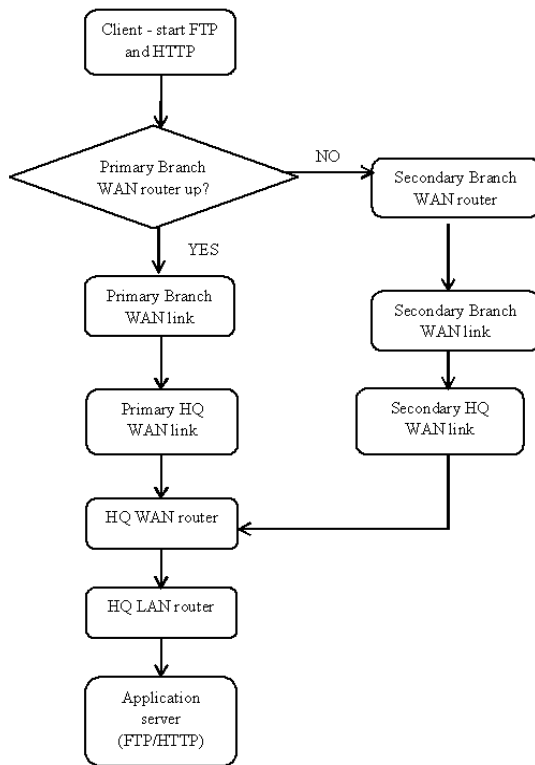


Figure 4: Client to App. Server W-VRF-lite

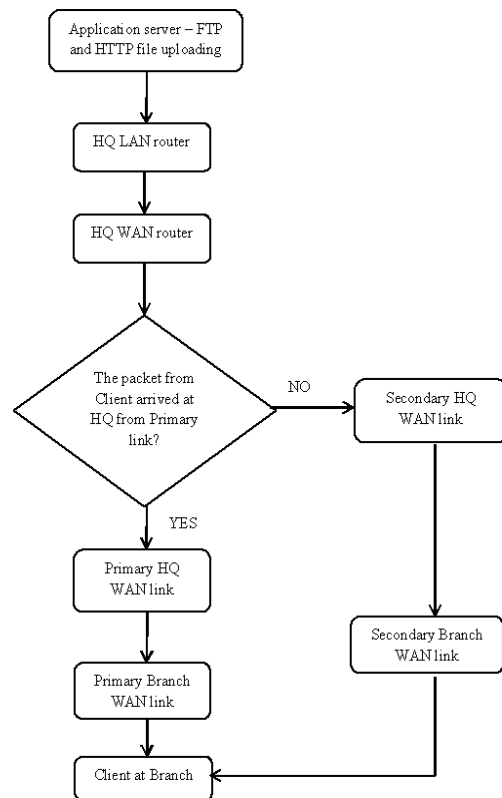


Figure 5: App. Server to the Client W-VRF-lite

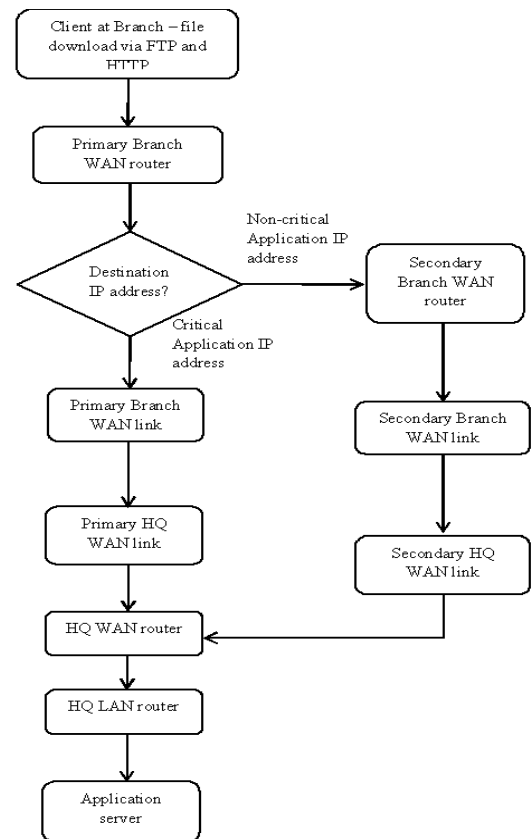


Figure 6: Client to App. Server VRF-lite

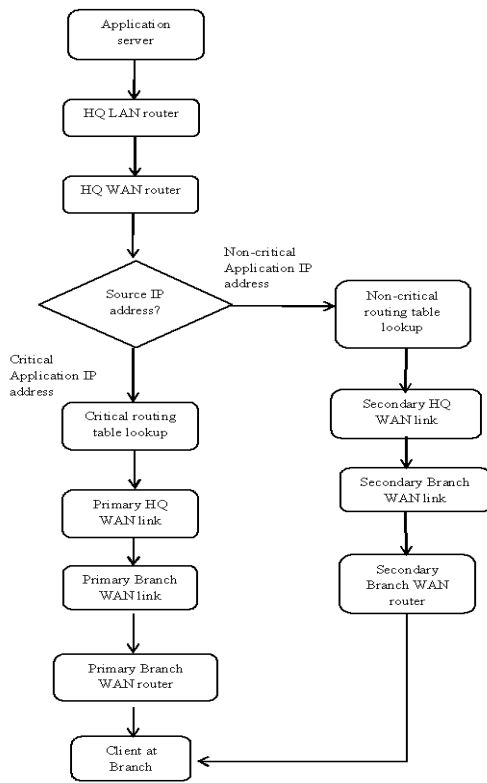


Figure 7: App. Server to Client VRF-lite

ii. Traffic Management and Segregation Process VRF-lite

Figure 6 shows process of packet transfer from Client to Application Server with VRF-lite. Packets flow from Client at Branch to the application server at the HQ. Once the client initiates the connection to the application server, the packets flow from the Client PC to the Primary Branch WAN router. The Primary Branch WAN router makes decision whether the packets are to be routed via Primary Branch WAN link or Secondary Branch WAN link. In this setup, traffic with the destination IP address of the critical application at the HQ is routed via Primary Branch WAN link while the traffic with the destination IP address of the non-critical application is routed via Secondary Branch WAN link. All packets are routed to the HQ WAN router and to the HQ LAN router. Then, HQ LAN routed the packets to the application servers located at the HQ. Figure 7 show process of traffic flow from Application Server to Client with VRF-lite. Applications at the HQ are defined in two categories which are critical application and non-critical application. Here, FTP application is defined as the critical application while the HTTP application is defined as the non-critical application. The VRF-lite method enabled HQ router to have two different routing table simultaneously in the router. The first routing table is to maintain the forwarding and receiving traffic of the IP address for the critical application (FTP) while the other routing table is to forwarding and receiving traffic of the IP address for the non-critical application (HTTP). When HQ router received the packets from branch, the HQ will forward the traffic to its LAN which contained FTP and HTTP server. To make sure the return traffic from the HQ to the Branch flows in the right direction which are whether through the Primary Branch

WAN link or through the Secondary Branch WAN link, the VRF-lite is playing the most vital role in segregating the traffic. Hence, both primary and secondary link of the HQ and Branch is being utilized when applying the VRF-lite traffic segregation method at the HQ router.

C. Data collection

File transfer via FTP and HTTP is used in the test bed setup to generate the traffic. Two different type of the protocol is used to imitate the traffic in the enterprise network that are consists of different type of traffic which are FTP and HTTP. FTP is defined as the critical traffic while HTTP is defined as the non-critical traffic. The traffic flows from HQ to branch and user at branch downloaded data from HQ.

IV. RESULT AND ANALYSIS

Table 1 shows the listed the measured throughput and bandwidth utilization of all five monitored links during the file transfer via FTP and HTTP. There are two types of the scenario which is without traffic management and with traffic management with VRF-lite technique is collected.

A. Without Traffic Management VRF-lite

Branch is utilized the Primary Branch WAN link. At this time, the client at the branch is downloading 100 MB file at the HQ server via HTTP and FTP simultaneously and the Primary Branch router is handling all the traffics. Graph shows that the bandwidth utilization of the Primary Branch WAN link is very high which is utilized approximately 100% of the link. The red light in the graph at the Primary Branch WAN link graph indicated that the link is under critical condition and the congestion is occurred. Figure 9 shows that the bandwidth utilization at the Secondary Branch WAN link is low. During this time, the secondary branch is in the standby mode. No data traffic is flowing through the secondary Branch WAN link Graph presented that there is some bandwidth utilization at the link which is around 0.05% on the average. The bandwidth of the link is utilized by the routing protocol BGP and EIGRP in sending hello, keep alive message and updates to the neighboring routers in order to converge, maintain and updating routing table.

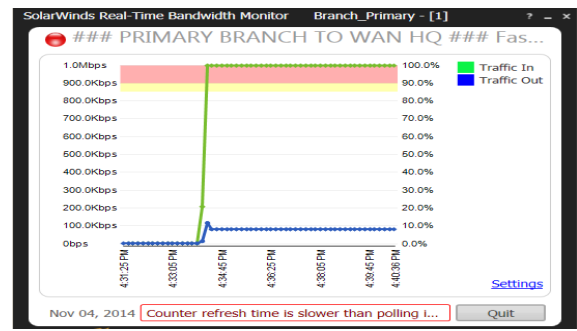


Figure 8: Primary Branch WANw-VRF-lite

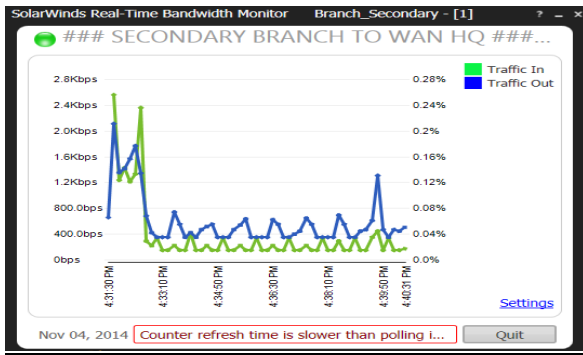


Figure 9: Secondary Branch WAN w-VRF-lite

Figure 10 shows the bandwidth utilization at the LAN link of the branch which is 1.38 % of the links. Unparalleled growth in bandwidth of the WAN-LAN link can cause congestion at the WAN link as in this graph. LAN link shows bandwidth is utilized only 1.38 % with the amount of 1.38 Mbps which is from the LAN point of view is very low. There is around 98.62% is not being utilized yet by the user. However, at the WAN link in Figure 11, the bandwidth of the link has been utilized 100% with the amount of 1 Mbps. From the throughput of the data transferred itself that we can see that there is 0.38 Mbps of the packets was dropped during the transfer. At the HQ link, Primary HQ WAN link is being used to transfer the data from the HQ to the branch. Figure 12 shows that 7.5% of the link bandwidth is being utilized in order to transfer the 100 Mb file via FTP and HTTP simultaneously. Since the Secondary Branch WAN link is not being utilized, the Secondary HQ WAN link is also not being used in data transfer because it is directly connected to the Secondary Branch link which the situation is as similar as Secondary Branch WAN link.

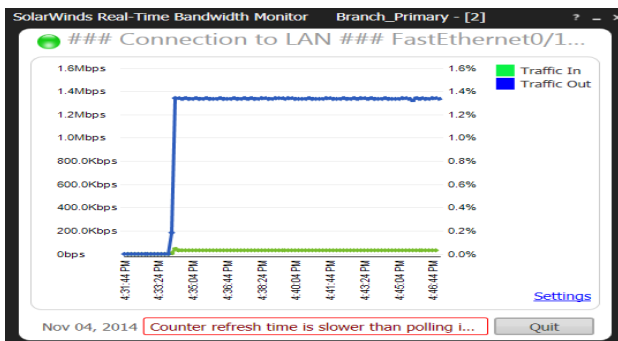


Figure 10: Branch LAN w-VRF-lite

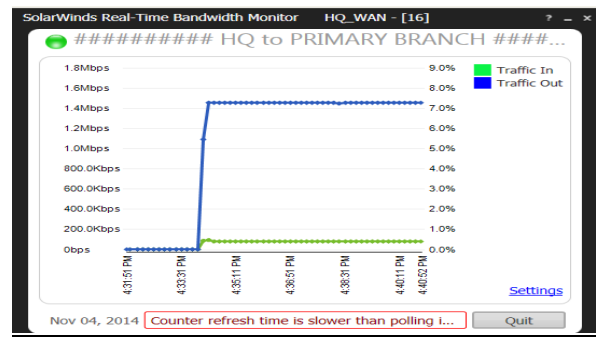


Figure 11: Primary HQ WAN w-VRF-lite

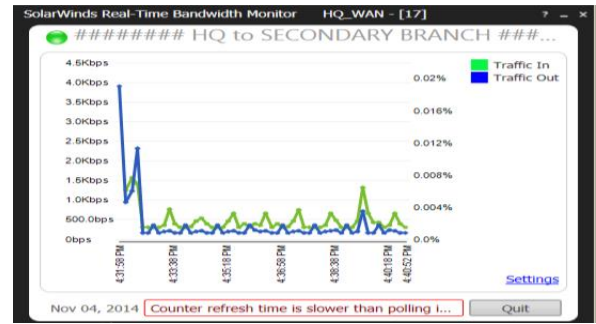


Figure 12: Secondary HQ WAN link w-VRF-lite

B. Traffic Segregation VRF-lite applied at HQ

Figure 13 and 14 respectively shows the bandwidth utilization of the Primary Branch WAN link is 58% while the bandwidth utilization for the Secondary Branch WAN link is 85%. The Primary Branch WAN link is utilized to request and receive the FTP data while the Secondary Branch WAN link is utilized to request and receive the HTTP data during the simultaneous file transfer from HQ to Branch via HTTP and FTP. Graph shows that during simultaneous file transfer, the Primary Branch WAN link is not congested with the high traffic and the Secondary Branch WAN link also being utilized. The load balance and utilization of both links at one time is achieved. Path diversity and partial loss of information is also applied in this situation. If the Primary Branch WAN link is disconnected or down, only the FTP file transfer is interrupted while the HTTP file transfer is not interrupted. Hence, only partial data is lost which are data transferred via FTP. This situation is also applied on the other way around. During the outage for one of the links, only some application is affected and the Branch will not be experiencing total loss of connection to the HQ.

Figure 15 shows file transfer and Branch LAN link utilization is 1.38% with the amount of 1.38 Mbps. The Branch LAN do not experienced with packet loss since there is no congestion occur the LAN-WAN link. The total WAN utilization is 1.48 Mbps with 590 Kbps and 890 Kbps for Primary Branch WAN link and Secondary Branch WAN link respectively. The total outgoing traffic at both WAN links is higher than the outgoing traffic from the LAN. The Primary HQ WAN link is used to transfer FTP data from FTP server to the FTP client at the Branch while the Secondary HQ WAN link is used to transfer HTTP data from the HTTP server at HQ to the HTTP client located at the Branch. Figure 16 and 17

present and indicated that during the simultaneous file transfer, utilization of the Primary HQ WAN link is 2.9% of the link with the amount of 590 Kbps while the Secondary HQ link is being utilized at 4.5% of the link with the amount of 890 Kbps.

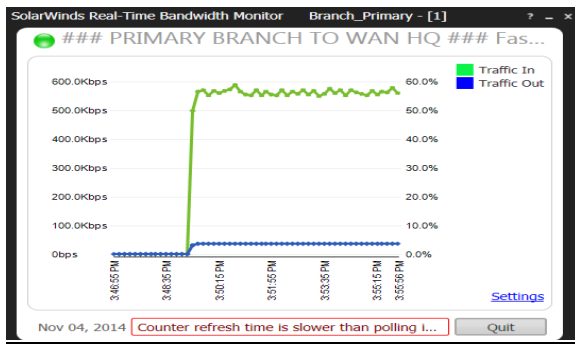


Figure 13: Primary Branch WAN link VRF-lite

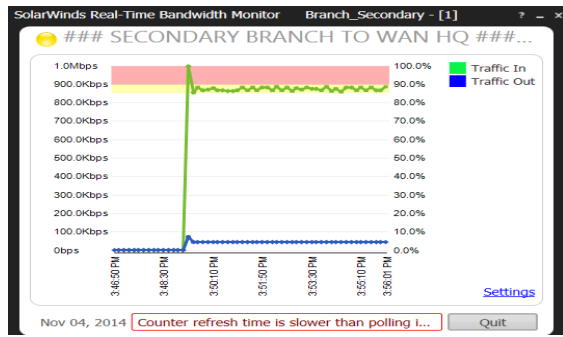


Figure 14: Secondary Branch WAN link VRF-lite

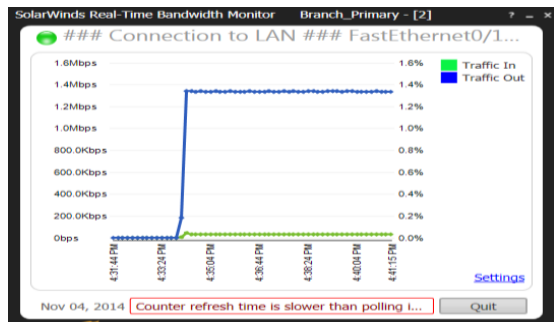


Figure 15: Branch LAN link VRF-lite

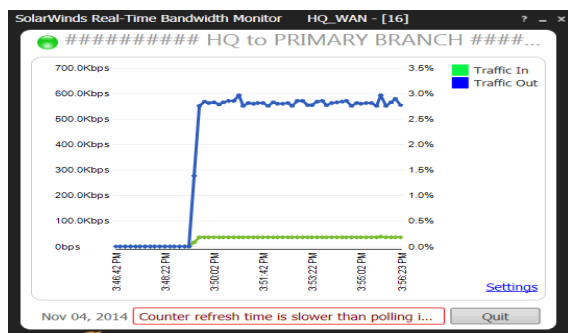


Figure 16: Primary HQ WAN link VRF

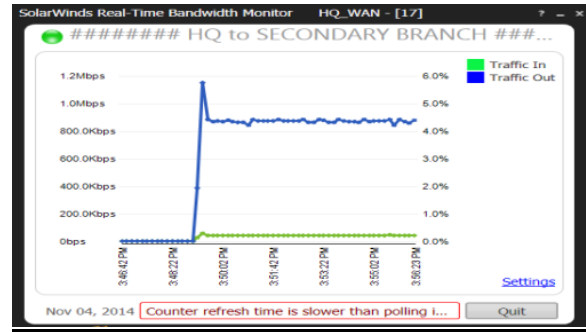


Figure 17: Secondary HQ WAN link VRF-lite

V. CONCLUSION

This research concludes that all objective are achieved where traffic management with VRF-lite on MPLS VPN are analyzed. QoS on bandwidth utilization of the stimulated enterprises network are implementation with simulation test bed as real MPLS VPN network. Result proven that by applying VRF-lite method at the HQ router, the congestion at the Branch WAN link can be avoided. In addition, VRF-lite are enabled both of the links whether at the HQ or the Branch is utilized and hence the load balanced and path diversity can be applied at the network. Overall performances of the network are increased.

REFERENCES

- [1] N Chaitou M, "On the calculation of inter-domains point to multipoint paths in MPLS networks," *International Journal of Network Science*, vol. 1, no.1, pp. 80-100, 2016.
- [2] El Hachimi, M., Breton M. A. and Bennani. M., "Efficient QoS implementation for MPLS VPN," *22nd IEEE International Conference on Advanced Information Networking and Applications-Workshops*, 2008.
- [3] Ab Rahman R, Alias FA, Kassim M, Yusof MI, Hashim H., "Implementation of high availability concept based on traffic segregation over MPLS-TE," *ARN Journal of Engineering and Applied Sciences*, vol. 10, no. 3, pp. 295-301, 2015.
- [4] Sairam, A.S. and Barua. G., "Effective bandwidth utilisation in multihoming networks," *IEEE First International Conference on Communication System Software and Middleware (Comsware)*, 2006.
- [5] Kyandoghere, K., "A customized service availability concept based on traffic segregation, path diversity and hierarchical restoration," *Proceedings of the Third IEEE International Conference on public telecommunication transport networks in Electronics, Circuits, and Systems) ICECS'96*, 1996.
- [6] Cisco. Cisco IOS IP Switching Command Reference: Configuring VRF-lite patent Software Configuration Guide - Release 12.2(31)SG. (2011).
- [7] Gobena Y, Durai A, Birkner M, Pothamsetty V, Varakantam V, "Practical architecture considerations for Smart Grid WAN network," *IEEE Power Systems Conference and Exposition (PSCE), IEEE/PES* 2011.
- [8] Cisco. Layer 3 MPLS VPN Enterprise Consumer Guide Version 2. ug 8 2008. Available from: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/L3VPNCon.html. Accessed 1st Feb 2016, 2016.
- [9] Parra, I.M.O.J.S., D.G.L. Rubio, and I.M.L., Castellanos. MPLS/VPN/BGP Networks Evaluation Techniques, 2012.
- [10] Zhao, Y. and Z. Deng, "A Design of WAN Architecture for Large Enterprise Group Based on MPLS VPN," *International Conference on Computing, Measurement, Control and Sensor Network.*, 2012.
- [11] Polezhaev, P., A. Shukhman, and Y. Ushakov, "Implementation of dynamically autoconfigured multiservice multipoint VPN," *9th IEEE International Conference on Application of Information and Communication Technologies (AICT)*, 2015.

- [12] Theodoro L. C, Leite PM, de Freitas HP, Passos ACS, de Souza Pereira JH, de Oliveira Silva F., “Revisiting Virtual Private Network Service at Carrier Networks: Taking Advantage of Software Defined Networking and Network Function Virtualization,” *The Fourteenth International Conference on Networks*, 2015.
- [13] Raspall, F., “Building Nemo, a System to Monitor IP Routing and Traffic Paths in Real Time,” *Computer Networks*, 2016.
- [14] Nagaraja, M.G., R.R. Chittal, and K. Kumar, “Study of network performance monitoring tools-SNMP,” *International Journal of Computer Science and Network Security*, vol. 7 no. 7, pp. 310, 2007.

Table 1
Bandwidth Utilization of the link

Scenario	Throughput and Percentage Bandwidth Utilization on the link				
	HQ Primary WAN (BW =20MB)	HQ Secondary WAN (BW=20MB)	Branch Primary WAN (BW=1MB)	Branch Secondary WAN (BW=1MB)	Branch LAN (BW=100 MB)
Without Traffic Management	1.42 Mbps, 7.5%	1 Kbps, 0.07%	1 Mbps, 100%	2.5 Kbps, 0.08%	1.38 Mbps, 1.38%
Using Traffic Segregation, VRF-lite applied at HQ	590 Kb, 2.9%	890 Kb, 4.5%	590 Kb, 58%	890 Kb, 85%	1.38 Mbps, 1.38%