IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 2, Ver. II (Mar.-Apr. 2017), PP 12-19
www.iosrjournals.org

Voip on IP PBX System Using Secure VPN Communication and Delay Analysis

Md. Mahbubur Rahman[1], Kazi Md. Shahiduzzaman[2], B.K. Karmaker[3], Md. Mehedi Hasan Khan[4]

[1]Lecturer, [2,3]Assistant Professor, Department of Electronics and Communication Engineering, Jatiya Kabi Kazi Nazrul Islam University (JKKNIU), Bangladesh
[4]MIS Manager, Kwun Tong Apparels Ltd.

Abstract: *VoIP (Voice over Internet Protocol) is the next generation telecommunication whereas traditional telecommunication systems have disadvantages on IP networking, ATM, Voice and Data communication. Security breaches, maintaining large network, QoS are important issues associated with communication. These led us to research and introduce virtual private network (VPN) for voice and data communication on hybrid private branch exchange (PBX). It can be implemented over the skeleton of existing architectures that helps organizations connect the spread out sites and distributed workers through a secure VPN using the existing public or private network. Voice can be transferred on secure VPN backbone and delay analysis of the network is the main objectives and IP PBX or SIP server which is used for voice gateway. Network simulation helps to analyze the possible problems of the data and delay which make us more confident of this research.*

Keywords: *H.323, IP, PBX, VoIP, VPN, SIP*

I. Introduction

The internet is a communication system which interconnects computers and gives information globally. A lot of service depends on internet like e-mail, website, data and software etc. Voice transfer through internet which is called VoIP. Its low cost led massive business in next generation Telecommunication. Not only voice transfer but also video calls and video conferencing are possible now a day. New software introduces with new features and grows business in international market. Security is important while growing software activities. For the stability, vulnerability of software and hardware we must ensure security. Therefore, in this paper our main objective is to secure the VoIP communication on IP PBX system and delay analysis. IP PBX is a hardware which is used for VoIP calls and easier to web based configuration or software which can transfer voice using Session Initiation Protocol (SIP) protocol. This hardware supports SIP trunks, E1/T1 trunk from Public Switched Telephone Network (PSTN), Foreign Exchange office (FXO) and Foreign exchange subscriber (FXS). Security threats on VPN are a big issue when tunneling two different networks. This paper will cover security policy while VoIP calls transmitted on VPN network using IP PBX system.

IP PBX delivers multi-functions and high performance. Simple management, reduced communication cost, seamless connectivity with remote users and between geographically dispersed branches which are the benefits of using the system. The system ensures open-standard SIP protocol and is hence interoperable with SIP proxies, gateways and IP phones. Communication of small and mid-sized enterprises as well as geographically distributed offices, remote workers and contact centre is much simplified and enhanced with IP PBX system.

Why security is needed for VoIP? Tremendous growth of voice traffic security is most important issue. For this reason, we are going to discuss the threats and how to mitigate by using secure VPN network in this paper.

In section 2, we have described the major securities on VPN network. To secure data and voice traffic these security options may help to an organization's IT infrastructure also. Any organization must think about secure information sharing comprehensively otherwise weak protection may harm the information which will create huge loss of that organization. Few people would argue with the idea that a data network needs to be secure but the same security is needed for voice also because the attacks aren't new not only for data network but also telecommunication environment. They can expose the worms and viruses and hacks the network. We are using OPNET simulation tool to optimize the network delay.

II. Techonology And Security Process For Voip

To overcome attacks on VoIP network, new technology and security issues are discussed in this section.

1. Proposed Technology

New technology is provided here for securing voice communication on a VPN infrastructure [1-2]. VPN can provide a secure and inexpensive communication mechanism that is an extension of the public internet through a private network. Private tunnels ensure point-to-point communication and data transfer. We discuss some experiments how securely transfer voice over IP communication using VPN. For this purpose we prepare a windows 2003/2008 server with PPTP VPN service and a Linux server machine and SIP enabled Software or Hardware IP PBX system [3-5].

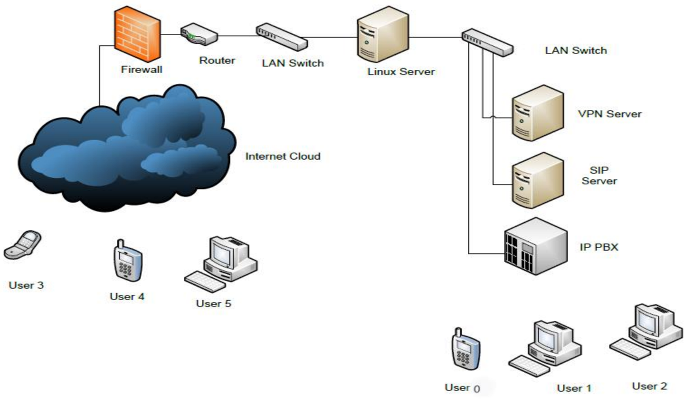


Figure 1: Proposed Secured Network

There is a firewall box which protects from various malicious attacks first from internet cloud. It can be server or hardware firewall [6]. Hardware firewall is a built-in firewall system of an individual operating system. Server based firewall is configured by an individual whatever he likes by his decision. Iptables firewall can be used in the server [7]. Various types of attacks are possible from the internet cloud to this server (firewall). So protection is most important. All the devices have individual firewall system in our infrastructure. First firewall can protect DoS (Daniel of Service) attack, Malware and other attacks and also ensure the port and public IP authentication. Figure 1 we find router after the firewall system which can route the voice / data. It has strong firewall that is called ACL (access control list) build by Cisco system [8]. Not only Cisco system now a day's many companies build router and add specific security system. Router has the capability of checking authorized IP block and ports. It also manages 802.1 q techniques. Then there is manageable LAN switch which allows the VLAN access of Linux server. Linux server has done important role in the infrastructure. It is using iptables script firewall system. Script is forwarding specific ports on VPN server and SIP server which convert private IP to public IP [9]. Linux server ensures MAC and IP based firewall to access only VPN and SIP server. VPN server has also firewall system which allows IP addresses from outside using a specific range or fixed IP or DHCP based IP addresses [10]. SIP server allows IP addresses which are allowed by VPN server.

2. Step by Step at a glance

Internet Cloud	Firewall
User/Client wants to register to SIP server / IP PBX.	Authenticate Public IP address. Protect DoS, Malware and other attacks. SIP/H.323 ports

Router	VLAN (LAN Switch)
Accept Authentic IP addresses and ports and deny others IP address access.	Decrease broadcast domain and ARP attacks.

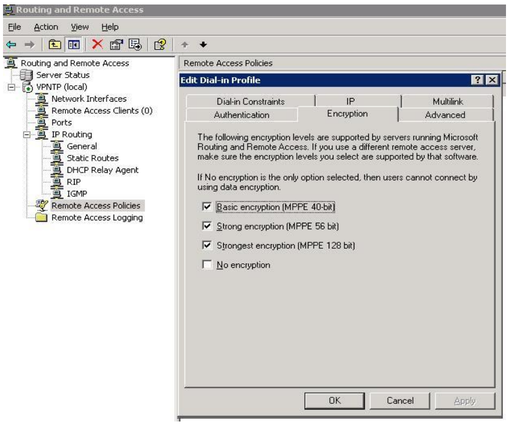
Linux Server	VPN Server
Filter IP address, MAC and Ports[We should protect Linux server (root access, authorized IP addresses for Administration, checking logs, disable unnecessary services and disable unnecessary ports)]	VPN server checks the authentic IP address and authorized users in the database or any other authentic method and finally encrypts the voice/data.

SIP Server/ IP PBX
SIP Server/IP PBX will check the authorized IP address, MAC address, port and authorized user then the user will be registered.

3. Implementation Process of Security Issues

Windows 2003/2008 server has PPTP VPN service which is enabled with Static IP and MAC authentication. So when any terminal connected with VPN then it gets a private IP Address and verifies MAC then it authenticates for VoIP services.

There are some figures from 2 to 5 shows how the security policies are ensured



The following encryption levels are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the encryption levels you select are supported by that software.

If No encryption is the only option selected, then users cannot connect by using data encryption.

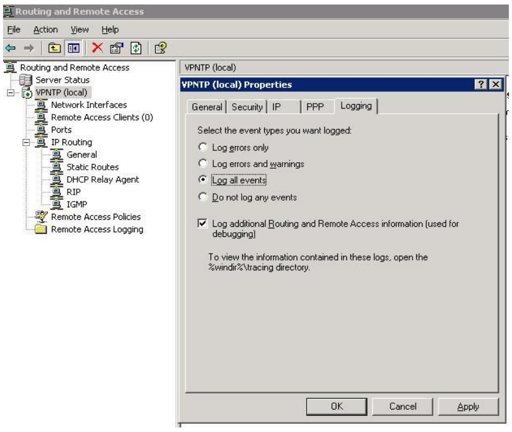
☑ Basic encryption (MPPE 40-bit)

☑ Strong encryption (MPPE 56 bit)

☑ Strongest encryption (MPPE 128 bit)

□ No encryption

Figure 2: Encryption algorithm for PPTP VPN



Select the event types you want logged:

○ Log errors only

○ Log errors and warnings

● Log all events

○ Do not log any events

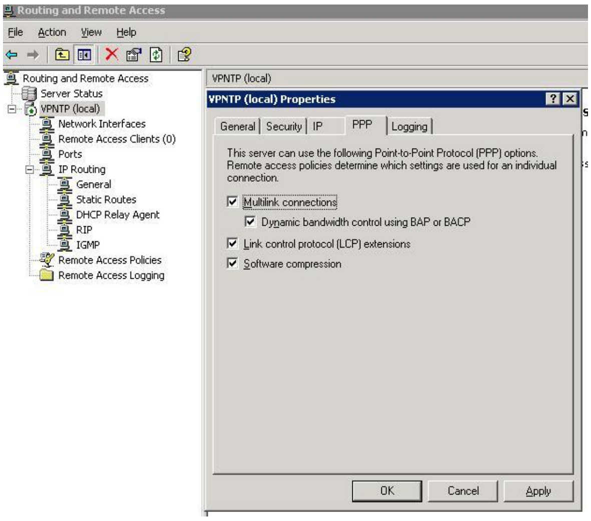
☑ Log additional Routing and Remote Access information (used for debugging)

To view the information contained in these logs, open the %windir%\tracing directory.

Figure 3: Log analysis for VPN users

The Figure 2 has shown some encryption levels supported by servers running Microsoft routing and remote access. The encryption techniques are Basic encryption (MPPE 40-bit), Strong encryption (MPPE-56 bit) and Strongest encryption (MPPE 128 bit). If we don’t use any of this encryption just tick mark on No encryption. We get this feature from remote access policies.

The Figure 3 shows how all the event logs file are stored in the windows system. There are some options: log errors only, log errors and warnings and log all events. If we don’t need any of these options just tick mark on Do not log any events. We get this option from VPNTP (local) properties.



This server can use the following Point-to-Point Protocol (PPP) options. Remote access policies determine which settings are used for an individual connection.

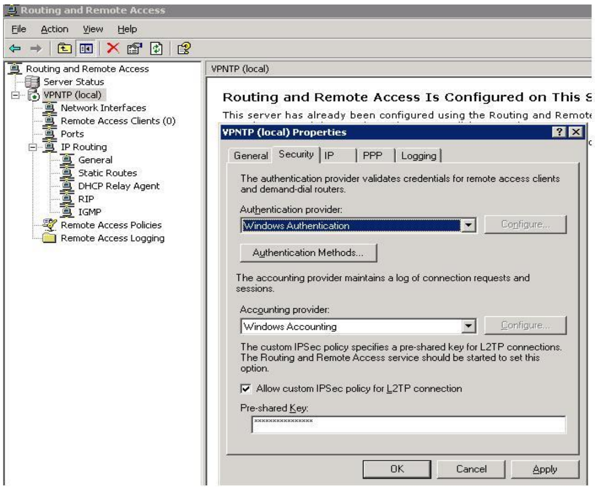
☑ Multilink connections

☑ Dynamic bandwidth control using BAP or BACP

☑ Link control protocol (LCP) extensions

☑ Software compression

Figure 4: Remote connection type for an individual



Routing and Remote Access Is Configured on This S

This server has already been configured using the Routing and Remote

The authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider: Windows Authentication

The accounting provider maintains a log of connection requests and sessions.

Accounting provider: Windows Accounting

The custom IPSec policy specifies a pre-shared key for L2TP connections. The Routing and Remote Access service should be started to set this option.

☑ Allow custom IPSec policy for L2TP connection

Pre-shared Key: ****************

Figure 5: Authentication provider validates credential for remote access clients

The Figure 4 shows some Point to Point (PPP) options which settings are used for an individual connection. These are Multilink connections, Link control protocol (LCP) extensions and Software compression [8] [11]. This option is found from VPNTP (local) Properties. While Figure 5 shows the authentication provider validates credential for remote clients and demand-dial routers. We can use different authentication methods but here we using Windows authentication method. The custom IPSec policy specifies a pre-shared key for L2TP connections. The routing and remote access service should be started to set this options. Here we can set our own pre-shared key.

1. In Linux server we configure MAC based NAT firewall which becomes an authentication part when any terminal connect for VoIP as well as internet connection.

iptables -A FORWARD -i ethX -o ethY -s X.X.X.X -m mac --mac-source 00:24:21:25:E0:35 -j ACCEPT

2. Here we configure VPN server with Private IP address so that VPN server could not be hacked by the Hackers [12-13]. Linux server firewall will forward VPN server's private IP to public IP. So it will be more secure to ensure VoIP communication.

iptables -t nat -A PREROUTING -p tcp -d <Public IP> --dport 1723 -j DNAT --to-destination < Private IP of VPN Server>

iptables -t nat -A PREROUTING -p 47 -d <Public IP> -j DNAT --to-destination <Private IP of VPN Server>

For server security we remove default port to access the server.

Port 22 [We change it to another port number]

IP based access to server:

sshd:<Allow host IP >

We deny public IP address to access the server because if we allow public IP address its vulnerable and attacker can attack this server easily. The default configuration is allowed all IP addresses.

sshd: ALL

We should check the ports which are running on the server and stop the unnecessary ports and services.

PORT	STATE	SERVICE
22/tcp	open	Ssh
53/tcp	open	Domain
113/tcp	open	Auth
953/tcp	open	Rndc
3128/tcp	open	squid-http
10000/tcp	open	snet-sensor-mgmt

VPN tunnel users will login access 2 times (VPN Software Restriction) if wrong password then it will suspend 2 hours for that user.

SIP Authentication for user login in dialer 2 times (Dialer Restriction) if wrong password then it will also suspend 2 hours.

If any user login failed after 2 hours, then user account will be inactive. Then the user will contact will the administrator to active.

Password type: Capital letter, Small letter, Symbol and Number.

Length: 10

Encryption: Enabled

Some persons should be dedicated for checking the firewall, Router, Linux server, VPN server and IP PBX access log. If any unauthorized access found, then immediate action should be taken. Every server has access log option and very easy to monitor the logs. Unauthorized access checkup or system access privilege should be maintained carefully.

Physical security is most important and it forms the basis for many other security efforts also [14]. It refers to the protection of building sites and equipment from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage (for example, electrical surges, extreme temperatures, and spilled coffee). So it requires suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

4. Overview of security

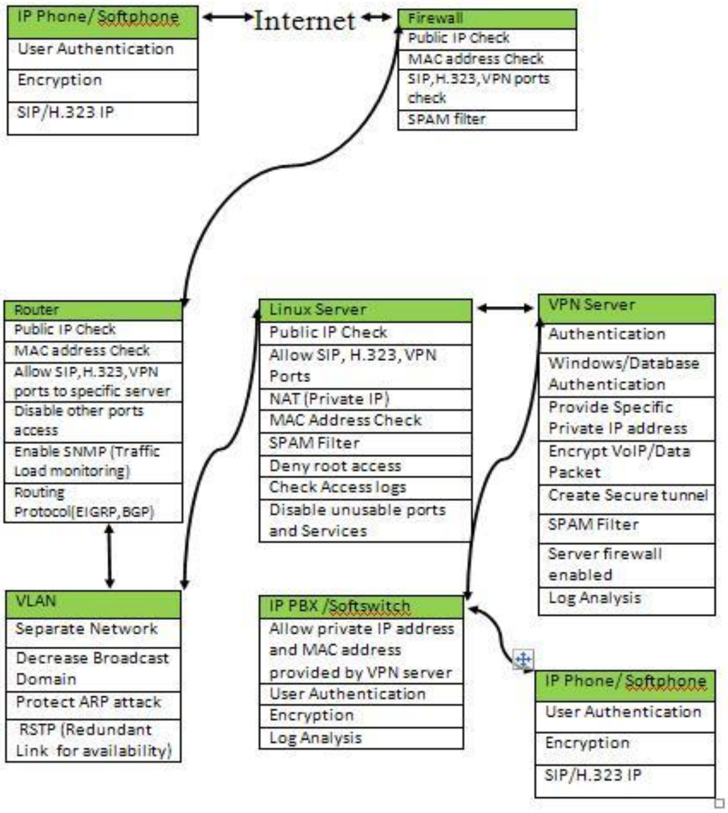


Figure 6: Overview of security policies

III. Delay Analysis Of The Proposed Network

The aim of this research is to secure the network using VPN communication and the performance of network load, delay and throughput need to analyze. So OPNET is a simulation tools to get the result of the performance based on VPN network [15]. Network delay is an important issue for VoIP communication. If latency or delay is high then calls may cut, interrupt and distort. We put up the simulation to analyze the delay. The results obtained by the simulation are analyzed to obtain the performance of the VPN based network. The vast array of design factors such as number of calls made per unit time, voice codec, VoIP traffic, type of service, etc makes it difficult to determine the behavior of PBX network based on VPN backbone. The simulation results provided concrete information on the basis of mathematical calculations. Hypothesis could be deduced from the data obtained and the feasibility of the different networks could be judged. Network A: One-star topology with 30 nodes each connected to a LAN switch 3. We can consider each node as softphone or IP Phone. LAN Switch 3 is directly connected with LAN Switch 2. VPN Server and IP PBX are also connected on LAN Switch 2. The following diagram illustrates the simulated network:

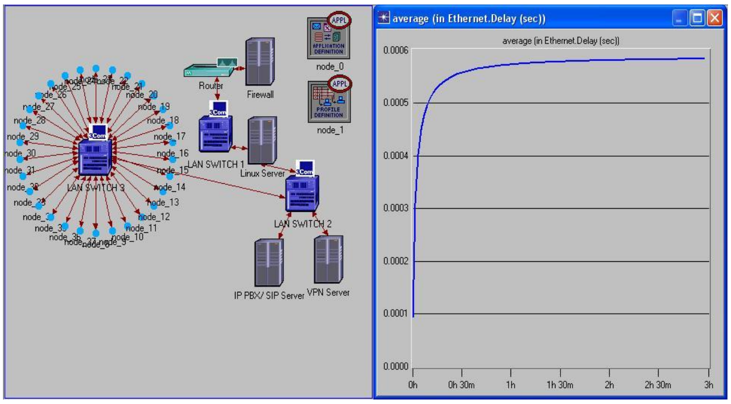


Figure 7: Network B with 30, 30 and 30 nodes in different LAN Switches.

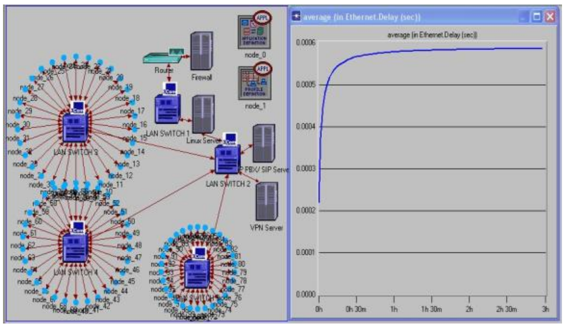


Figure 8: Network A with 30 nodes in each topology

The diagram shows the simulated network where the topology is star. The nodes are 10_BASE_T which have dedicated connection to the LAN Switch 2. On the right side are the performance graphs in terms of Delay in seconds. The delay has been analyzed for the network globally. The delay and load on the network have been measured for a time period of three (3) hours as shown on the x-axis. The load has been calculated on a scale of 0 to 800 bits/sec and Ethernet delay on a scale of 0 to 5 milliseconds. Initially, it is seen that the delay increases steeply in the first 5 minutes, after that it becomes constant at 4.75 milliseconds. It stays in that way over the next 2.55 hours. An Ethernet delay of 4.75 milliseconds is acceptable for any network architecture. The load is seen to rise steeply in the first half hour and upon reaching 675 bits/second, it attains a constant rate and stays between 600 bits/second to 700 bits/second for the remaining time. So it is seen that the Ethernet load is also at an acceptable level. Network B: Three star topologies from different networks were connected to each other with the help of LAN switches. One topology had one LAN switch containing thirty (30) nodes. Another had thirty (30) nodes and the third one with thirty (30) nodes. The diagram below shows the simulated network. The performance in terms of delay and load are also illustrated graphically in Figure 8.

The diagram reflects the simulated network where the topology is star. The nodes are 10_BASE_T which have dedicated connection to the LAN switches. On the right side are the performance graphs in terms of Delay in seconds and Load in bits/second. The delay has been analyzed for the network globally. The delay and load received on the network have been measured for a time period of three hours as shown on the x-axis. The load has been calculated on a scale of 0 to 2,000 bits/sec and Ethernet delay on a scale of 0 to 6 milliseconds. Initially, it is seen that the delay increases steeply in the first 5 minutes, after that it becomes constant at 5.7 milliseconds with small decreases at different time periods. It stays in that way over the next time period. An Ethernet delay of 5.7 milliseconds is definitely acceptable.

The load is seen to rise steeply in the first 5 minutes and upon reaching 18,00 bits/second, it comes down and attains a constant rate and stays 18,00 bits/second for the remaining time. So it is seen that the Ethernet load is also at an acceptable level. Hence we can reach the conclusion that network B has an architecture that has greater load and hence more overhead on the network. Following is a graphical representation of the results comparison between the two proposed network architectures that have been simulated.

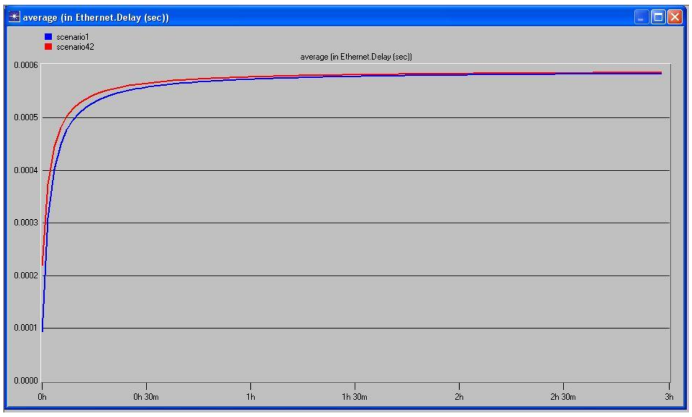


Figure 9: First Network IP PBX and VPN server's network delay and load

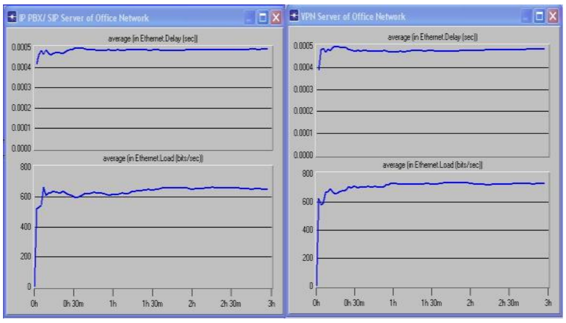


Figure 10: Comparison of the performance between the two proposed networks

The Figure 10 shows first network's average Ethernet delay (sec) and average Ethernet Load (bits/sec) of IP PBX/ SIP server and VPN Server. We see the Ethernet delay of IP PBX and VPN server is almost 5 ms and average Ethernet load is 600 bits/sec to 800 bits/sec. While the Figure 11 shows second network's average Ethernet delay (sec) and average Ethernet Load (bits/sec) of IP PBX/ SIP server and VPN Server. We see the Ethernet delay of IP PBX and VPN server is almost 5-6 ms and average Ethernet load is 1500 bits/sec to 2000 bits/sec because of big network exist 90 nodes.

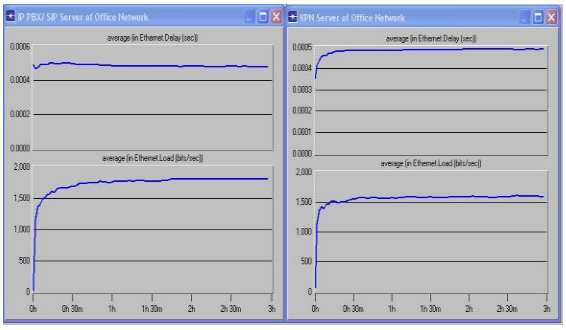


Figure 11: IP PBX delay and load comparison between two networks

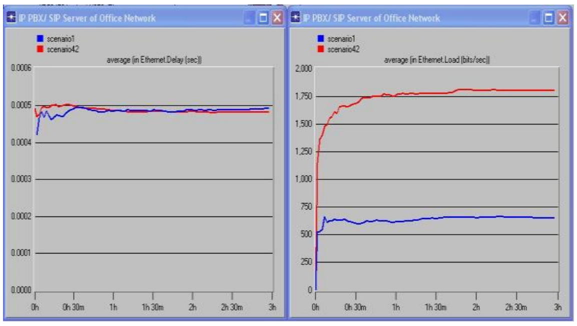


Figure 12: Second Network IP PBX and VPN server's network delay and load

The Figure 12 compares between first and second network on the basis of average Ethernet delay and average Ethernet load of IP PBX / SIP Server. The blue mark is for first network and red mark is for second network.

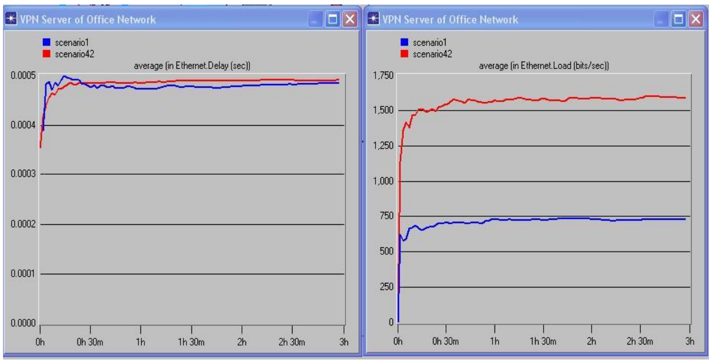


Figure 13: VPN Server delay and load comparison between two networks

The Figure 13 also compares between first and second network on the basis of average Ethernet delay and average Ethernet load of VPN Server. The blue mark is for first network and red mark is for second network. The results show that although the delay of both the networks are at a considerable level, the traffic received is far greater in network B compared to network A. Same is the case for load which is significantly greater for network B as well. So finally we reach our goal that overall network delay is less than 6 milliseconds which is considerable level for VoIP communication [16-17]. For security purpose firewall, router, LAN Switch and linux server are implemented in our research. So VoIP on IP PBX using secure VPN communication is fully implemented and ensure maximum security. There is another option we implement that is delay analysis because it's an important issue for VoIP communication. Both networks which are implemented to analysis for delay we find the delay is less than 6 milliseconds. This type of delay is acceptable for any VoIP communication.

OPNET is an engine that can be used to identify the network flaws. It included faults such as violation of policies and inefficiency in the network. The engine can be used to identify hidden errors in the network. The OPNET report has verified the first case network. It reflected that the data were obtained from the devices.

OPNET is a discrete event simulator, hence the results of the simulation is not always the same. So the scenarios when we use more nodes / workstations then get good simulated results. The results of the simulations were almost identical with minor differences.

IV. Conclusions

The main objective of this work is to implement the security of VoIP communication using IP PBX system based on VPN network. The behavioral analysis is also established with the OPNET simulation results. The analysis is made by focusing the results on VPN statistics, flow delay and point to point load. The paper highlights the theoretical and empirical research results of IP PBX based on the VoIP protocol suite, in the VPN backbone. The approach helped us answer the following questions:

- The challenges in security using VPN network.
- VPN with IP QoS influences delay in the VoIP network.
- SIP/H.323/IAX user can be registered more securely.
- Firewall, router and linux server all protects from clients/users from any type of vulnerabilities based on backbone.

Finally, we have carried out simulation on the proposed idea. The results of the simulation give us concrete data to state that VoIP based IP PBX on VPN

References

[1] J. C. Snader, VPNs Illustrated: Tunnels, VPNs, and IPsec. USA: Addison Wesley Professional, 2005. http://www.irma-international.org/viewtitle/33054/

[2] G. Mehdi, "Future of VoIP over Wireless in Economic Downturn," Blekinge Institute of Technology, 2009.

[3] Phone Systems to Power Your Business -VoIP, PBX,IP PBX. Available: http://www.digium.com/en/

[4] http://technet.microsoft.com/en-us/library/cc771298(v=ws.10).aspx

[5] http://www.vps-tutorial.info/2011/01/10/pptp-vpn-setup-xen-centos5/

[6] "A novel approach for security issues in VoIP networks in virtualization with IVR" International Journal of Distributed and Parallel Systems (IJDPS) Vol. 3, No.3, May 2012.http://arxiv.org/ftp/arxiv/papers/1206/1206.1748.pdf

[7] "Issues and challenges in securing VoIP"http://nsl.cse.unt.edu/~dantu/cae/Dantu/Issues_and_Challenges_in _Securing _VoIP.pdf

[8] C. Lewis, S. Pickavance, M. Morrow, J. Monaghan, and C. Huegen, Selecting MPLS VPN Services. Cisco Press, 2006.

[9] http://www.centos.org/docs/4/html/rhel-sg-en-4/s1-firewall-ipt-fwd.html

[10] http://phillipcooper.co.uk/2011/10/dhcp-relaying-over-ipsec-with-a-back-end-centos-5-5-server/

[11] Sela Frnklen, VPN 2nd chapter. http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

[12] Patrick C.K. Hung and Miguel Vargas Martin, (2006) "Security Issues in VoIP Applications", IEEE CCECE/CCGEI, pp 2361-2364.

[13] Miguel Vargas Martin and Patrick C.K. Hung, (2005) "Towards A Security Policy for VoIP Applications", Electrical and Computer Engineering, pp 65-68

[14] " VoIP Securities for Dummies",Available:www.penninetelecom.com/files/VoIP_Security_for_Dummies.pdf

[15] OPNET Technologies, Inc., "OPNET Modeler: Network Simulation," 2011 http://www.opnet.com/solutions /network_ rd/modeler.html.

[16] "ITU-T Recommendation G.1010: End-user multimedia QoS categories," ITU,2001.

[17] "ITU-T recommendation G.109: Definition of categories of speech transmission quality", ITU, 30th September 1999.

[18] Network computing. Security big security flaws found in Asterix PBX, IAX VoIP Client. http://www.networkcomputing. com/channels/networkinfrastructure/showArticle.jhtml?articleID¼189400851; June 13, 2006.

[19] David Butcher, Xiangyang Li and Jinhua Guo, (2007) "Security Challenge and Defense in VoIP Infrastructures", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, Vol. 37, No. 6, pp 1152-1162.

[20] K. Jannu and R. Deekonda, "OPNET simulation of voice over MPLS with considering Traffic Engineering," Blekinge Institue of Technology, 2010.

[21] Naveed Iqbal and Fahad Mumtaz Cheema, "QoS of VoIP in Wireless Networks," Blekinge Institute of Technology, 2009.