Study the Best Approach Implementation and Codec Selection for VoIP Over Virtual Private Network

Mohd Nazri Ismail
Department of Malaysian Institute of Information Technology, University of Kuala Lumpur, Malaysia

Abstract: *In this research, we propose an architectural solution to implement VoIP over Virtual Private Network (VPN) technology in campus environment between branches. The objective of this evaluation is to measure the quality of the VoIP performance over VPN technology. This study is to analyze the VPN over open source application (e.g., Windows and Linux operating system), and hardware device (e.g., Juniper) performance areas evolved with the quality of service delivered by VoIP conversation between branches. This study focuses on quality of voice prediction such as 1). the performance of VoIP activity and 2). delay and packet loss. The most apparent of implementing VoIP over VPN in campus environment is to define the best solution between open source application (e.g., Windows and Linux operating system) and hardware device that can be used in operational environment. Based on the finding result, VoIP over VPN measurement through hardware device is able to contribute better performance compare to open source application such as CPU utilization, MOS, delay and jitter.*

Keywords: *MOS, operating system, VoIP, VPN, system performance.*

Received December 4, 2010; accepted May 24, 2011

1. Introduction

As with most new technologies, Voice over Internet Protocol (VoIP) brings new challenges along with the benefits. The main challenge is VoIP's extreme sensitivity to delay and packet loss compared with other network applications such as web and e-mail services. A basic understanding of VoIP traffic and of the quality metrics provided by VoIP monitoring tools will help to keep VoIP network running smoothly. IPv4 over IPv6 can improve the Internet or Intranet, with benefits such as:

- Expanded addressing capabilities.
- Server less auto configuration (plug-and-play) and reconfiguration.
- More efficient and robust mobility mechanisms.
- End-to-end security, with built-in, strong IP-layer encryption and authentication.
- Streamlined header format and flow identification.
- Enhanced support for multicast and QoS.
- Extensibility: improved support for options/ extensions.

In this paper, the study will compare the performance of VoIP over VPN implementation using hardware and software platform. It is to define which VoIP Codecs can perform and achieve a good performance result on hardware platform or software platform. The experiment is conducted and tested using VoIP over VPN to analyze performance issues as follows:

a. Using differences codecs on VoIP softphone.
b. Implementing two different platform of VPN based on hardware (Juniper Netscreen 25) and software.

2. Related Works

Virtual Private Networks (VPNs) provide a secure and reliable communication between customer sites over a shared network [1]. Nowadays, VPNs is considered the strongest security solutions for communications over IP networks. Most VPN solutions are implemented to tunnel data traffic while the trend toward a converged data and voice network, however, places new demands on VPNs to support real time traffic [2, 3]. The main issues on VoIP are: 1). Security and 2). QoS Packet transmission of voice can introduce new impairments, including packet loss, extra sources of delay, and the use of compressed speech coding, all of which may affect voice quality delivered to the user [8]. QoS of the voice is affected by delay, jitter, and packet loss [6, 7]. There are several vulnerabilities occur during voice conversation such as [4]:

1. Circuit-switched technology vulnerabilities.
2. VoIP technology vulnerabilities for example IP Phone and PC-based phone.
3. VoIP gateway vulnerability.

Networks need to be more intelligent, secure and have a high level of performance. The more challenges facing the deployment of VoIP in large enterprise networks are the interoperability, security, and bandwidth management issues. These three problems

are major stumbling blocks that keep VoIP technology from being implemented immediately into large corporations until these problems are fixed [8]. The VoIP performance metrics include delay, jitter, packet loss and Mean Opinion Score (MOS) [5, 9].

Therefore, this study is to provide and solve a security mechanism and performance issue on VoIP over VPN technology implementation.

3. Methodology

Figure 1 shows the overall framework of VoIP over VPN technology in campus environment. There are five phases development process such as: 1). Planning, 2). Design, 3). Implementation, 4). Testing, 5). Compare, and 6). Compile. Figures 2 and 3 show the implementation of VoIP over VPN using open source application and hardware device. In the experiment, the analysis performance will focus on codec selection measurement during conversation between two parties. Network management system is used to analyze VoIP over VPN technology in campus environment. Figure 4 shows the process and criteria selection of VoIP performance evaluation.

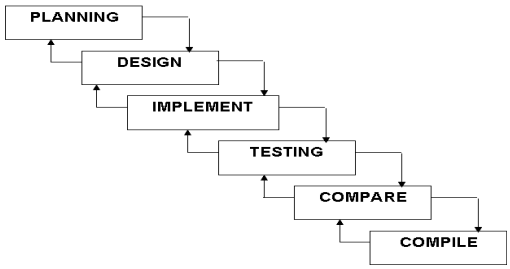


Figure 1. Framework of VoIP over VPN technology in campus environment.

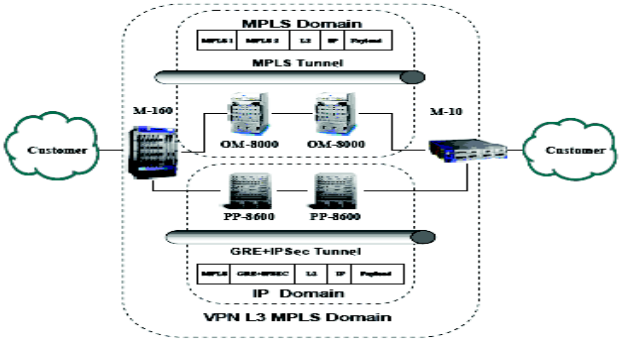


Figure 2. Implementation of VoIP over VPN using hardware platform.

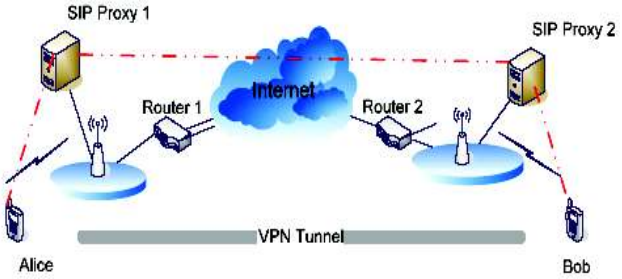


Figure 3. Implementation of VoIP over VPN using software platform.

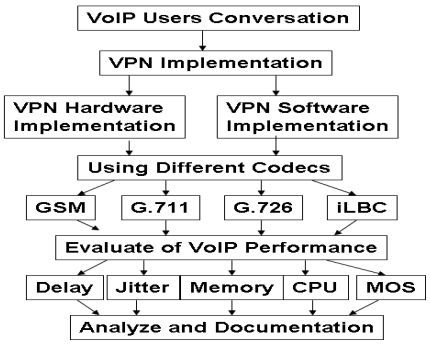


Figure 4. Process and criteria selection of VoIP performance evaluation.

4. Analysis and Results

The coursework in this module is a group-work project. Students are required to be in a group of four or five. For ease of managing groups by tutors, group members should be officially timetabled for the same practical session and they will have to be in the same group that they sign up with initially for the life-cycle of the project (guidelines implemented in 2000/2001). Though these are the guidelines, but experience tells us that managing groups of varying capability, attitude, promptness, is not an easy task. Group leadership is rotational as per major milestone or as students prefer it to be. The individual mark of each member in the group is based on group's results, his/her contribution to the group, and self- critical appraisal of the his/her experience in undertaking the project where students critically analyse the major problems faced in the project, lessons learned, and future enhancements to the run of the project as well as enhancements to the problem being tackled.

In order to be in-line with the key objectives of this module, students used a software development process in carrying out the different activities of the assignment. In addition, they were required to use the Unified Modelling Language (UML) [2] to document the requirements and design models. Moreover, state-of-the-art tools were used to support the process they used, UML, and developing the system's prototype. As per group-work deliverables, students reported on the following.

5. Analysis of Exam Results

Several experiments will conduct and to measure the performance of VoIP over VPN such as: 1). CPU Utilization, 2). Memory Performance, 3). Delay, 4). Mean Opinion Score, and 5). Jitter. All the result is capture using VQ Manager. This VQ manager is suitable application to work in voice packet environment.

5.1. System Performance

In this section, it will discuss on system performance (memory). The observation show that Codec G.711

(23.2%) and G.726 (23.2 %) generate highest percentage memory usage for hardware VPN implementation refer to Figure 5 and Table 1. iLBC Codes has generated the lowest memory usage (17.3%) compare for others codecs. Figure 6 shows the highest memory usage (20.1%) for VPN software implementation using G.711 and GSM codecs. This study has concluded and summarized all the VoIP codecs performance through VPN implementation in Figure 7.

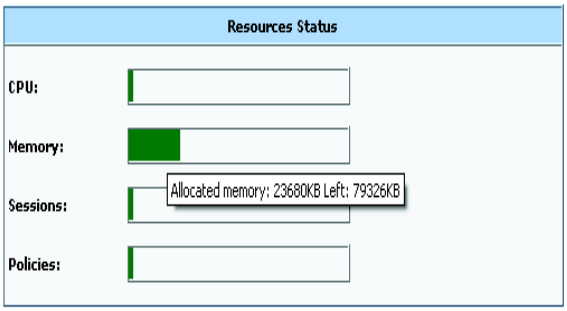


Figure 5. Memory usage for hardware implementation (netscreen 25).

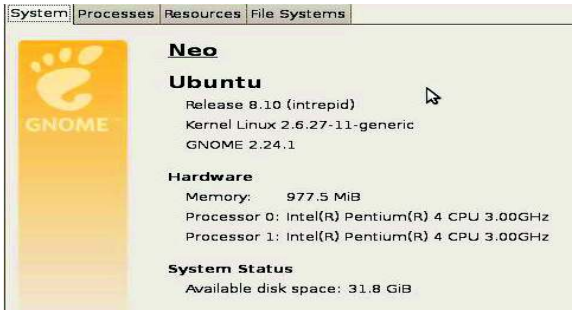
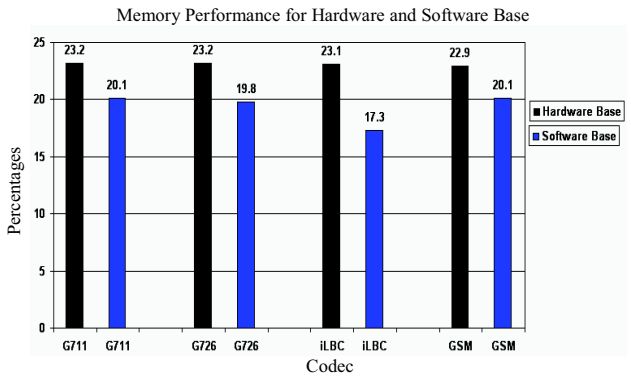


Figure 6. Memory usage for VPN software implementation.

Table 1. Comparison between hardware and software VPN implementation: memory usage.

Device	Juniper Netscreen 25	Ubuntu Server
Memory	103.006 MB	977.5 MB

Figure 7. Overall memory performance: VoIP codecs selection.



5.2. CPU Utilization

The next experiment is to measure CPU utilization performance between hardware and software VPN implementation. Figures 8 and 9 show the CPU utilization results during VoIP conversation. It can conclude that CPU utilization performance using hardware based is not affected with VoIP conversation.

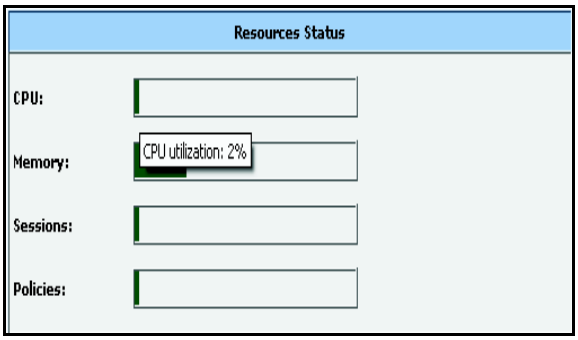


Figure 8. CPU utilization: VoIP through VPN hardware implementation.

Figure 9. CPU utilization: VoIP through VPN software implementation.

Table 3 shows VoIP Codec G.711 achieved the highest result 80% using VPN software implementation and follows by G.726 is 77.5%. VoIP over VPN hardware implementation has generated a lowest CPU utilization (2%) compare to software base refer to Table 2.

Table 2. CPU utilization-VoIP over VPN hardware implementation.

	Hardware Base (%)			
	G.711	G.726	iLBC	GSM
CPU Utilization	2	2	2	2

Table 3. CPU Utilization-VoIP over VPN software Implementation.

	Software Base (%)			
	G.711	G.726	iLBC	GSM
CPU Utilization	80	77.50	72.50	44.25

5.3. Delay

Then, this study will monitor and analyze VoIP delay performance over VPN implementation. The output results from VPN hardware will compare with VPN software implementation. VoIP over VPN hardware has generated higher delay for G.726 Codec refer to Figures 10, 11 and 12. Besides, VoIP over VPN

software implementation has also generated higher delay for GSM Codec refer to Figures 13, 14 and 15.

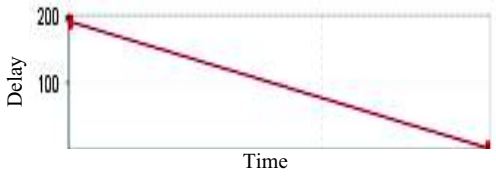


Figure 10. Delay-VoIP over VPN hardware implementation for G.726 codec.

Figure 11. Delay-VoIP over VPN hardware implementation for GSM codec.

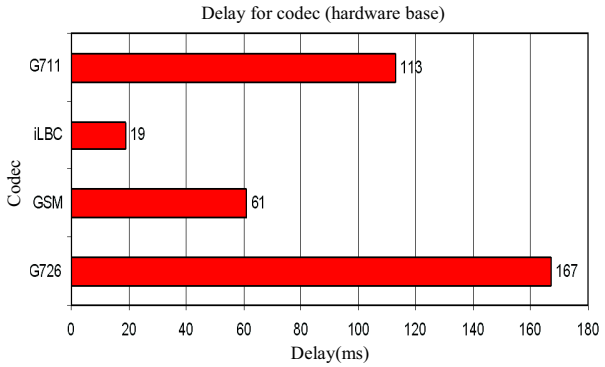


Figure 12. Overall delay-VoIP over VPN hardware implementation.

For VPN hardware implementation, overall results show that VoIP codec G.726 achieve delay 167ms, codec G.711 achieve delay 113ms, then codec GSM achieve 61 ms and codec iLBC achieve 19ms refer to Figure 12. For VPN software implementation, overall results show that codec G.726 achieve delay 268ms, codec G.711 achieve delay 246ms and codec GSM achieve 378ms refer to Figure 15.

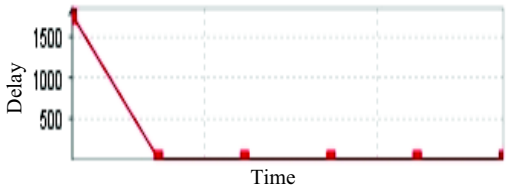


Figure 13. Delay-VoIP over VPN software implementation for GSM codec.

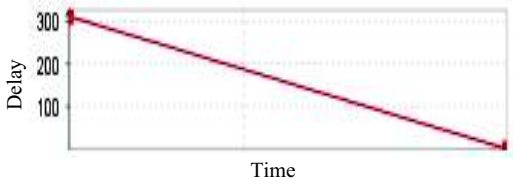


Figure 14. Delay-VoIP over VPN software implementation for G.726 codec.

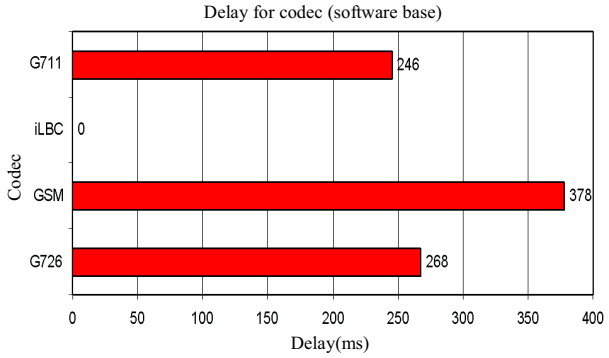


Figure 15. Overall delay-VoIP over VPN software implementation.

5.4. Jitter

The next experiment, the study will conduct and test on jitter performance for VoIP over VPN implementation. The result shows that VoIP over VPN hardware implementation will generate low jiiter compare to VoIP over VPN software implementation refer to Figures 16 and 17.

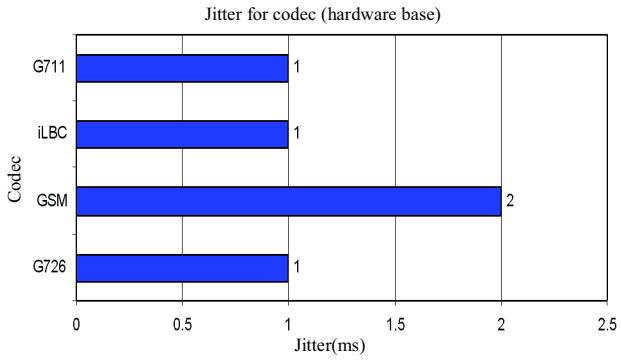


Figure 16. Overall Jitter-VoIP over VPN Hardware Implementation.

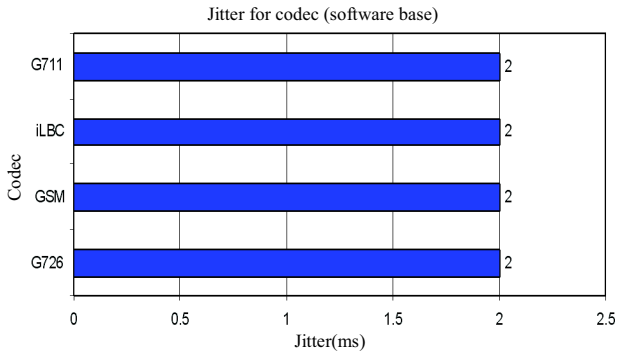


Figure 17. Overall Jitter-VoIP over VPN software implementation.

For VPN hardware implementation, overall results show that VoIP codecs such as G.711, G.726, GSM and ilBC generate jitter range 1ms-2ms. For VPN software implementation, overall results show that VoIP codecs (G.711, G.726, GSM and iLBC) generate jitter 1ms.

5.5. Mean Opinion Score (MOS)

Figure 18 shows the comparison of VoIP performance over VPN using hardware and software base. In this

experiment, the study will using MOS approach to evaluate our VoIP performance using several types of codecs. In the experiment, 20 users are selected to test VoIP quality over VPN. The rating is based on:

1. Unsatisfactory-Very annoying distortion which is objectionable.
2. Poor-Annoying distortion but not objectionable.
3. Fair-Perceptible distortion that is slightly annoying.
4. Good-Slight perceptible level of distortion but not annoying.
5. Excellent-Imperceptible level of distortion.

For hardware, codec G.711 is the higher codec rating 4.25. codec G.726 is the best codec for software base with rating 4.15. The lowest codec for hardware and software based on MOS measurement is GSM.

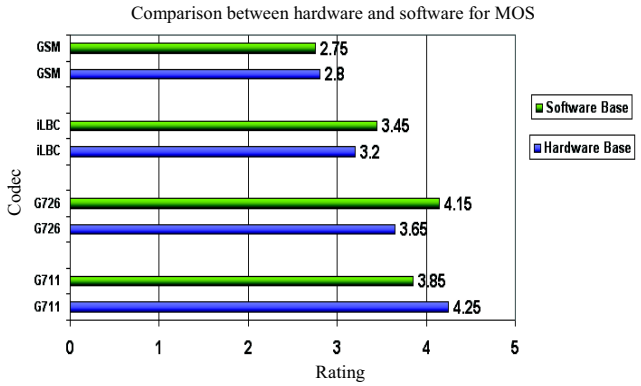


Figure 18. Comparison between hardware and software for MOS.

This study has concluded that based on the findings, VoIP over VPN implementation using hardware and software base is able to secure conversation between two parties. Based on the overall analysis this study can be concluded that VoIP over VPN software can degrade VoIP performance compare to VoIP over VPN hardware refer to Tables 4 and 5.

Table 4. Overall VoIP performance-VPN using hardware implementation.

	Software Base			
Codec	**G711**	**G726**	**iIBC**	**GSM**
CPU Utilization	High	High	High	Medium
Memory Performance	Medium	Medium	Low	Low
Delay	High	High	Low	High
MOS	High	Medium	Medium	Medium
Jitter	High	High	High	High

Table 5. Overall VoIP performance-VPN using software implementation.

	Hardware Base			
Codec	**G711**	**G726**	**iIBC**	**GSM**
CPU Utilization	Low	Low	Low	Low
Memory Performance	High	High	High	High
Delay	Medium	Medium	Low	Medium
MOS	High	Medium	High	Medium
Jitter	Low	Low	Low	High

6. Conclusions and Future Work

This paper discussed which VoIP over VPN implementation between open source application and hardware device in campus environment. This research was to investigate and define the performance of VoIP over VPN technology. In this article, this study has shown the performance of: 1). CPU utilization, 2). Memory usage, 3). Delay, 4). Jitter, and 5). MOS. This study conclude that base on the findings, VoIP over VPN using software base can contribute higher delay, jitter and CPU utilization compare to VPN hardware device. Memory usage and MOS indicator experiments show that a moderate result for VoIP over VPN using software base. It is recommended to implement VoIP over VPN using hardware base in order that to achieve a good quality service conversation. In future work, it should consider implementing techniques to improve quality of VoIP over VPN using mesh wireless network. Therefore, efficient and effective techniques are important to implement in order to achieve robust VoIP service and security issue.

References

[1] Arturo P., Victor Z., Angel M., and Carlos G., "Quality of Service Analysis of IPSec VPNs for Voice and Video Traffic," *in Proceedings of Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services*, pp. 43, 2006.

[2] Hunt G. and Arden P., "QoS requirements for a voice-over-IP PSTN Source," *BT Technology Journal*, vol. 23, no. 2, pp. 37-47, 2005.

[3] Kumudu S., Munasinghe K., and Seyed A., "Wireless VPNs: An Evaluation of QoS Metrics and Measures," *in Proceedings of International Conference on Mobile Business*, pp. 616-622, 2005.

[4] Monia G., Sudhakar G., and Gholamali C., "Resource Optimization Algorithms for Virtual Private Networks using the Hose Model Source," *The International Journal of Computer and Telecommunications Networking*, vol. 52, no. 16, pp. 3130-3147, 2008.

[5] Mohd I., "Measurement of V2oIP over Wide Area Network between Countries Using Soft Phone and USB Phone," *The International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 343-348, 2010.

[6] Sang-Jo Y., Seung-Sun Y., Chang-Yong L., and Geuk L., "Development of Internet Phone (VoIP) for Voice Security on VPN Environment Full Text," *in Proceedings of the International Conference on Convergence and Hybrid Information Technology*, Daejeon, pp. 293-300, 2008.

[7] Thanasis G. and George D., "Design of a Charging and Accounting Architecture for QoS-Differentiated VPN Services to Mobile Users," *Computer Communications, Quality of Future Internet Service*, vol. 27, no. 4, pp. 364-373, 2002.

[8] Wafaa B., Samir T., and Carole B., "VPN Analysis and New Perspective for Securing Voice over VPN Networks," *in Proceedings of the 4th International Conference on Networking and Services*, USA, pp. 73-78, 2008.

[9] Xianhui C. and Lee J., "VoIP Performance Over Different Interior Gateway Protocols," *International Journal of Communication Networks and Information Security*, vol. 1, no. 1, pp. 34-41, 2009.

Mohd Nazri Ismail is a lecturer at University of Kuala Lumpur. He is completed his PhD in Computer Industry Department (FTSM Faculty) and specializing in computer networking, at UKM in November 2010. He has many years experience R&D computer networking. Before joining University of Kuala Lumpur, he was system analyst at Bank Simpanan Nasional and network engineer at MIMOS Berhad. In MIMOS, he has been exposed in R&D for Wireless, Infrared, WAP, Remote Access Server, VoIP and IP telephony technology. He holds a MS degree by research in engineering science at Multimedia University. He has researched under "prepaid and postpaid VoIP architecture in rural areas" during his MS Degree at MMU. He received a BS degree in computer science from UKM, Malaysia. He has experience in network simulation tool such as matlab, NS-2, OPNET and OMNET++.