Review of First Hop Redundancy Protocol and Their Functionalities

Priyanka Dubey*[1], Shilpi Sharma*[2], Aabha Sachdev*[3]

*Amity University, Noida, Uttar Pradesh, India

***Abstract*- In this paper, we are focusing on data link layer protocols. First, when designing a network, one of the most important things to focus on when is designing a network on how to deal with failure. A major part of this research is trying to explore First Hop Redundancy Protocol and providing as much redundancy and security into the network as financially possible, while also maintaining performance and manageability. From the client's view, the first set of the network they deal without, outside of their local subnet, is the default gateway; if this gateway goes down, then access to an entire network outside their own network would go down. One good ways to deal with this is to implement a first hop redundancy protocol. On Cisco equipment, there are a couple of different options to choose from, including Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP). This defines the complete overview and differences of these protocols.**

***Keywords*- FHRP, HSRP, VRRP, GLBP, MD5**

I. INTRODUCTION

First Hop Redundancy Protocol (FHRP) is a group of protocols that allow a router on a LAN network to automatically take over if primary default gateway router fails. It is developed to solution in shared networks such as Ethernet or Token Ring. The devices on shared network segment are configured with a single default gateway address that points to the router that connects to the rest of the network. The problem comes when this primary router fails and there is a second router on the segment that is also capable of being the default gateway but end devices don't know about it. Hence, if the first default gateway router fails, the network stops working. Solution to this problem is First Hop Redundancy Protocols. The three main First Hop Redundancy Protocols are HSRP, VRRP and GLBP.

First hop redundancy protocols such as HSRP and VRRP provide default gateway redundancy with one router acting as the active gateway router with one or more other routers held in standby mode. GLBP enables all available gateway routers to load share and be active at the same time. But before first hop redundancy protocols were available, networks relied on Proxy ARP and static gateway configuration.

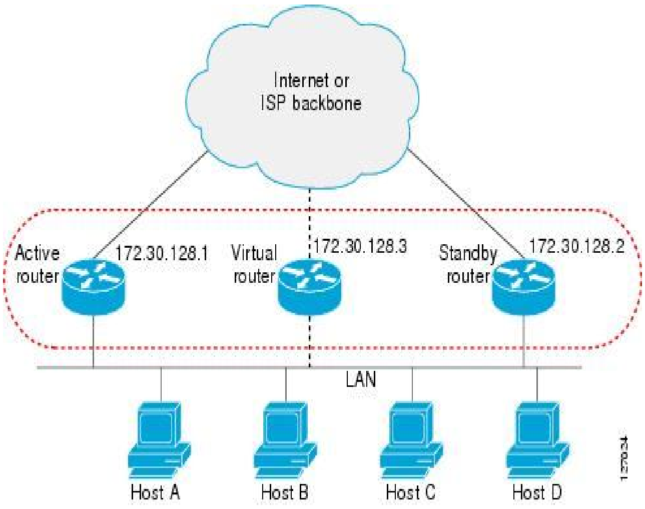

FIG. 1 Overview of First hop redundancy protocol

II. LITERATURE SURVEY

After study of RFC 2281, we came to know of the particular index 7 which show that this protocol does not provide security. The authentication field found within the message is useful for preventing misconfiguration. The protocol is easily subverted by an active intruder on the LAN. This can result in a packet black hole and a denial-of-service attack [1]. So an idea came into mind that this issue can be resolved using some algorithm or method which can provide more security.

III. TYPES OF FIRST HOP REDUNDANCY PROTOCOLS

There are many types of first hop redundancy protocols but in this paper we are going to Discuss HSRP, VRRP and GLBP.

A. Hot Standby Router Protocol (HSRP)

HSRP is a Cisco proprietary protocol that provides a mechanism which is designed to support non-disruptive failover. Without HSRP, each of the devices on the subnet would need to be individually configured to use a specific gateway, effectively not providing redundancy but limiting the number of clients that would be affected if a router were to go down. With HSRP, a group of routers (gateways) will be configured together, and a single HSRP virtual IP address and

MAC address will be created that are used by the devices on the subnet. The different routers in the HSRP will communicate to a select single active gateway that handles all live traffic. At this point, a single standby gateway is also selected. This standby gateway communicates with the active gateway via multicast on address 224.0.0.2 and will detect should the active gateway fail. When this happens, the standby gateways will take over the duties of the active gateway and continue traffic forwarding without much (if any) delay. When this happens, a new standby gateway is also selected.

In particular, HSRP protects against the failure of the first hop router. The protocol is designed for use over multi-access, multicast or broadcast capable LANs (e.g., Ethernet). A large class of legacy host which are not capable of dynamic discovery default router. HSRP provides failover services to those hosts.

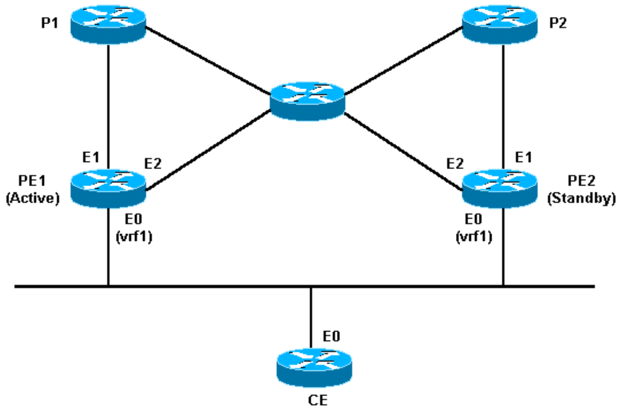

FIG. 2 OVERVIEW OF HOT STANDBY ROUTER PROTOCOL

B. *Virtual Router Redundancy Protocol (VRRP)*

VRRP is an open standard that can be used in environments where equipment from multiple vendors exists. Its operation is similar to HSRP but differs in a couple of ways. In VRRP, like with HSRP, a group is configured that contains a number of routers (gateways); one will be selected by the network engineer to be the master. The master router's physical IP address of the interface connecting the subnet 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, should the master fail. The IP address used always belongs to the master router which is referred to as the IP address owner. When the master router recovers, it will take back the duties of routing for that IP address.

It is possible to have multiple VRRP groups on a single subnet, which can be used to spread the load of the traffic coming off of a subnet. However, this must be done manually at the client's location, by changing their default gateway addresses.

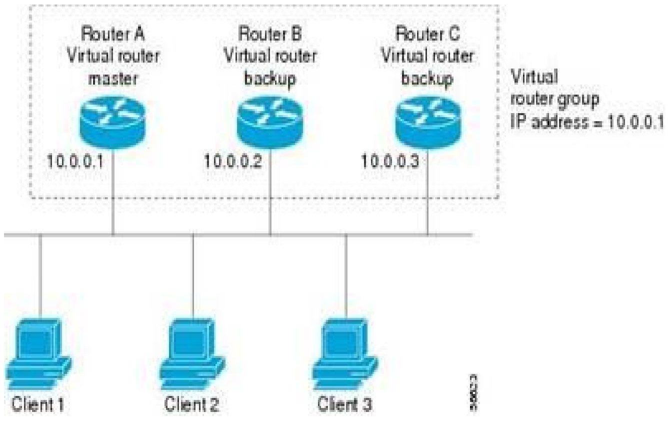

FIG. 3 OVERVIEW OF VIRTUAL ROUTER REDUNDANCY PROTOCOL

C. *Gateway Load Balancing Protocol (GLBP)*

GLBP is another Cisco proprietary first hop redundancy protocol. GLBP offers something that HSRP and VRRP does not i.e dynamic load balancing. In GLBP all of the routers that exist within the GLBP group are active and are forwarding traffic. When a GLBP is configured, one of the routers within the group will be elected as the Active Virtual Gateway (AVG) each of the other routers will act as back up. The AVG is responsible for assigning virtual MAC addresses to each of the members of the GLBP group; each of these members is referred to as an Active Virtual Forwarder (AVF). The AVG is responsible for responding to ARP request by subnet devices, and selecting which group's router will handle the traffic. The IP address of the default gateway is the same across all of the subnet devices; this IP address is virtual. When the device ARPs for a MAC address, the AVG will respond with one of the virtual MAC addresses. This way, the AVG is able to control which router will handle the load of each individual subnet device.

GLBP weighting has the ability to place a weight on each device when calculating the amount of load sharing that will occur through MAC assignment. Each GLBP router in the group will advertise its weighting and assignment. The AVG will act based on that value.

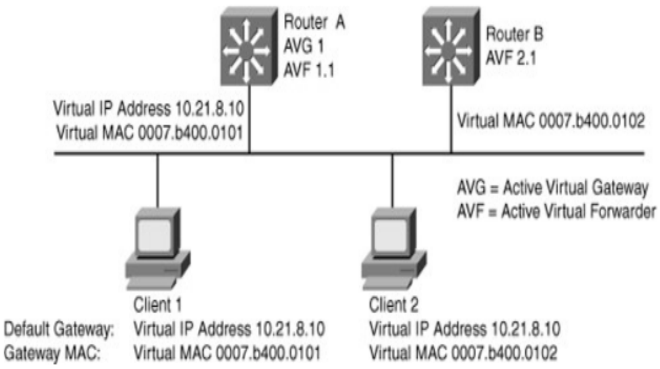
Router A
AVG 1
AVF 1.1
Router B
AVF 2.1
Virtual IP Address 10.21.8.10
Virtual MAC 0007.b400.0101
Virtual MAC 0007.b400.0102
AVG = Active Virtual Gateway
AVF = Active Virtual Forwarder
Client 1
Client 2
Default Gateway:
Gateway MAC:
Virtual IP Address 10.21.8.10
Virtual MAC 0007.b400.0101
Virtual IP Address 10.21.8.10
Virtual MAC 0007.b400.0102

FIG. 4 STRUCTURE OF GATEWAY LOAD BALANCING PROTOCOL

Protocol Features		HSRP	VRRP	GLBP
Router role		1 active router. 1 standby router. 1 or more listening routers.	1 master router. 1 or more backup routers.	1 AVG routers (active virtual gateway). Up to 4 AVF routers on the group (active virtual forwarder) passing traffic. Up to 1024 virtual routers (GLBP groups) per physical interface.
		Use virtual IP address.	Can use real IP address, if not, the one with highest becomes master.	Use virtual IP address.
Scope		Cisco proprietary	IEEE standard	Cisco proprietary
Election		Active router Highest priority Highest IP (tiebreaker)	Master router Highest priority Highest IP (tiebreaker)	Active virtual gateway Highest priority Highest IP (tiebreaker)
Optimization feature	**Tracking**	Yes	Yes	Yes
	Pre-empt	Yes	Yes	Yes
	Timer adjustments	Yes	Yes	Yes
Traffic type		224.0.0.2-udp 1985(version 1) 224.0.0.102-udp 1985(version 2)	224.0.0.18 - UDP 112	224.0.0.102- UDP 3222
Timers		Hello – 3 seconds	Advertisement- 1 second	Hello– 3 seconds
		(hold) 10 seconds	(master down interval)3 * advertisement+ skew time	(hold) 10 seconds
			(Skew time)(256 - priority)/256	
Load balancing functionality		Multiple HSRP group per interface/ SVI/routed int.	Multiple VRRP group per interface/ SVI/routed int.	Load balancing oriented-weighted algorithm. Host dependent algorithm. Round robin algorithm (default).
		Requires appropriate distribution of GW IP per clients for optimal load balancing (generally through DHCP).	Requires appropriate distribution of GW IP per clients for optimal load balancing (generally through DHCP).	Clients are transparently updated with MAC according to load balancing algorithm through ARP requesting a unique virtual gateway.

TABLE 1 DIFFERENCE BETWEEN FEATURES OF HSRP, VRRP, GLBP

After describing all the protocols of First Hop Redundancy Protocols, we come to issues present. This Issue discussion is presented as conclusion to the review conducted in this document.

IV. ISSUES IN FHRP

As Index 7 of RFC 2281 tells that these protocols do not provide security; the authentication field found within the message is useful for preventing misconfiguration. The protocols are easily subverted by an active intruder on the LAN. This can result in a packet black hole and a denial-of-service attack. It is difficult to subvert the protocols from outside the LAN as most routers will not forward packets addressed to the all-routers multicast address (224.0.0.2) [1].

This issue of HSRP can be resolved using MD5 algorithm with it because MD5 algorithm provides hash functions which can’t be re-engineered. So it will be appropriate solution of this problem. Thus LAN can be made more secure and it can be saved from internal attacks.

V. CONCLUSION

In this paper, we have discussed about some first hop redundancy protocols like HSRP, VRRP and GLBP, their working scenario and difference between these all. Every protocol works in its own specific way and contains different type specialty within it.

VI. FUTURE SCOPE

In future work, we will implement the explanation and validation of it. And after that we will work upon the various features within it. Furthermore we will define more precise technique for it which will be able to provide more security and authenticity to LAN.

REFERENCES

[1] T. Li Juniper Networks, B. Cole Juniper Networks, P. Morton Cisco Systems, D. Li Cisco Systems, RFC 2281 March 1998.

[2] R. Rivest MIT Laboratory for Computer Science and RSA Data Security, Inc. RFC 1321,April 1992

[3] Deering, S., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[4] United States Patent. Patent Number: 5,473,599. Standby Router Protocol. Date of Patent: Dec. 5, 1995.

[5] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[6] Deepakumara J., Heys H.M. and Venkatesan R., FPGA Implementation of MD5 Hash Algorithm, Canadian Conference on Electrical and Computer Engineering, 2001, vol. 2, pp. 919-924, 2001.

[7] Alok Kumar Kasgar, Jitendra Agrawal, Satntosh Shahu, “New modified 256-bit MD5 Algorithm with SHA Compression Function”, March 2012.

[8] S. Chang, M. Dworkin, Workshop Report, The First Cryptographic Hash Workshop, Report prepared, NIST 2005.

[9] Xiao Yun Wang, Dengguo, HAVAL-128 and RIPEMD], Cryptology ePrint Archive Report 2004/199, 16 August 2004,

[10] J. Black, M. Cochran, T. Highland: A Study of the MD5 Attacks: Insights and Improvements, March 3, 2006

[11] Tao Xie and Dengguo Feng (30 May 2009). How to Find Weak Input Differences for MD5 Collision Attacks.

[12] Christof Paar, Jan Pelzl, Bart Preneel (2010). Understanding Cryptography: A Textbook for Students and practitioners. Springer. p. 7. ISBN 3642041000.