JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN COMPUTER ENGINEERING

ANALYSIS OF QOS ENABLED MPLS VPN VOIP NETWORK WITH RIPV2 ROUTING PROTOCOL.

[1] MR. DHAVAL PARMAR, [2] DR. T. P. PATALIA

[1]M.E.[Computer Engineering] Student, Department Of Computer Engineering, V.V.P Engineering Collage, Rajkot, Gujarat, India.
[2] Dr. Tejas.P.Patalia, Head & Associate Professor, Computer Engineering Dept., V.V.P. Engineering Collage, Rajkot, Gujarat, India.

dhaval2006ind@googlemail.com, pataliatejas@rediffmail.com

ABSTRACT: ***MPLS (Multiprotocol Label Switching) based VPN (Virtual Private Network) introduced for overcome many disadvantages (security, cost, Large network management, delay, traffic malfunctioning, etc.) of traditional IP, ATM and Frame relay networking. MPLS VPN makes possible to interconnect the remote sites and workers through secure and reliable links by using public internet backbone. In this paper, analyze the behavior of RIPv2 (Routing information protocol version 2) based MPLS VPN architecture by using intense VOIP traffic with help of OPNET simulation process and unique network architecture. At last, the conclusion is made that RIPv2 based MPLS VPN architecture has produce VPN delay, LSP delays and p2p Queuing delay so it is not best solution for the large network environment.***

Keywords—Routing Protocol, RIPv2, IP, VoIP, MPLS, VPN, QoS, MPLS-VPN

I: INTRODUCTION

Voice over Internet Protocol (VoIP) becomes recently popular in industry which provide voice communication over traditional IP networks like Internet and Public Switched Telephone Network (PSTN). VoIP comes with function of converting voice signals into digital signals and transmits over Internet[1]. It still require good packet switching technology to overcome delay and provide real-time voice services. MPLS (Multi Protocol Label Switching) introduced for faster data transmission and QoS (Quality of Service) enabled secure network with VPN (Virtual Private Network) to enhance the speed and accuracy over public network backbone[2]. RIPv2 (Routing Information Protocol version 2) can be used to run as a IGP (Interior Gateway Protocol) for a network infrastructure situated within large distance[3]. The purpose of this paper is to analyze VoIP with QoS in MPLS VPN backbone in terms of parameters like delay, load, packet loss, throughput , bit errors etc..[1].

II: NETWORK INFRASTRUCTURE WITH SITE TO SITE VPN ENABLED MPLS NETWORK IN ENTERPRISE.

It becomes hard to isolate the actual network design in virtual environment and also predict the behaviors of MPLS VPN infrastructure because of variety of network design available. For the simulation purpose the OPNET is used to derive the network infrastructure and obtain the data for analysis. Some implementation factors could be also involved in the network such as VoIP traffic, voice codec, TOS (Types of Service) etc[1]. QoS is the main factor to prioritize the voice traffic within the network backbone. Interior Gateway Routing protocol needs to configure for the devices within a sites of VPN in inside network. The network backbone is designed as 70% of all link capacity is only allows VoIP traffic to protect it from bursts. The network topology needs to design to perform simulation. VoIP traffic will be used across the desired network. For populating voice traffic the backbone need to be created and for that MPLS VPN scenario is used. Simulation is used to analyze the behavior of network backbone with different metrics like VPN delay, Load and throughput. Interior gateway protocols RIPv2 is used to perform the routing task within a backbone. Network scenario is presented in Figure-1[4]. It shows the two different VPN sites with MPLS backbone infrastructure. The voice traffic is populated within both end sites of VPN and QoS is applied throughout the network devices. RIPv2 is used as an Interior Gateway Protocol. BGP (Border Gateway Protocol) also configured within edge routers of the backbone network infrastructure. All PE and CE are BGP members. All routers within a network backbone are interconnected with PPP_SONET_OC3 (155 Mbps) links. Additionally IP QoS is configured in every router in MPLS VPN network with Priority queuing and protocol based specifications. IP address scheme is applied with different network and subnet mask associated with it. Simulation model needs the following network equipments.

1. Autonomous Systems (AS)
   AS 1 : 4 Provider Routers (P)
   3 Provider Edge Routers (PE)

AS 2 : Site 1& Site 2
2 Customer Routers (C)
1 Customer's Edge Routers (CE)

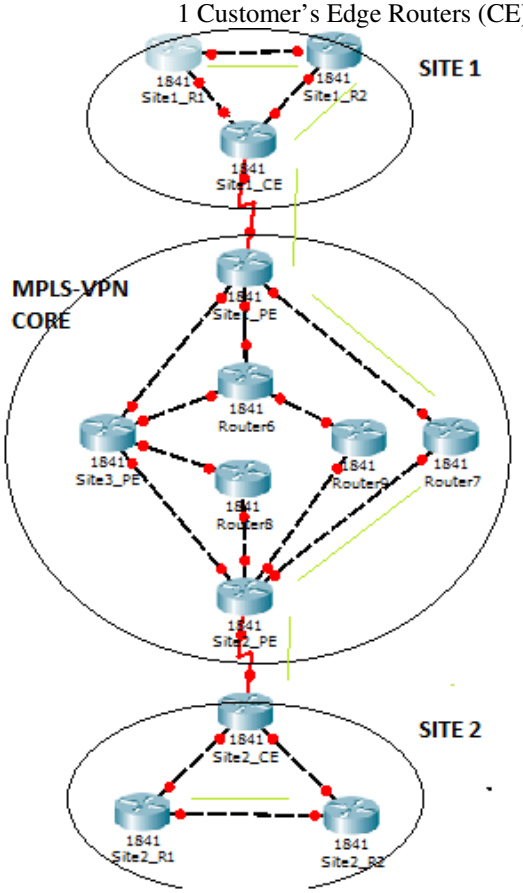

Fig.1 MPLS VPN with RIPv2

III: SIMULATION AND RESULTS

IP QoS needs to implement in every single node of the network to provide high priority for voice traffic. Two parameters can be consider to provide QoS. 1) QoS scheme : Prority Quering 2) QoS profile : Protocol Based. The VoIP traffic is used to analyze MPLS VPN because it is highly delay sensitive as compared to video and other data traffic. Here the case of VoIP traffic considered for different call rate per hour.

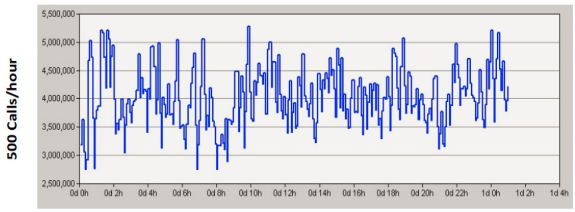

Fig.2 VoIP traffic Generated by DES (bits/sec)

The Figure-2 describe the total VoIP traffic in bits/sec. For 500 calls per hour the average traffic load in is approximately 4000000 bits/sec.

For the simulation purpose, VoIP traffic has been configured between two sites of network by using "Create Traffic Flow" option. The parameters are[6]:

1) Call rate : 500 Calls/hour
2) Call duration average : 300 seconds
3) Voice flow duration : 90000 seconds
4) Encoder scheme : Interactive voice with delay, throughput and reliability
5) Overhead (bytes): UDP/IP

For analysis of results, following discrete event simulation (DES) statistics are chosen[6]:

1) MPLS VPN :
   - VPN Delay (Sec)
   - VPN Load (bits/sec)
   - VPN Throughput (bits/sec)
2) IP background traffic Delay (Sec)
3) Flow Delay (Sec)

As from the existing study in this field the 25 hours of timestamp is selected to perform operation. IGP in this case is chosen RIPv2 and it become transient with the lower timestamp than 25 hours [5]

1) MPLS VPN: VPN Delay (Sec)

This statics provide delay between two sites of VPN in MPLS VPN. The delay is measures as time takes between first and last PE of providers network. It means VPN delay is not physical link delay. The maximum end-to-end delay for MPLS VPN infrastructure is 400MS.

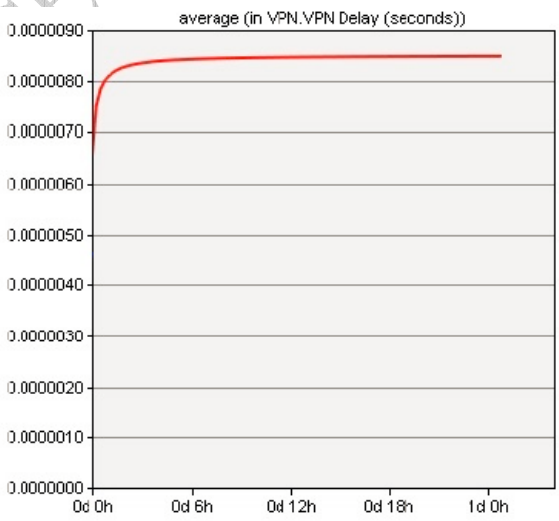

Fig.3 VPN Delay for 500 VoIP calls

Figure-3 shows the VPN delay for 500 VPN calls per hour. The sample mean for VPN delay for RIPv2 is 8.38E-006.

VPN Load and Throughput (bits/sec)

The network throughput and load are main entity that ensure how the network is capable of handling the traffic. Load stands for amount of VPN-traffic entering the "Provider's Network" through first router of backbone which is PE. While, Throughput stands for the amount of VPN-traffic leaving the "provider's Network" through last router of backbone i.e Egress PE. Statistics are measured in bits per seconds.

MPLS VPN			
			RIP v2
VPN LOAD	Sample Mean		3,863,662.369
	Variance		83,733,909,515.660
	Standard Deviation		289,368.121
	Confidence Interval	90%	3,815,821.508--3,911,503.231
		95%	3,806,660.492--3,920,664.247
		99%	3,788,774.699--3,938,550.040
VPN THROUGHPUT	Sample Mean		3,873,168.332
	Variance		83,493,180,614.371
	Standard Deviation		288,951.866
	Confidence Interval	90%	3,825,396.289--3,920,940.374
		95%	3,816,248.452--3,930,088.212
		99%	3,798,388.387--3,947,948.276

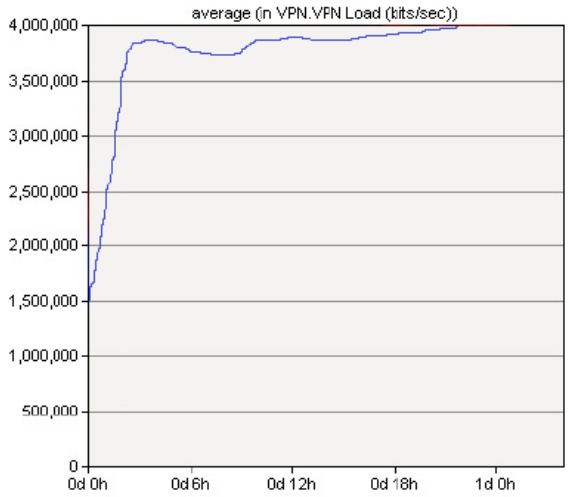

Fig.4 VPN Load (bits/sec) For 500 Voice Calls

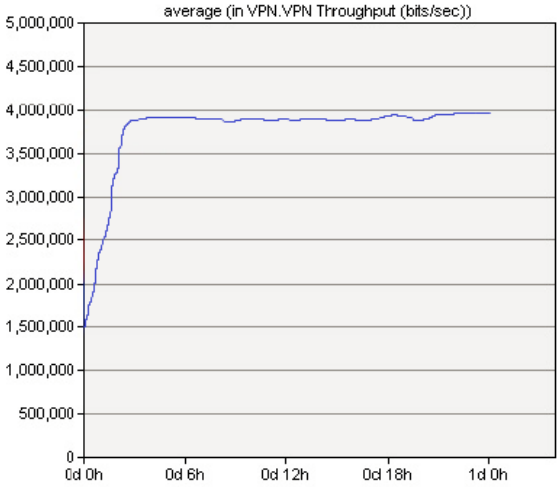

Fig.5 VPN Throughput (bits/sec) For 500 Voice Calls

Table 1: VPN Load & Thoughput (bits/sec) For 500 Voice Calls

Figue 4,5 and Table 1 shows the VPN Load and VPN Throughput in bits/s for 500 VoIP calls per hous. In this case RIPv2 is consider as IGP. It is observed that sample mean of VPN load for RIPv2 is 3,863,662.369 bits/s. While the sample mean of VPN throughput for RIPv2 is 3,873,168.332 bits/s.

2) IP Background traffic delay (sec)

Travel time of traffic in background is statically measure at flow from the flow source to the flow destination. This statistic is recorded only for those flows whose source is this node, on a per-flow basis.

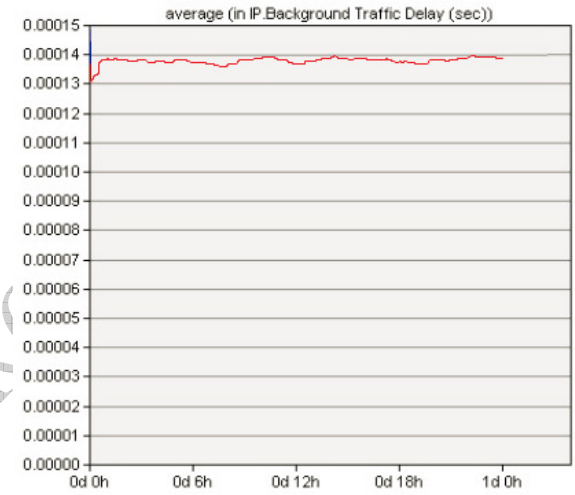

Fig.6 Bkg Traffic delay(sec) For 500 VoIP Calls

Table 2: Bkg Traffic delay(sec) For 500 VoIPCalls

	MPLS VPN	
		RIPv2
Sample Mean		0.0001382
Variance		1.319E---013
Standard Deviation		3.632E-007
Confidence Interval	90%	0.0001381769-.0001381924
	95%	0.0001381754-0.0001381939
	99%	0.0001381726-0.0001381968

From Figure-6 and Table 2 it is observed that the RIPv2 has introduce delay for VoIP background traffic in MPLS VPN backbone. Sample mean of traffic delay for RIPv2 is 0.0001382s.

3) Flow Delay (Sec)

Delay is observed by packet belonging to a specific flow in the LSP. Time spent by a a packet of a given flow inside the Label Switched Path. The statistics

will be anotated with the source-destination IP addresses and LSP name at the end of the simulation run.

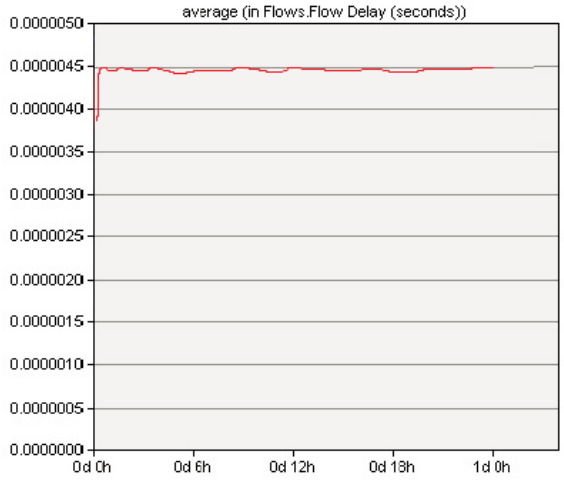

Fig.7 Flow Delay between Sites For 500 VoIP Calls

Table 3: Flow Delay between Sites For 500 VoIPCalls

		MPLS VPN
		RIPv2
Sample Mean		4.495E-006
Variance		8.303E-015
Standard Deviation		9.112E-008
Confidence Interval	90%	4.480E-006, 4.510E-006
	95%	4.477E-006, 4.513E-006
	99%	4.472E-006, 4.519E-006

Figure 7 and Table 3 provides detail statistical of the packet flow delay in the LSP of MPLS VPN from Site1_PE to Site3_PE with respect to RIPv2 routing protocol. The sample mean of packet flow delay for RIPv2 is 4.50E-006s

IV: CONCLUSION

The main objective of this paper " Analysis of QoS Enabled MPLS VPN VOIP Network with RIPv2 Routing Protocol" is to analyze the potential behavior of MPLS VPN with QoS with OPNET simulation. It also found the challenges deploying MPLS VPN with Interior Routing Protocol (RIPv2) and Exterior Routing Protocol (BGP) and QoS for the whole infrastructure for priories the Voice traffic. The statistical data is derived from the various VPN statistics like delay, load, throughput and flow delay. The statistical data and analysis prove that the RIPv2 is still a good enough routing protocol to deploy within the MPLS VPN architecture. And this architecture is scalable and flexible enough to provide well-organized voice packet transmission, load balancing, consistency, data security, network isolation from networks and end-to-end controlled connectivity with QoS guaranteed. Also proves the RIPv2 routing protocol can be deploy within a medium range network infrastructure as it acquire non transient state as the time passes.

REFRENCES

[1] Tamási Levente, Orincsay Dáiniel, Józsa Balázs Gábor, Magyar Gáibor "Design of survivable VPN based VoIP networks" *Design of Reliable Communication Networks.IEEE*, [2005].

[2] Isaias Martinez-Yelmo, David Larrabeiti, and Ignacio Soto, Universidad Carlos III de Madrid
Piotr Pacyna, AGH University of Science and Technology "Multicast Traffic Aggregation in MPLS-Based VPN Networks" *IEEE Communication Magazine, October* [2007]

[3] Chen, Jui-Fa ; Lin, Wei-Chuan ; Bai, Hua-Sheng Dai,Shih-Yao "Messages interchange protocol based on routing information protocol in a virtual world" *Advanced Information Networking and Applications*, [2005]

[4] Geng, Rong ; Guo, Lei ; Wang, Xing-Wei Wei "QoS-Aware Multipath Routing Protocol based on local information for Ad Hoc networks" *Computer Engineering and Technology (ICCET),2nd International Conference* [2010]

[5] Wang, Bin, Zhang, Jian-hui, Chen, Wen-Ping, Guo, Yun-fei "A Fast Reroute Mechanism for RIP Protocol" *Circuits, Communications and Systems. PACCS '09. Pacific-Asia Conference on* [2009]

[6] Zong-Hua Liu, Student Member, IEEE, Jyh-Cheng Chen, Senior Member, IEEE, and Tuan-Che Chen, Student Member, IEEE "Design and Analysis of SIP-Based Mobile VPN for Real-Time applications" *IEEE Transactions on Wireless Communications, Vol. 8, No. 11, November* [2009]