



# Deploy Redundancy of Internet using First Hop Redundancy Protocol and Monitoring it using IP Service Level Agreements (IPSLA)

Mohammad Hamid Ibrahim<sup>1</sup>, Komil B. Vora<sup>2</sup>, Kunal Khimani<sup>3</sup>  
 PG Student<sup>1</sup>, Professor<sup>2,3</sup>  
 Department of IT  
 V.V.P. Engineering College, Rajkot, India

## Abstract:

Availability and Security of the services are very important factors for the cross-platform network, in order to succeed the desired outcome, we are exploring First Hop Redundancy Protocol (FHRP) such as, Gateway Load Balancing Protocol (GLBP) Hot Standby Router Protocol (HSRP) and Virtual router redundancy protocol (VRRP). These protocols are providing redundancy and Reliability into the data link layer of Open System Interconnection (OSI) model by allowing multiple hosts to make a group among of them for load distribution and they are appearing in the form of a single virtual link. one or more than one router will be acting as an active hop for load balancing and forwarding the clients request to outside of the network, few more routers will be kept in a standby mode for a situation where if one of the active Hops fails down then Redundancy protocol will maintain connectivity by forwarding the clients requests to another Hop in the equivalent Group. For monitoring and measuring the performance of redundancy protocols, we deploy internet protocol Service Level Agreements (IPSLA) which is Feature of internetwork operating system (IOS) that allows us to analyse the active traffic of IP service.

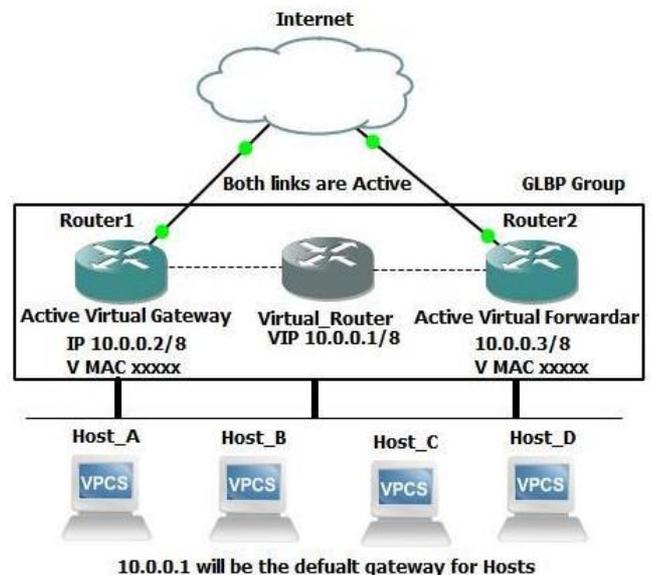
**Keywords:** FHRP, STP, GLBP, HSRP, IPSLA, MD5, VIP

## I. INTRODUCTION

Internet Protocol (IP) network host does not have any routing intelligence data, in fact the information concerning to routing is located in the routers which are default gateway of a network with a public Internet protocol (IP) that handles forwarding of packets from a Source to a destination and vice versa, However in single default gateway network all the load will be on a single router which forwards the total request of the clients to other networks, if the single default gateway fails hosts within the same subnet won't be able to establish communication with other networks.

**Therefore we need redundant links and load sharing among the routers in internet protocol (IP) networks.**

A method for addressing the sole default gateway problem is to deploy First Hop Redundancy Protocols such as Hot Standby Routing Protocol (HSRP), Gateway load balancing Protocol (GLBP), virtual Redundancy Routing Protocol (VRRP) Which are suitable option for creating redundancy and load balancing in IP network, FHRP Protocols are able of selecting automatically another route on a Local Area Network (LAN) for routing if the default router fails. These protocols can be deployed in already designed network Without bringing any physical changes in devices we essential need to perform some modification logically in the Network Layer by making a group among of the routers and assigning a virtual internet protocol (VIP) address which will be acting as default gateway for the clients. For tracking and monitoring the default gateway of our network we will deploy IP Service Level Agreements (IPSLA) which is uses the active Traffic for measuring the network performance and increasing the productivity of our network.



**Figure.1. GLBP Redundancy**

### A. Redundancy

Redundancy refers to the carriage of the similar information over multiple redundant links. Redundant links provides more ways to get the data from its source to a destination. By creating redundant link we can avoid interruption in the work and eliminate network downtime caused by link failure, which is to be expected as a cable failure or internet service provider (ISP) or any security attacks which potentially disruptive the network operation. In Internet protocol (IP) networks there are multiple solutions for increasing the network available and reliability by creating redundant links among the Switches and the routers, we can deploy First Hop Redundancy Protocol

(FHRP) protocol and in switching environment we can deploy Spanning Tree protocol (STP) which is used for managing the redundant links and avoiding the loops among the switches.

**B. FHRP Protocols Review**

First Hop Redundancy Protocol (FHRP) is used in a situation where there are two or more than two gateways are connected to a network if one goes down another will provide redundancy and service to the network. [1] First hop redundancy protocol is a networking protocol used to protect default gateways by allowing two or more routers to provide load balancing and redundancy for that address in the event of active router failure. [2] From the client's point of view default gateway is the first point for them to communicate with other networks if the default gateway goes down due to some reason which can be a cyber-attack or can be Internet service provider (ISP) failure, at that time all the client won't be able to establish connections with outside of their segment. for addressing single link communications there are some FHRP protocols which provide the functionality of load balancing and security into data link layer while we can maintaining its functionality and manageability by using internet service level agreements(IPSLA).[3]

**C. HSRP**

Hot Standby Router Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway. HSRP provides fast fault-tolerant in default gateway which takes less than 10 seconds for changing the default path to another available path in the same group. [4]

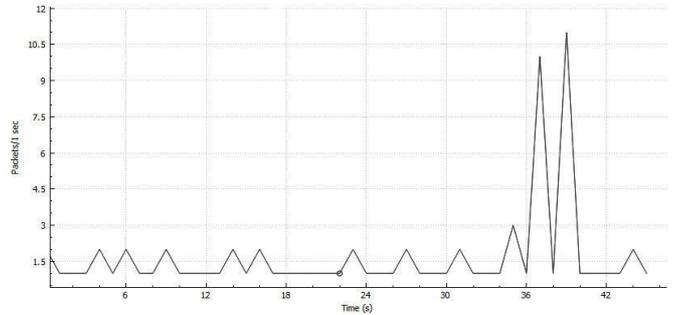
```
C:\>ping 10.0.0.254 -t
Pinging 10.0.0.254 with 32 bytes of data:
Reply from 10.0.0.254: bytes=32 time=41ms TTL=255
Reply from 10.0.0.254: bytes=32 time=20ms TTL=255
Request timed out.
Reply from 10.0.0.254: bytes=32 time=22ms TTL=255
Reply from 10.0.0.254: bytes=32 time=22ms TTL=255
Reply from 10.0.0.254: bytes=32 time=36ms TTL=255

Ping statistics for 10.0.0.254:
    Packets: Sent = 6, Received = 5, Lost = 1 (16% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 41ms, Average = 28ms
```

**Figure.2. HSRP while changing it is Path from one router to another router**

**D. VRRP**

Virtual Router Redundancy Protocol (VRRP) is an open standard protocol that can be used in such environments where equipment from multiple vendors exists the objective of VRRP is creating redundant links to disregard network downtime affected by a single link failure. Its process is similar to HSRP but varies in a couple of ways In VRRP a group is configured that contains a number of routers (gateways) one will be selected by the network engineer as master router in group. The physical IP address of the master router's is used by the clients as a default gateway. The backup members of the VRRP group will communicate with the master gateway and take over the duties of forwarding traffic if the master router fails. [6] VRRP is using Message Digest MD5 authentication keychain algorithm for communications in same group and has a faster timer for its default hello messages in every 1 second, VRRP have some limitation like direct tracking is not possible and does not support load balancing between different active links. [7]



**Figure.3. VRRP Hello messages interval**

HSRP uses industry standard Message Digest MD5 algorithm for authentications and security improvements. There are some limitations in HSRP protocol first limitation which arises is TRACKING when the serial Link which is straight connected to the ISP logically goes Down HSRP cannot determine to change it is default routers. HSRP is Cisco proprietary protocol it cannot be run on other vendor's routers. Large hello message interlude of 3 seconds i.e. hello packets are substituted between routers for every 3 seconds. HSRP is not able to provide load balancing in default gateway. [5]

**E. GLBP**

Gateway load balancing protocol (GLBP) creates a good failover and performs dynamic load balancing in default gateways of a network to prevent congestion and ensures smooth operation. By deploying GLBP protocol we can fully utilize our Resources such us routers and bandwidth. GLBP provides Reliability in the gateway of our network by distributing the load among several active paths. the best feature which GLBP providing is Failsafe as it automatically routes the packets to the different node if a node fails and keeps the network alive and constant provides short response time to enables tasks to be completed quickly.[8] GLBP has some limitations which is cisco propriety protocol can't be deployed by other vendors devices and also it uses Plaint text authentication will sending hello messages to each other in same group.

**Table.1. FHRP protocol comparison**

Protocol	FHRP Protocol Comparison		
	HSRP	VRRP	GLBP
Terminology	One active one standby	One master one backup	AVG and AVF
Communication	Ipv4 UDP 1985	112 INA	IPv4 UDP3222
Authentications	Plan Text MD5	Plan Text MD5	Plan Text
Active Selector	Highest value	Highest value	Highest value or highest IP
Active Timer	10s	10s	10s
Load balancing	NO	NO	Yes

**II. CONCLUSION**

After comparison of First hop redundancy protocol we come to that point that every protocol as some advantages and some limitations. Hop Stand routing protocol (HSRP) is a cisco proprietary protocol providing good redundancy protocol but cannot perform load balancing. Virtual Router Redundancy Protocol (VRRP) is an open source protocol for different vendor's products if we have in our organizations this protocol

as same limitation as HSRP which does not support load shares or load balancing among active links. Gateway load balancing protocol (GLBP) is also Cisco proprietary protocol which can perform Load balancing and also provide redundancy into default gateway of a network use Plaintext authentication which is a big limitation of this protocol a hacker easily can capture the network traffics and can attack into our network.

### III. PROPOSED WORK

While gateway Load balancing Redundancy protocol (GLBP) communicating and authenticating with each other in the same group using hello message for exchanging information between each other the hello message packets can be captured and Decrypted. In future we need to focus on different algorithms and different methods for addressing the authentication between hops in same group of GLBP protocol. They are sending hello message in plain text which can be easily captured and read by hacker if hacker got access to our authentication code or password so he or she easily can configure his own router and make the router as member of our group and makes his router highest priority and capture data and information.

### IV. ACKNOWLEDGEMENT

First of all, I personally want to appreciate management of the Vyavasayi Vidya Pratishathan (V.V.P) Engineering College for giving me the chance of being a student here to fulfill my dreams. I would also like to thank Principal Sir, HOD of IT department and staff members of IT Dept. for providing me support in all the aspects whenever I needed, also let me thank my expert advisor Professor Komil B. Vora for his nonstop sustenance his patience and motivation guidance's throughout of my research works and writing of my theses.

### V. REFERENCES

[1]. Nikhil Hemant, "Virtual Router Redundancy Protocol-A Best Open Standard Protocol in Maintaining Redundancy", *International Conference on Web Services Computing (ICWSC) 02 jun2011*.

[2]. Shilpi Sharma, "Review of First Hop Redundancy Protocol", *International Journal of Engineering Trends and Technology*, (IJETT) Volume 4 Issue 5- May 2013 ISSN: 2231-5381.

[3]. Sathis Kumar, "IP Redundancy and Load Balancing With Gateway Load Balancing Protocol", *International Journal of Scientific Engineering and Technology (ISSN: 2277-1581) Volume No.4 01 March. 2015*.

[4]. B.I.D. Kumar, "Performance Evaluation of HSRP based reliable Multi homed Network", *International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 6, Issue 8 August 2017*.

[5]. Er.Avtar Singh, "Review On High Availability And Faster Convergence In IP Networks", *international Journal Of Advanced Research In Computer Science Volume 8, No. 7, July – August 2017 ISSN No. 0976-5697*.

[6]. Ralph Droms, Ted Lemon, "The DHCP Handbook. SAMS Publishing", p. 436. ISBN 0-672-32327-3

[7]. T. Mann, J. Mogul, "Reverse Address Resolution Protocol", R. Finlayson, June 2000.

[8]. Microsoft, "TCP/IP Network Interface Configuration", 7 January 2009. Retrieved 2 June 2013. "Updated: January 7, 2009".

[9]. Source:[https://en.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol).

[10]. <http://www.9tut.com/hot-standby-router-protocol-hsrp-tutorial>.

[11]. [https://en.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol#Overview](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#Overview).