International Conference - Innovation-2021-Innovation-2021
International Journal of Scientific Research in Computer Science, Engineering and Information Technology ISSN : 2456-3307 (www.ijsrcseit.com)
Volume 8, Issue 3, May-June-2021

Performance Analysis of a Large-Scale Enterprise Network in Real Time Environment

Md. Taslim Arefin*, Md. Tauhidunnabi Likhon, Chowdhury Badrul Huda, Diganta Roy
Department of ETE, Daffodil International University, Dhaka, Bangladesh
Corresponding Author Email : arefin@diu.edu.bd*

ABSTRACT

An enterprise network is a communications backbone that helps to connect computers and other related devices across a large workgroup networks that provides insight and data accessibility. In this paper an enterprise network model has been designed based on real time environment. A comparative analysis of MPLS network over conventional Internet Protocol (IP) network has been performed. Different routing protocols such as OSPF, EIGRP, RIPv1, RIPv2 and MPLS have been considered in the performance analysis. GNS3 has been used to simulate the both networks and the comparative analysis has been made based several parameters such as Packet jitter, Packet delay, Packet drop etc. The simulation results have been analyzed which indicates that MPLS network has performed better than conventional IP network in real-time applications such as Voice and video. MPLS L3 VPN has been used in the proposed model.

Keywords : Enterprise Network, MPLS, VPN, GNS3

I. INTRODUCTION

An enterprise network is an enterprise's communications backbone that helps connect computers and related devices across departments and workgroup networks, facilitating insight and data accessibility[1][3]. An enterprise network reduces communication protocols, facilitating system and device interoperability, as well as improved internal and external enterprise data management. So we choose an area as like as an enterprise network, then we design the enterprise network simply and required. After identify the problems, we also try to solve it. Then we use different protocols. Such as RIPv1, RIPv2, EIGRP, OSPF and MPLS. After analyzing all protocols, we select OSPF is the best one for faster communication in the enterprise network. In this protocol, security is not reliable but we need to make the security reliable. So, we can use Firewall, ACL, L3 VPN. To overcome the enterprise network model limitations, we suggested our proposed model.

In our proposed network model applying OSPF protocol with MPLS L3 VPN, ACL, Firewall configuration the hole protocol can provide us higher security and less traffic when the data is passing through the proposed network model better than the enterprise network model [2][13]. The purpose of writing this paper is to show the best protocol that is used in a large-scale enterprise network which is

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

reliable & faster. We breakdown the limitation of an enterprise network model through our proposed network model.

The specific objectives of this research are given bellow:

- ✓ To gain proper knowledge about enterprise network.
- ✓ To apply & discuss about different protocol.
- ✓ Suitable protocol will provide for depend upon situation.
- ✓ To provide high security, less traffic & high-speed data flow for large area.
- ✓ To provide proper network service & distributed application for required host.

II. NETWORK MODEL DESIGN

An enterprise network is also known as a corporate network. The enterprise network model is shown in figure 1.

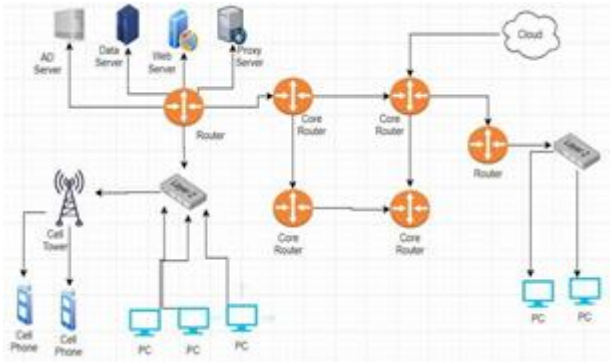

Figure 1: Enterprise Network Model

Figure-1 shows that, Public cloud directly connected to the gateway router. The Data server or storage server provides the data for LAN connection and cell phone via the cell tower for their required. In this paper we used different routing protocols for our work purpose. Those are

- ✓ Static Routing Protocol
- ✓ Dynamic Routing Protocol
- ✓ MPLS Protocol

An enterprise network required some features. Those are given below [10]

- ✓ Core Layer
- ✓ Distribution Layer
- ✓ Access Layer
- ✓ LAN
- ✓ WAN
- ✓ LAN & WAN Distribution

Core Layer: The core layer is a high-speed switching backbone and should be designed to switch packets as fast as possible. This layer of the network should not perform any packet manipulation, such as access lists and filtering, that would slow down the switching of packets [7].

Distribution Layer: The distribution layer is located between the access and core layers and helps differentiate the core from the rest of the network. The purpose of this layer is to provide boundary definition using access lists and other filters to limit what gets into the core. Therefore, this layer defines policy for the network [5].

Access Layer: The access layer, which is the lowest level of the Cisco three tier network model, ensures that packets are delivered to end user devices. This layer is sometimes referred to as the desktop layer, because it focuses on connecting client nodes to the network [6].

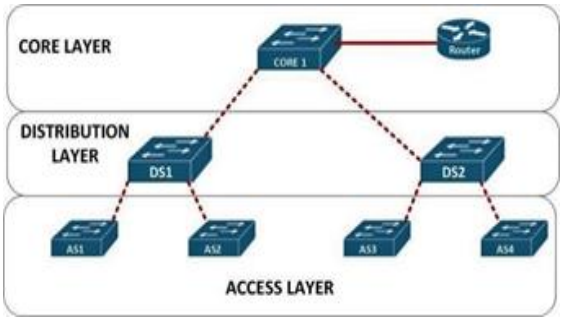

Figure-2: Layer Design in an Enterprise Network

LAN: A local area network is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building [5].

WAN: A wide area network is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking. Wide area networks are often established with leased telecommunication circuits [4][7].

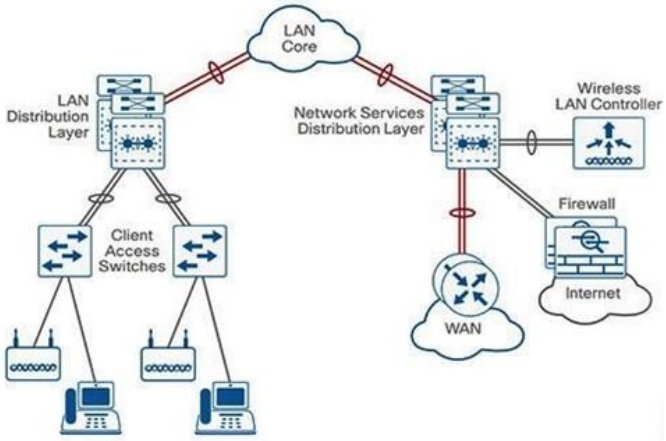

Figure-3: LAN & WAN Network Distribution Design

In this Figure-3 with the LAN core network goes to the LAN distribution Layer. By the requirement of the client the network has been distributed. Here, firewall is also used for protecting the LAN network [8][9].

To analyze the performance, we have designed two scenario using GNS3. Those are-

- ✓ Scenario 1: Enterprise Network Model
- ✓ Scenario 2: Proposed Network Model

a.Enterprise Network Model

An enterprise network infrastructure that provides access to network communication services and resources to end users and devices that are spread over a single geographic location. It may be a single building or a group of buildings spread over an extended geographic area [8].

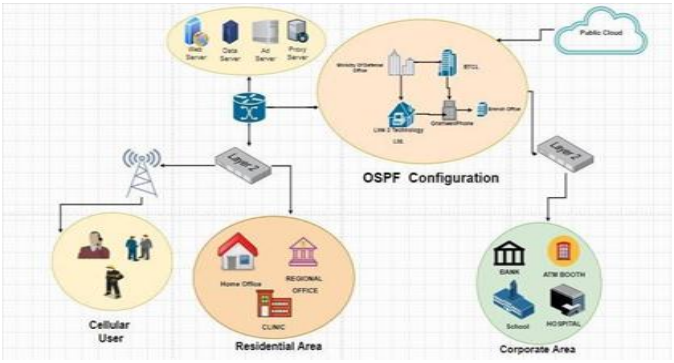

Figure-4: Enterprise Network Model

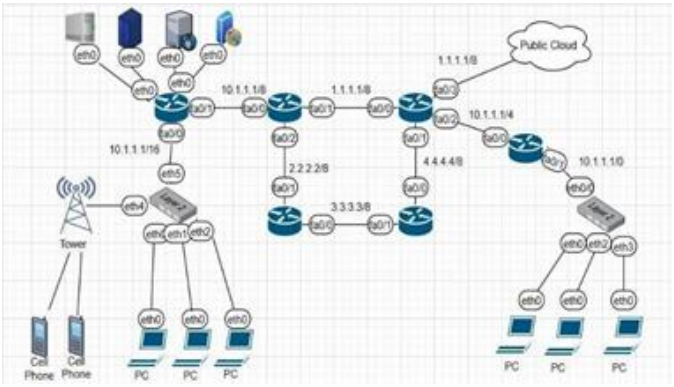

Figure-5: Enterprise Network Model in GNS3

Figure-4 and 5 show an enterprise network. To facilitate our work, we are splitting the whole enterprise network into several small area network. Every small area network is represented as a core router. Cellular & Residential area are connected with layer 2 switch. Layer 2 switch are also connected with servers. Such as Web server, Data server, Ad server, Proxy server. All the server are connected with Public Cloud. In the same way the Corporate area is also connected.

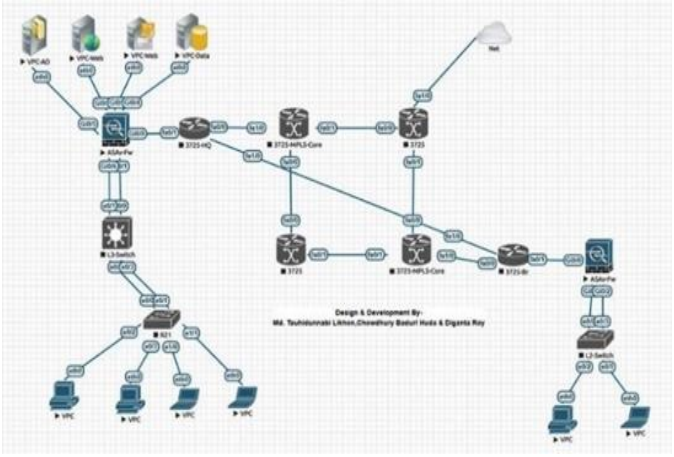

Figure-6: RIP Configuration

Figure-6 shows that Routing Information Protocol (RIP) has been configured. The core router neighborly connected each- other and they are able to pass the packet.

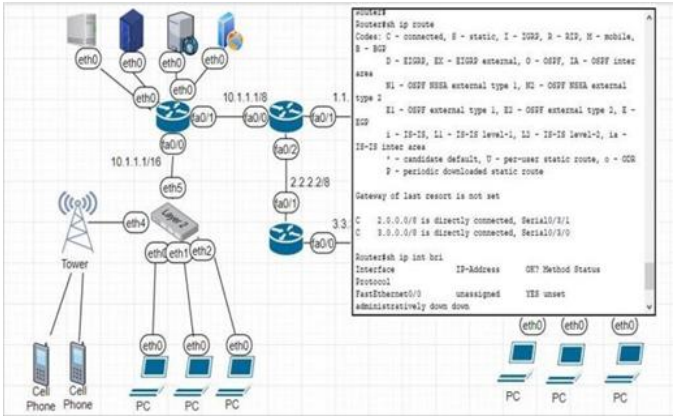

Figure-7: OSPF Configuration

Figure-7 shows that Open Shortest Path Fast (OSPF) has been configured. The core router neighborly connected each-other and they are able to pass the packet in shortest

b.Proposed Network Model

Figure- 8 and 9 show our proposed network model. To facilitate our work, we are splitting the whole proposed network into several small area network. Every small area network is represented as a core router.

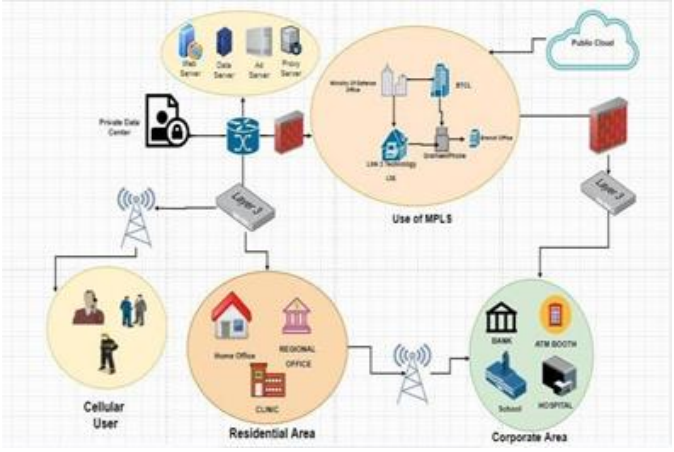

Figure-8: Proposed Network Model

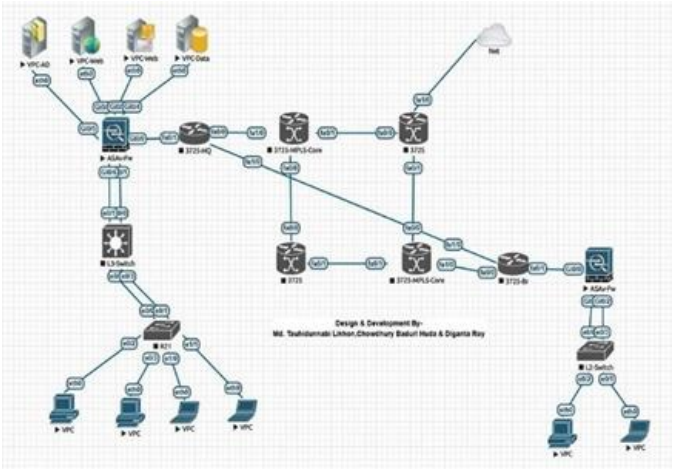

Figure-9: Proposed Network Model in GNS3

Cellular network is connected with cell tower. Cell tower is connected with layer 3 switch that is subordinate with another core router and connected with several servers. Such as Web server, Data server, Ad server, Proxy server. Residential also connected with layer 3 switch and with subordinate with the same core router and also the servers. These servers ae connected with Public Cloud. Corporate area is connected with layer 3 and another core router with firewall. Firewall protect unacceptable IP network or service. Private Data Center is use only for Ministry of defense office. Here the Residential & Corporate area are also connected with cell tower for data communication.

III. SIMULATION AND ANALYSIS

Simulation is the process of testing a designed model on a platform which imitates the real environment. It provides the opportunity to create, modify and study the behavior of proposed design so that one can predict its strengths and weakness before implementing the model in real environment. We used the popular simulator in this project is-GNS3. Simulation flowchart has been shown in figure 10.

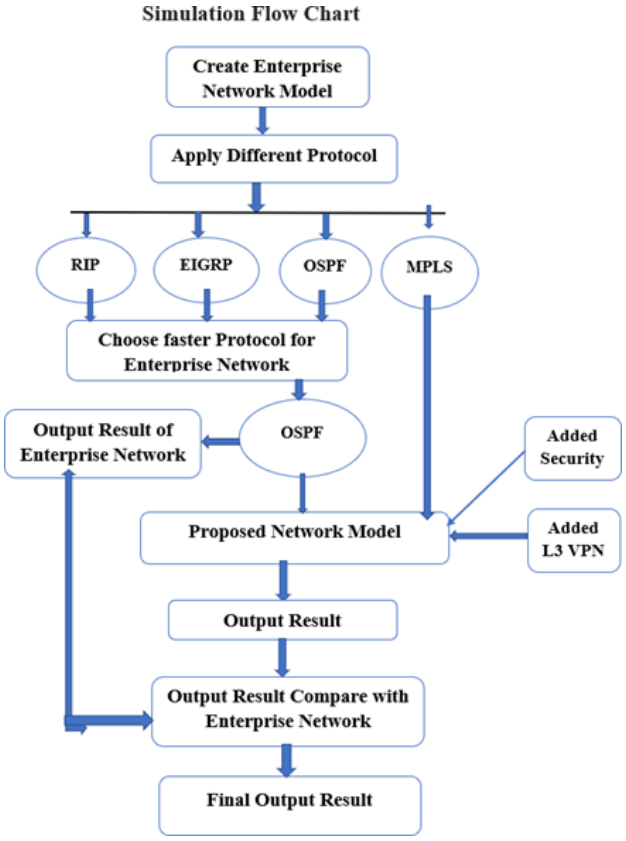

Figure-10: Simulation flowchart

Output Result of Proposed Network Model

Figure-11 is configured with MPLS L3 VPN and it shows MPLS packet forwarding table. That means the hole network is established. Also shows that with hop-to-hop connectivity packets are passing one network to another network.

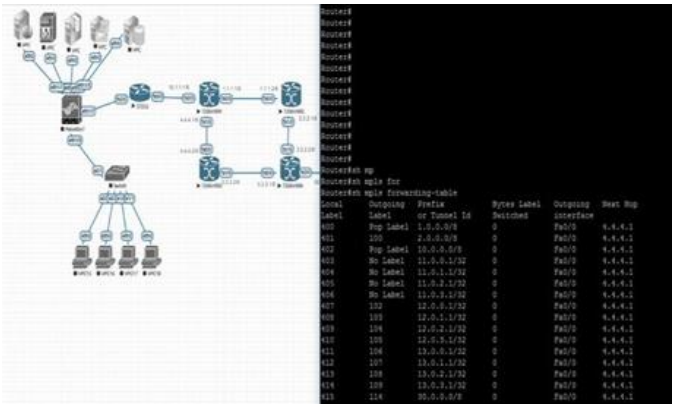

Figure-11: MPLS L3 VPN Configuration

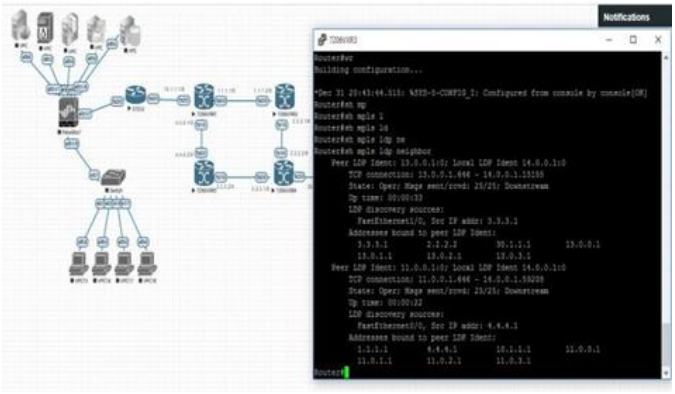

Figure-12: Checking MPLS Neighbor Connectivity

Figure-12 shows MPLS neighbor connectivity. With that the network is able to pass broadcast message to all neighbor network. If any of the neighbor network doesn't get any broadcast message then the total connectivity is unstable.

IV. PERFORMANCE ANALYSIS

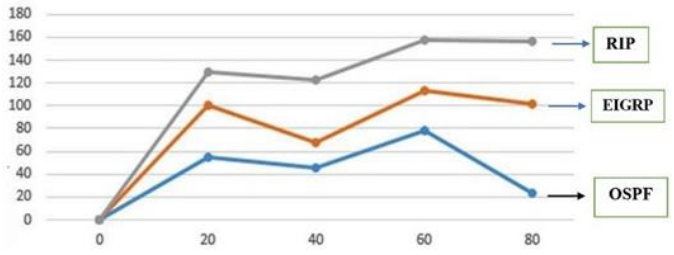

Figure- 13: Network Packet Delay

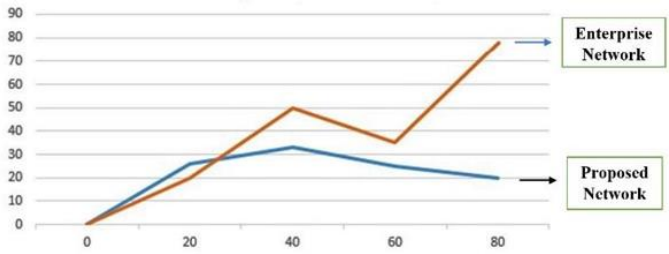

Figure-14: Packet delay Enterprise Network Vs Proposed Network

Figure-14 shows line graph where vertical axis is packet delay and horizontal axis is simulation time (ms) and showed Packet delay Enterprise Network VS packet delay Proposed Network. Here, the proposed model network's packet delay is less than the enterprise network's packet delay.

Packet Loss

Packet loss is where network traffic fails to reach its destination in a timely manner. Most commonly packets get dropped before the destination can be reached. Packet loss can be calculated by [12],

Packet dropped/loss, Pd = Ps – Pa

Where, Ps is the amount of packet sent and Pa is the amount of packet received. Here we have done all the calculation using GNS3 visual trace analyzer.

Packet Delay

Packet delay refers to the time taken for a packet to be transmitted across a network from source to destination. Packet delay or end-to-end delay can be calculated by,

End-to-end delay, D = Td –Ts [11]

Where, Td is packet receives time and Ts is the packet sends time at source node.

Figure- 13 shows line graph where vertical axis is packet output and horizontal axis is simulation time (ms) and also show the output of different protocol is in graphical way. Here the packet delay time of the OSPF is less than EIGRP & RIP. So OSPF is the best protocol for this enterprise network.

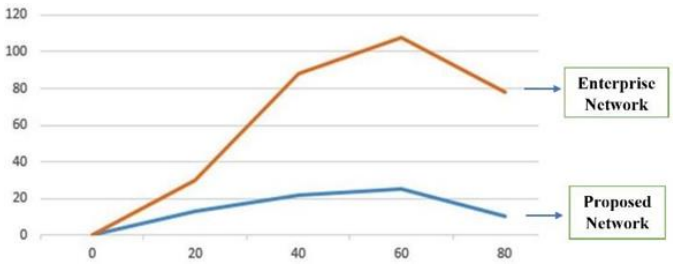

Figure-15: Packet Loss Enterprise Network Vs Proposed Network

Figure-15 shows line graph where vertical axis is packet loss and horizontal axis is simulation time (ms) and showed Packet loss Enterprise Network VS packet loss Proposed Network. Here, the proposed model network's packet loss is less than the enterprise network's model packet loss.

V. CONCLUSION

In this paper it has clearly indicated that MPLS technology has performed better than the other protocol. MPLS protocol Provide high speed data flow, provide high security, provide Less traffic, proper network service and distributed application for required host. After analyzing our work, we have come to the conclusion that configuring MPLS with L3 VPN for a large-scale network the data transfer rate is high. This protocol is able provide higher security, reliable network, less traffic when the data are transferring from one network to another.

VI. REFERENCES

[1]. Hao Yang, Ricciato, F., Songwu Lu, Lixia Zhang; Securing a wireless world Proceedings of the IEEE Volume 94; Feb. 2006

[2]. Lucent Technologies; Users Guide for the ORiNOCO Managers Suite; Nov. 2000 12 Wi-Fi Alliance; Wi-Fi Protected Access: Strong,

Standard Based, Interoperable Security for todays Wi-Fi Network.

[3]. Leinwand, Allan, Bruce Pinsky, and Mark Culpepper. Cisco router configuration. Cisco Press, 1998.

[4]. Gurkas, G.Z., Zaim, A.H., Aydin, M.A.;Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks; International Symposium on Computer Networks,2006; June 200

[5]. Mentze, Duane, and David McAnaney. "Automatic networking device configuration method for home networking environments."

[6]. KeunSoon Lee, HyoJin Kim, JooSeok Song; Lightweight packet authentication in IEEE 802.11; Wireless Telecommunications Symposium, 2005; April, 2005

[7]. Manivannan, N., Neelameham, P.;Alternative Pair-wise Key Exchange Protocols (IEEE802.11i) in Wireless LANs; International Conference on Wireless and Mobile Communications, 2006. ICWMC '06; July 2006

[8]. Ju-A Lee, Jae-Hyun Kim, Jun-Hee Park, Kyung-Duk Moon; A Secure Wireless LAN Access Technique for Home Network; IEEE 63rd Vehicular Technology Conference, 2006;

[9]. Kassab, M., Belghith, A., Bonnin, J., Sassi, S.; Fast pre- authentication based on proactive key distribution for 802.11 infrastructure networks; Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling; 2005

[10]. Yurcik, William J. "Network Topologies." Computer Sciences, edited by K. Lee Lerner and Brenda Wilmoth Lerner, 2nd ed., Macmillan Reference USA, 2013.

[11]. R. PRODANOVIC, D. SIMIC , Holistic Approach to WEP Protocol in Securing Wireless Network Infrastructure. Com SIS , Vol. 3, No. 2, pp. 97—113, (2006)

[12]. A.Haque, K.A.M Lutfullah, M.Zahedul Hassan, M.R.Amin, “Performance Analysis and the Study of the behaviour of MPLS Protocol”

[13]. J.Barakovic, A.Husic“QoS design issues and traffic engineering in next generation IP/MPLS network”, june 2007