**A**

**Project Report on**

**IMPROVED NETWORK SECURITY OF TELECOMMUINCATION NETWORK USING LOAD BALANCING**

**Submitted to the partial fulfillment of the requirement for the award of the degree of**

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE & ENGINEERING**

**Submitted by:**

Diksha Maurya(RA511003030426)

Vanita Chandra(RA1511003030418)

Deepankar Ratra(RA1511003030434)

**Supervised by:**

**Ms. Arnika Jain**

**Assistant Professor (CSE)**

****

**SRM Institute of Science and Technology**

**(Deemed to be University u/s of UGC Act, 1956)**

**NCR Campus, Modinagar**

**BONAFIDE CERTIFICATE**

This is to certify that project Report entitled **“Improved Network Security of Telecommunication Network using Load Balancing”,** which is submitted by **Diksha Maurya (RA1511003030426), Vanita Chandra (RA1511003030418), Deepankar Ratra (RA1511003030434)** in the partial fulfillment of the requirement for the award of degree B.Tech(CSE) of SRM Institute of Science and Technology, NCR Campus, Modinagar, Ghaziabad is a record of the candidate own work carried out by them under my own supervision.

|  |  |
| --- | --- |
| …………………….........  (Signature) | …..............................................  (Signature) |
| Dr. R. P. Mahapatra | Dr. Jitendra Singh |
| HOD (CSE) | Supervisor |
|  | Assistant Professor (Sr.G) |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

INTERNAL EXAMINER EXTERNAL EXAMINER

**ACKNOWLEDGEMENT**

We would also like to express our special thanks to **Ms. Arnika Jain,** Assistant Professor and Project Supervisor of SRM Institute of Science and Technology, NCR Campus, Modinagar, for their insight and knowledge on the subject, who imbued us with the feeling to work assiduously.

We feel compelled to articulate our thankfulness to Dr. Jitendra Singh, Mr. Naresh Sharma and Mr. B. K. Saraswat, Project Coordinators, SRM Institute of Science and Technology NCR Campus, Modinagar, for there enlightening dexterity which was truly a perennial source of inspiration.

We would like to express our hearty gratitude to Dr. D. K. Sharma, Dean, SRM Institute of Science and Technology, NCR Campus, Modinagar, under whose auspices we were able to work on our project work.

Also, we extend our sincere regards and thanks to Dr. R. P. Mahapatra, Head of the Department, Computer Science and Engineering, & Dean Admission, SRM Institute of Science and Technology, NCR Campus, Modinagar, for his suggestions.

We are also indebted to all the teaching and non-teaching staff members of our college for helping us directly or indirectly by all means throughout the course of our study and project work.

Finally, we take this opportunity to thank our parents, family members and friends for their moral support and help and extended thanks to our well wishers.

**Diksha Maurya(RA511003030426)**

**Vanita Chandra(RA1511003030418)**

**Deepankar Ratra(RA1511003030434)**

**DECLARATION**

We, **Diksha Maurya(RA1511003030426), Vanita Chandra(RA1511003030418), Deepankar Ratra(RA1511003030434)** hereby declare that the work which is being presented in the project report “**Improved Network Security of Telecommunication Network using Load Balancing**” is the record of authentic work carried out by us during the period from January ’12 to May ’12 and submitted by us in partial fulfillment for the award of the degree “**Bachelor of Technology** in **Computer Science and Engineering**” to **SRM IST, NCR Campus, Ghaziabad (U.P.).** This work has not been submitted to any other University or Institute for the award of any Degree/Diploma.

**Diksha Maurya(RA511003030426)**

**Vanita Chandra(RA1511003030418)**

**Deepankar Ratra(RA1511003030434)**

**CONTENTS**

[ABSTRACT 6](#_Toc7100474)

[INTRODUCTION 7](#_Toc7100475)

[LITERATURE SURVEY 9](#_Toc7100476)

[PROJECT OBJECTIVE 12](#_Toc7100477)

[SOFTWARE SPECIFICATION 13](#_Toc7100478)

[WORKING OF VPN 14](#_Toc7100479)

[CATEGORIZATION OF VPN 16](#_Toc7100480)

[ **Site-to-Site VPN** 16](#_Toc7100481)

[ **IPSEC VPN** 16](#_Toc7100482)

[ **SSL VPN** 16](#_Toc7100483)

[IPSec VPN 18](#_Toc7100484)

[TYPES OF LOAD BALANCING TECHNIQUES 19](#_Toc7100485)

[ **Round Robin** 20](#_Toc7100486)

[ **Weighted Round Robin** 20](#_Toc7100487)

[ **Least Connection** 20](#_Toc7100488)

[ **Weighted Least Connection** 20](#_Toc7100489)

[ **Agent-Based Adaptive Load Balancing** 20](#_Toc7100490)

[ **Chained Failover (Fixed Weighted)** 21](#_Toc7100491)

[ **Weighted Response Time** 21](#_Toc7100492)

[ **Source IP Hash** 21](#_Toc7100493)

[ **Software Defined Networking (SDN) Adaptive** 22](#_Toc7100494)

[ROUND ROBIN LOAD BALANCING TECHNIQUE 23](#_Toc7100495)

[DATA FLOW DIAGRAM 24](#_Toc7100496)

[SCREENSHOTS 25](#_Toc7100497)

[FUTURE SCOPE 26](#_Toc7100498)

[CONCLUSION 27](#_Toc7100499)

# ABSTRACT

Internet Security and fast communication is the need of the hour in this era of growing technology to provide secure data transmission between two communicating bodies. Enabling security using VPNs play an important role in protecting company communications from unauthorized accessing or replication.

The most suitable procedure is implemented through Cisco Packet Tracer. By designing and implementing this project we illustrate a number of security principles and technologies, including **integrity, authentication, key management and key exchange.**

We are introducing **load balancing** which distribute workloads uniformly across servers to optimize network efficiency, reliability and capacity. It also provides an additional advantage of failover. If one server fails, a load balancer immediately redirects its workloads to a backup server, thus mitigating the impact on end users.

# INTRODUCTION

Communication is an important means in the modern world and with the introduction of internet, telecommunication, it has become very important to transfer data with good efficiency and cost productivity. Internet has innovated our everyday life. It has made our life simple and easy. Internet simply means sharing of data. It is used for various purposes like Telecommunication, Business, Education, Welfare of people, Medical Education, Automation, Technical Assistance, Digital Marketing, Innovation, Shopping, Research and Development, Digital Transactions, etc.

But sometimes, using Internet can have some disadvantages such as Application Vulnerabilities, Cyber Vulnerabilities DDoS attacks, Hacking, Intrusion such as phishing, online viruses, Trojans, worms and more.

However, it is really challenging to use this network of public communication without any chance of risk. There are predators who use internet to get good people in a very dangerous and harmful situation. Also, there are a lot of unscrupulous businesses that has flourished on the internet to take edge of people. Therefore, the use of IPSec VPN enables companies or organizations to maintain fast, secure and reliable communications and hence making it a necessity for all organizations. It can be deployed at Internet Service Provider or over public Internet.

It is imperative that all the data network that are encrypted does not have to compromise with the security of one device for another. Thus multiple servers also known as server farm or server cluster are maintained by organization to supply server functionality far beyond the capability of single device. Hence, these multiple servers are used to aid in **load balancing** of servers. Load Balancing came into picture in the early 1990’s when organizations wanted to improve serviceability of applications that are running on servers.

Load Balancing provides assistance as ‘Traffic Managers’ of servers. Load Balancing means the distribution of tasks onto multiple devices such as servers so as to improve scalability and provide redundancy to application. No two devices can be connected to the same server as it would likely cause a sudden decline in connection speed. It also makes sure no server is inactive.

Additionally, it provides extensibility of addition or subtraction of servers on request. Technically, it means router has multiple paths to a destination when forwarding a packet. Load Balancing characteristics include reliability and performance for web servers and other mission - critical servers. Though Load Balancing is a very vast topic but its future scope also incorporates more sophisticated load forecasting techniques.

# LITERATURE SURVEY

1. Hitesh Dhall, Dolly Dhall, Sonia Batra, Pooja Rani, “Implementation of IPSec Protocol”, 2012 Second International Conference on Advanced Computing & Communication Technologies, 15 March 2012
   * IPsec can be implemented and deployed in the end hosts or in the gateways/routers or in both.
   * As IPsec is tightly integrated into the network layer, it can avail the network services such as fragmentation.
   * Sending and receiving data packets with IPsec needs more time as compared to sending data packets without Ipsec.
2. Anuradha Sharma (IT Dept.), Seema Verma (Comp. Network) , “A Survey Report on Load Balancing Algorithm in Grid Computing Environment”, International Journal of Advanced Engineering Research and Studies, IV/II , 2015
   * Comparative analysis of Existing Load Balancing Algorithms in Grid Environment.
   * Some algorithms does not specify memory requirement of the job while submitting the jobs to the selected resources and some of the algorithm does not considered communication cost, which we cannot neglect.
3. Rahul Godha, Sneh Prateek, “Load Balancing in a network” , International Journal of Scientific and Research Publications, Volume 4, Issue 10, October 2014 Research
   * Introduces a new mechanism for load balancing using heaps which will help automatically and dynamically distribute traffic across multiple servers.
   * At every sub-network level maintain a maximum heap which stores the score on every server.
   * The load balancer will store and maintain a maximum heap and redirect the request to the server whose store is maximum.
   * Advantages: since it uses heap search time will be of order of O(n).

1. helps achieve higher level of fault tolerance.

2. is secure and robust

* + Disadvantages : To make the reordering of the heap faster , we need to know load on each of the servers beforehand.

1. A Novel Technique for Load Balancing in Cloud Computing Environment Renu Choudhary, Dr.Abhay Kothari

* To improve the performance in different types of cloud a number of Load balancing techniques are used. These Load balancing techniques are selected as per the load received. Depending on the load and the distance from the user, applications are directed to the data center to optimize the performance
* Round Robin performs the basic type of load balancing and functions simply by providing the list of IP address of cloudlet. It allocates first IP address to the first requester then second IP address to the second request or for a fixed interval of time known as time slice. If the request is unable to finish within the given slice time, it will have to wait for the next cycle to get it turn for execution. This will continue till submitted tasks are not completed.
* Active Monitoring Load Balancer - This load balancer find outs the active VM and also to event out the active task at any point of time.
* Throttled Load balancer - This load balancing technique ensures that only as per-defined number of internet cloudlets are allocated to a single VM at any point of time. If more groups are presents in the data center than then number of available VM than some of the requests have to be queued until the next VM is available.

# PROJECT OBJECTIVE

We are using internet for almost everything. It provides data and information that is used to gain knowledge for the personal, social and economic development.

Almost everyone in this modern world uses internet. Some uses for it social networking, some for research, some for gaming, some for expanding their business, etc. Now that internet has become a vital part of our lives, we must be worried about its security. With society practically running on internet, cyber security is a real threat to many business and homes. Various people uses internet as a medium of money transactions. If the security is compromised, then the results could be severe.

What VPN provides is an encrypted channel where people can send their data in a scrambled way so that security is not compromised. The information transmitted between the sender and receiver is through the encrypted channel that cannot be read by anyone else. It adds a layer of security and privacy. A VPN is a tool to protect your privacy and increase your security on the Internet.

VPN can be categorized as Site-to-Site VPN, IPSEC Remote Access VPN, Clientless SSL VPN. The main objective for this project is to establish a secure communication between sender and receiver using IPSEC Remote Access VPN so that data can be shared without compromising the security

We are using multiple backend servers, also known as **server farm** or **server pool** to enhance security and help in sharing the load on a single server .

The advantages with this objective will include to serve hundreds or thousands of servers in a **fast** and **reliable manner**.

Project Goals : Comparative study of various load balancing strategies are made and the most secured one is then implemented.

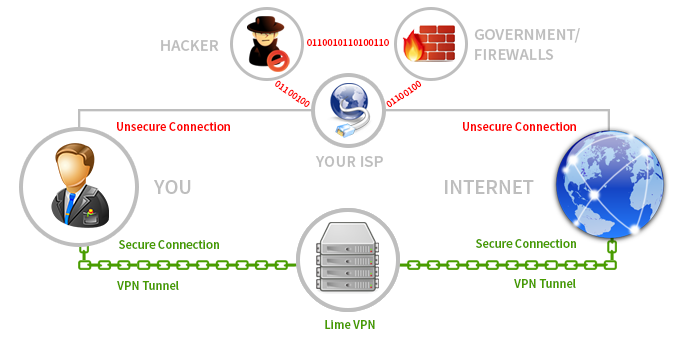
# SOFTWARE SPECIFICATION

Operating System : Windows 10

Software Used : Cisco Packet Tracer.

# WORKING OF VPN

VPN provides a secure connection between sender and receiver. When we are using the internet, we are transmitting our data through an unsecure connection. Any hacker can steal our data if the connection is not secure. Sometimes government blocked sites for a particular region which cannot be accessed by a user. In that case, VPN comes into play. It provides a VPN tunnel through which data is transmitted in an encrypted format so that no can steal our data. Also, data is transmitted to a VPN server which is geographically located in some another region by which we can access the blocked content.



There are a lot of VPN servers which can be used to provide a secure channel. But sometimes, there is a high load on a particular VPN server due to high network traffic.

Therefore, we are using multiple backend servers, also known as server farm or server pool to enhance security and help in balancing the load on a single server.

# CATEGORIZATION OF VPN

VPN can be categorized as follows:

1. Site-to-Site VPN
2. IPSEC VPN
3. SSL VPN

## **Site-to-Site VPN**

A Site-to-Site VPN allows organizations to create a secure connection over public network. It makes computer resources from one location available to staff at other locations. An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world.

## **IPSEC VPN**

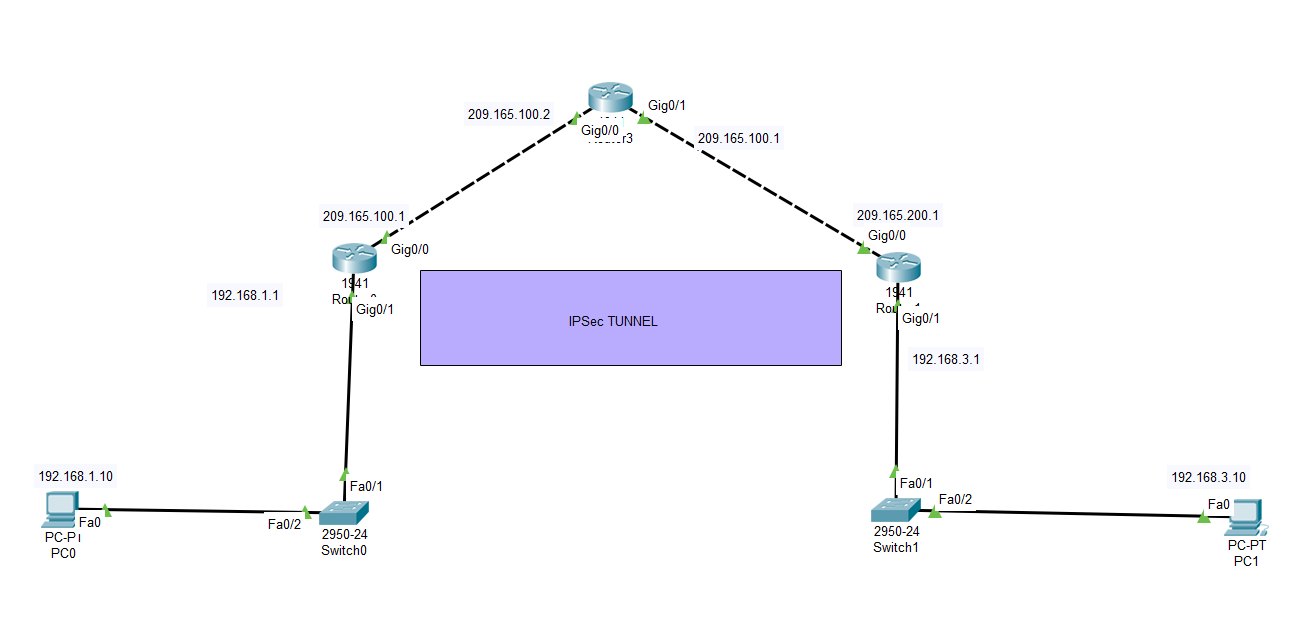
Internet Protocol Security, also known as IPSEC is a general IP security mechanism. It is used to provide authentication, confidentially, rejection of replayed attacks and key management. It can be used to provide security to individual user. It secures the routing architecture. It provides additional security to firewall/routers from all the traffic crossing the perimeter.

## **SSL VPN**

Secure Socket Layer VPN, also known as SSL VPN is used with a standard web browser. It uses Transport Layer Security (TLS) protocol in standard web browser to provide secure, remote access VPN capability. It uses end-to-end encryption to protect data that is transmitted between sender and receiver.

# IPSec VPN

Although SSL VPN, IPSec VPN and site-to-site VPN have the same purpose, they are very different in theory and practice. This often leads to a fundamental misunderstanding when configuring VPN along with the complexity of the problem. The site-to-site option is stationary whereas the remote access IPsec VPN option allows for connectivity from anywhere with an internet connection.

The SSL operates at layers higher than 3 and they don’t support applications that can’t be run through web browsers such as ping. The greatest advantage of IPSec is its transparency to applications. Since IPSec operates at Layer 3, it has essentially no impact on the higher network layers. As implied by its name, IPSec runs at the IP layer and, as such, is indifferent as to whether application traffic is being transported using TCP or UDP protocols. Consequently, IPSec is equally as appropriate for securing real-time traffic as it is for traditional data applications. In the below figure, an IPSec tunnel is created between Router 1 and Router 2. Data is transmitted in an encrypted format between these routers.

# TYPES OF LOAD BALANCING TECHNIQUES

There are many load balancing techniques which can be used to balance the load on a single VPN server.

* Round Robin
* Weighted Round Robin
* Least Connection
* Weighted Least Connection
* Agent Based Adaptive Load Balancing
* Chained Failover
* Weighted Response Time
* Source IP Hash
* Software Defined Networking (SDN) Adaptive

## **Round Robin**

Using this mechanism, the content access request is responded to by the load balance in a rotational basis.

## **Weighted Round Robin**

This algorithm maintains a weighted list of servers, where a heavier (higher) weight indicates preference.

## **Least Connection**

This algorithm considers the number of current connections each server has. When a client attempts to connect, the load balancer will determine the server with least number of connections and then assign the new connection to that server.

## **Weighted Least Connection**

A load balancer will consider two things: the weights/capacities of each server AND the current number of clients currently connected to each server.

## **Agent-Based Adaptive Load Balancing**

­­Each server in a network reports on its current load to the Load Balancer. This information from the servers is used to improve the decision making process for load balancing operations.

## **Chained Failover (Fixed Weighted)**

There is a predetermined **chain** of servers and all requests are sent to a server until it can't service more requests, then the next server in **chain** gets all requests.

## **Weighted Response Time**

A centralized scheduler assigns tasks to servers, processing on-line a sequence of task arrivals and departures. Each task runs for an unknown length of time, but comes with a weight that measures resource utilization per unit time. The *response time* of a server is the sum of the weights of the tasks assigned to it.

## **Source IP Hash**

This algorithm generates a unique **hash** key using the **source** and destination **IP** address of the client and server. This key is used to allocate the client to a particular server.

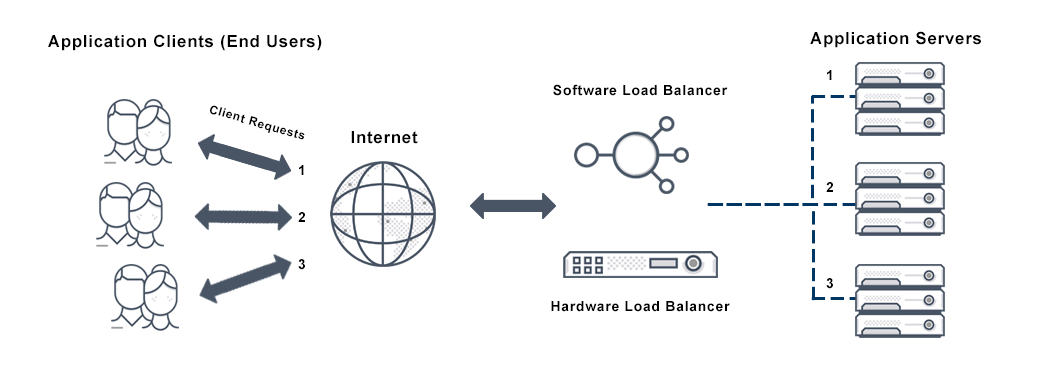
## **Software Defined Networking (SDN) Adaptive**

It uses multiple controllers in a network to solve the problems in single controller networks, to reduce the delay between controllers and switches.

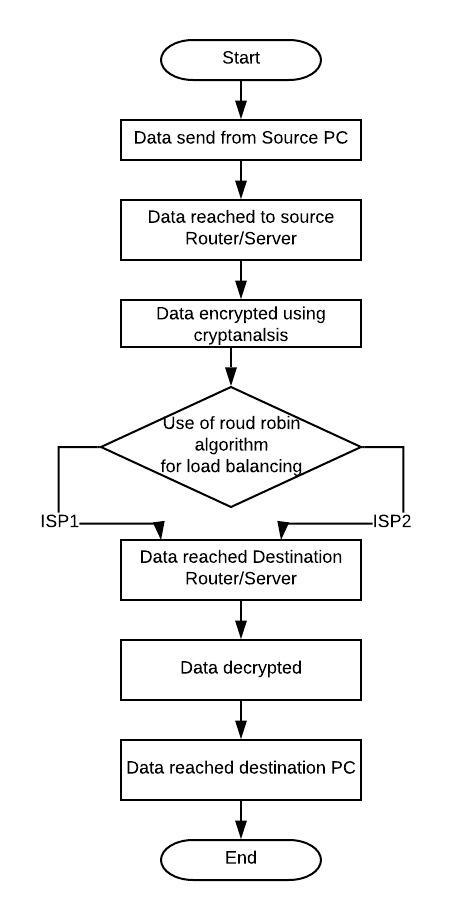
# ROUND ROBIN LOAD BALANCING TECHNIQUE

In Round Robin Load Balancing technique, a cyclical sequential distribution of requests per server is performed. It distributes the client request to multiple servers in a sequential way. The request goes to each server turn by turn.

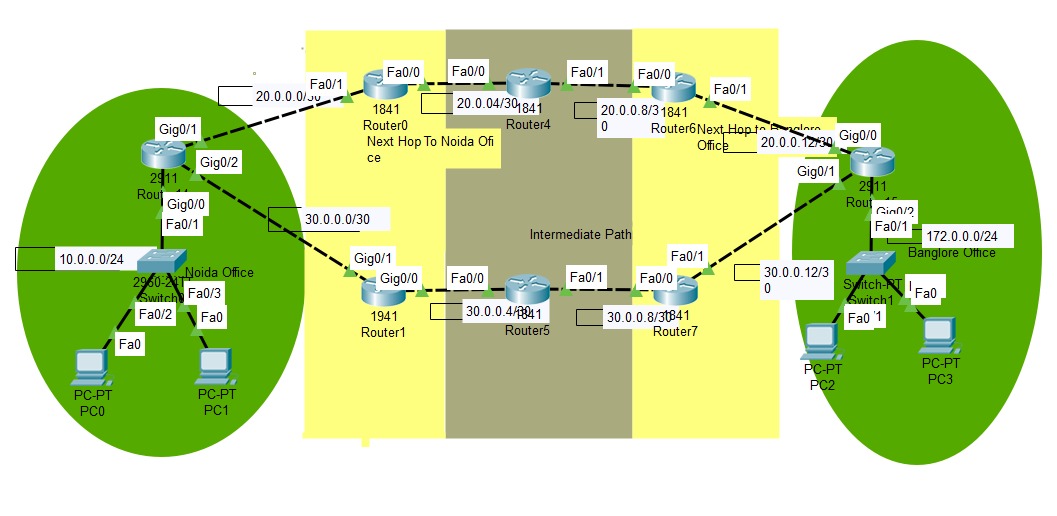
The round robin load balancing algorithm tells the balancer to repeat the distribution of servers to process the request in a cyclic way. It is most widely used load balancing technique as it is easy to execute. It works best when servers have roughly identical computing capabilities and storage capacity.

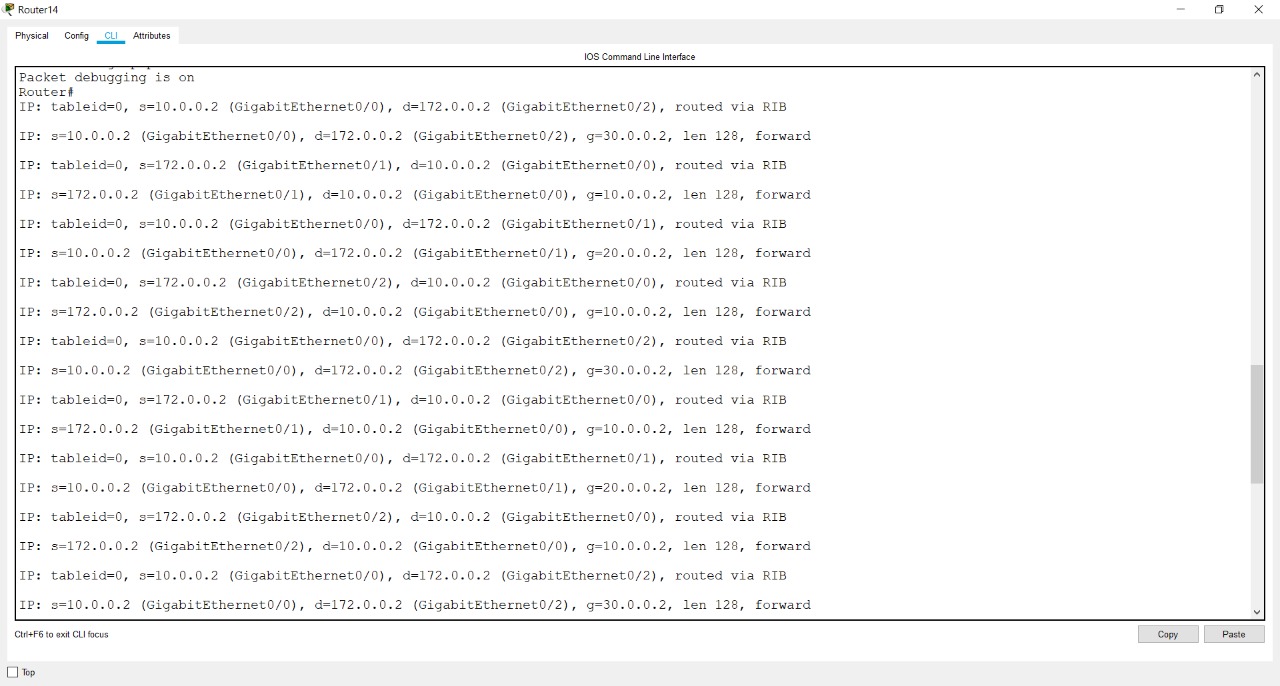
****

# DATA FLOW DIAGRAM

****

# SCREENSHOTS





# FUTURE SCOPE

Currently, the system is performing load balancing in VPN server using round robin algorithm. This is one of the basic technique that we have implemented considering our resources and requirements. The future scope of our project is-

* Optimized Performance of Routers.
* A limited number of routers are used in our project. It can be scale on a large number of routers which will increase the efficiency and performance of the network system.
* To use more efficient algorithms to increase the performance of various routers. Using different algorithm will eliminate the disadvantages of round robin. In round robin, the load balancer will distribute the load equally on both routers. So, one router may be loaded up a lot and go down.
* We can also use other techniques like SSL to implement VPN according to our requirements.
* Faster network system that will improve communication in sending and receiving data.

# CONCLUSION

The technology of our world is changing constantly and main application of this technology is communication. But due to some people misusing the technology they tend to disrupt the communication and compromise the security. Also, with advance security features, device sometimes compromise due to heavy load. So, to enable scalability, reliability and security, we have proposed the solution and implemented it.

This project was a very challenging task. My hypothesis was to implement load balancing with IPSec(VPN) in cisco packet tracer successfully which was not implemented earlier due to the constraints that simulator devices have such as difference of version, etc. After implementation, my results or output do support my hypothesis.

I think the commands that were executed for the results went smoothly and we faced no problems. This report has discussed how we can configure the load balancing on IPSec VPN technology. Because both are very different technologies and were never implemented before. The objective were to develop the necessary hardware configuration and software to have support of two technologies. However, both the objectives were met.

By implementing Load Balancing and then executing IPSec commands by overcoming compatibility issues of devices. If third party tries to eavesdrop the communication channel, they will never come to know about the source address, destination address or packet information due to encryption, authentication and integrity of Algorithm. Also, if due to heavy load on a server, the load balancing algorithm will distribute the load on another servers according to the constraints involved.