J. Appl. Environ. Biol. Sci., 7(3)268-278, 2017
© 2017, TextRoad Publication

ISSN: 2090-4274
Journal of Applied Environmental and Biological Sciences
www.textroad.com

Performance Evaluation of First HOP Redundancy Protocols (HSRP, VRRP & GLBP)

Zia Ur Rahman[*1], Safyan Mukhtar[2], Sajjad Khan[2], Raees Khan[2], Zakir Ullah[1], Reena Rashid[3], Waqas Ahmad[4]

Department of Computer Science, Bacha Khan University, Charsadda, KPK, Pakistan[1]
Department of Mathematics & Statistics, Bacha Khan University, Charsadda, KPK, Pakistan[2]
Department of Computer Science, Shaheed Benzir Butto Women University, Peshawar, KPK, Pakistan[3]
Department of Computer Science, University of South Asia, Lahore, Punjab, Pakistan[4]

Received: November 11, 2016
Accepted: January 28, 2017

ABSTRACT

The first hop redundancy protocols includes three protocols Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP). Each protocol has its own purpose and has its own advantages and disadvantages. FHRP was developed to reduce traffic loss. These protocols help particular organization to successfully send the traffic from source to destination without loss of many packets. In case of the failure of one system, there is a standby system which automatically activates itself and continues sending the traffic. The HSRP protocol and GLBP protocol are Cisco propriety whereas the VRRP protocol is the Institute of Electrical and Electronics Engineers (IEEE) standard. The paper contains the detail information of the protocols, their working and comparison between them. The comparison indicates that which protocol is best in which scenario and which is best among the three protocols. These protocols work on layer 3 devices that are on the Transport layer. The protocols are capable of transferring the traffic if one of the routers of the network goes down due to some technical fault. The FHRP includes different kind of protocols but the paper contains three main protocols that are HSRP, VRRP and GLBP.

KEYWORDS: FHRP (First Hop Redundancy Protocol), HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol), GLBP (Gateway Load Balancing Protocol)

1. INTRODUCTION

Protocol is a set of rules and regulations that determine how data will be transferred in the field of computer networking and telecommunication [1]. A routing protocol specifies how routers communicate with each other and how the data is transferred from one router to another and finally to the destination. Load balancing is the practice of distributing traffic among multiple paths to the same destination in order to use bandwidth efficiently. Sending all packets on a single route probably is not the most efficient use of available bandwidth and thus the bandwidth is wasted. Instead, load balancing or load balancing protocols should be implemented to swap traffic between two paths or more [2].

Its main goal is to improve throughput. It requires multiple routes or paths to divide the traffic or load distributed equally between the paths. Load balancing is implemented to improve the redundancy and throughput. To implement load balancing different routing protocols are used which equally distribute the traffic and utilizes the available bandwidth. In some cases the term load balance can be used interchangeably with the load sharing [3]. There should be a technique or protocol that can be used for the utilization of the available bandwidth. If the traffic is transferred from source to destination through router from a same path so the other path will transfer no traffic and hence there will be the loss of the bandwidth, to minimize such a situation there are some protocols used. Redundant links are used to double the available bandwidth. These links are also used for the load balancing in the network [4]. When the load balancing protocols are implemented on the routers then the protocols are able to transfer or forward the traffic with the help of routing table (Each router has its own routing table). Routing table has the information about the topology [5].

2. PROTOCOLS

A. HOT STANDBY ROUTER PROTOCOL (HSRP)
B. VIRTUAL ROUTER REDUNDANCY PROTOCOL (VRRP)
C. GATEWAY LOAD BALANCING PROTOCOL (GLBP

A. HOT STANDBY ROUTER PROTOCOL (HSRP)

Corresponding author: Zia Ur Rahman, Department of Computer Science, Bacha Khan University, Charsadda, KPK, Pakistan. Email: zia.cs@bkuc.edu.pk

One way to achieve maximum uptime that is the network does not fail is to use HSRP, which provide redundancy to the network that in case of failure the network should recover from first hop problem as soon as possible [5]. By sharing an IP address and a MAC (Layer 2) address, two or more routers can act as a single virtual router. The members of the virtual router group continually exchange status messages that which router is alive and which are down. The failure of one router will let another router to take the network responsibilities. In such a way the packets can easily be sending or received [6].

a. Operation

HSRP is a Cisco proprietary protocol that enables the network engineer to add more than one redundant device to achieve network reliability. The different routers in the HSRP group will communicate to select a single active router gateway that handles all the network traffic. When configuring a router to be an active router, the standby router at this point is also selected. Both the standby and the active router will communicate through sending a Hello messages and will detect if the active router fails. When the failure occurs one of the standby router take the duties of the active router with minimum delay and at the same time another standby router is selected.

b. Addressing

HSRP has a MAC address 00-00-0c-07-ac-xx, 00-00-0c represents Cisco, 07ac represents HSRP and xx represents group number. If group number is 5 so 05 will be placed instead of xx as 05 is the Hexa conversion of the 5 similarly if group number is 17 so 11 will be placed instead of xx.

c. Packet format

Version	Opcode	State	Hello time
Hold time	Priority	Group	Reserved
Authentication Data			
Authentication Data			
Virtual IP Address			

Table 1: HSRP Packet Format

In this Table 1, the fields are explained as follows.

- Version (1 octet): The version field defines the version of the HSRP. It may be version 1 or version 2.
- Op Code (1 octet): The Op Code describes the type of message that the packet contains. Possible values are: 0 - hello, 1 - coup and 2 - resign. Hello messages are used to check that the router running the HSRP is capable of being an active router. Coup messages are sent when a router is wishing to be an active router. Resign messages are sent when a router is no longer an active router.
- State (1 octet): Each standby router in the standby group has a state machine. The state field describes the current state of the router. There are different states: 0 - initial, 1 - learn, 2 - listen, 4 - speak, 8 - standby, and 16 - active.
- Hello time (1 octet): It contains the approximate period between the hello messages that the router sends, measured in seconds.
- Hold time (1 octet): Hold time indicates the amount of time that the router waits before the states of two or more routers are changed.
- Priority (1 octet): This field is used to check the priority of the routers. The highest priority router will be the active router of the network.
- Group (1 octet): This field specifies the standby group.
- Authentication Data (8 octets): This field contains eight-character password.
- Virtual IP Address (4 octets): If the virtual IP address is not configured on a router, the address can be learned from the hello message from the active router. An address is only learned if no HSRP standby IP address has been configured, and the hello message is authenticated (if authentication is configured).

Hot Standby Router Protocol example

In Figure 1 we have N2 as a computer or a sender device which will send data to the destination N1. We configure the HSRP protocol on the R1 and R2 router. The gateway needs to be mentioned on the source device so we add Virtual IP address as a default gateway. If we configure R1 to have a highest priority so the traffic will go to R1 then to R3 and then to N1 through switch, but if for some reason the R1 router goes down so the

R2 router will be able to take the responsibilities and the message sending will be done through R2. In HSRP the other router will not be able to take the duties of the first router until the preemption is disabled in the configuration mode of the router. Once the preemption is enabled so it can forward the traffic. Here the priority of the R1 is high so it is our active router and the R2 router will be our standby router. HSRP does not automatically do load balancing.

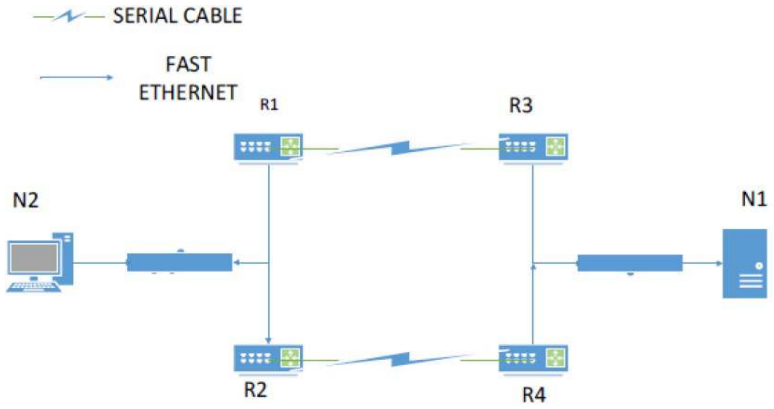

Figure 1: HSRP Example

B. **VIRTUAL ROUTER REDUNDANCY PROTOCOL (VRRP)**

VRRP is an open standard that can be used where the equipment of various companies exists. Its operation is nearly the same as that of HSRP but differs in a couple of ways [7]. In VRRP, like with HSRP, a group of routers are configured in which the network engineer selects one master router and the other a backup router. The physical IP address of the master router is used by the clients as a default gateway. The backup members of the VRRP group will communicate with the master gateway through hello messages and take over the duties of the master router when the master router goes down or some error occurs [7]. The IP address used always belongs to the master router which is referred to as the IP address owner. When the master router recovers from error it will again take its responsibilities back and will forward the network traffic itself [8].

a. Operation

VRRP adds a group of routers that can act as network gateways that enable the traffic to pass through that gateways. Routers in the VRRP group elect a master through the VRRP election mechanism to act as a gateway. VRRP works as follows:

- The role of the routers of the VRRP group is determined by their IP addresses and by their priorities. The router with the highest priority will be the master router and the others with the low priorities will be the backups. If during the election routers have the same priority, then one with the highest IP address becomes the master. The master send VRRP advertisements at regular intervals to notify the backups that it is working properly and each of the backups starts a timer to wait for advertisements from the master.
- In preemptive mode, when a backup receives a VRRP advertisement, it compares the priority in the packet of the master router with its own priority. In case, if the priority of the backup is higher than the backup will become the master otherwise, it remains as a backup router with the preemptive mode, a VRRP group always has a router with the highest priority as the master for packet forwarding to the destination.
- In non-preemptive mode, a router in the VRRP group remains a master or backup router as long as the master does not fail due to some reason. A backup does not become the master even if it is configured with a higher priority because the non-preemptive mode helps avoid frequent switch over between the master and backups.
- If the timer of a backup expires but the backup still does not receive any advertisement from the master so it consider that the master fails. In such a case, the backup consider itself as the master router and sends VRRP advertisements to all the other routers to start a new master election.

b. Addressing

VRRP has a mac address 00-00-5E-00-01-XX. 00-00-5E is derived from Internet assigned numbers authority (IANA), 00-01 indicates VRRP protocol and XX represents group number if group number is 5 so 05 will be placed instead of xx as 05 is the Hexa conversion of 5.

c. Packet format

Version	type	Virtual Rtr Id	Priority	Count IP Addrs
Auth Type		Advertisement Interval		Checksum
IP Address (1)				
IP address (n)				
Authentication Data (1)				
Authentication Data (2)				

Table 2. VRRP Packet Format

In Table 2, the fields are explained as follows:

- Version: The version field specifies the VRRP protocol version of the packet.
- Type: The type of the VRRP packet is specified in the TYPE field.
- Virtual Rtr ID: The Virtual Router Identifier (VRID) field identifies the virtual router this packet is reporting status for.
- Priority specifies the sending VRRP routers priority. VRRP routers backing up a virtual router has to use the priority values that varies from 1 to 254 (decimal).
- Count IP Addresses: The number of IP addresses that are present in this VRRP advertisement.
- Auth Type: Identifies the authentication method which will be used at the time of communication.
- Advertisement Interval: Advertisement interval indicates the time interval between advertisements generally in seconds. This time can be changed through configuration.
- Checksum: It is a 16 bit field which is used to detect data corruption while transferring the data.
- IP Address (es): Virtual router having one or more IP addresses.
- Authentication Data: Authentication is utilized for simple text authentication.

Virtual Router Redundancy Protocol example

In Figure 2 N2 wants to communicate with N1. The working of VRRP is the same as that of the HSRP but the difference is that we manually configure the HSRP router to take the duties of other router through the preempt enabled command but in VRRP we do not have to configure manually, if the router fails it will automatically take the duties of the active router. The router through which the traffic will pass is called the ACTIVE router and the router which is not the active router is called the backup router. Here if the priority of the cnc1 router is high so it will be the active router and the cnc2 with less priority will be the backup router. VRRP does not achieve load balancing automatically [9].

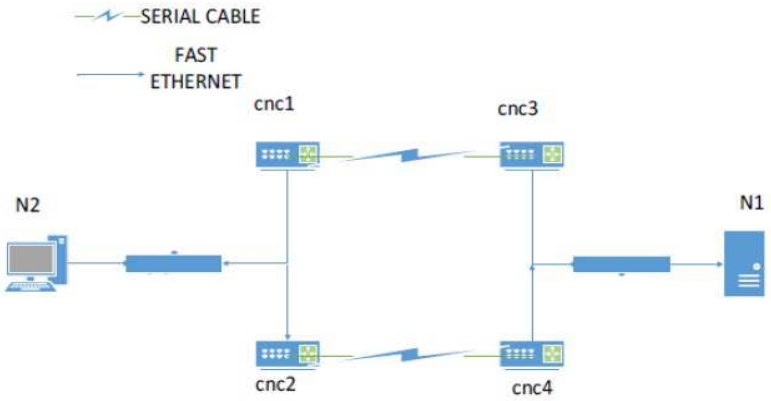

Figure 2: VRRP Example

C. **GATEWAY LOAD BALANCING PROTOCOL (GLBP)**

To achieve load sharing between the routers along with redundancy, Cisco has a new protocol called the GLBP. It is a Cisco proprietary that improves the efficiency of the FHRP by allowing automatic load balancing [10].

a. Operation

LBP specifies a protocol that provides load balancing over multiple gateways via a single virtual IP address. AVG is elected from the members of the GLBP group. Other members of the group provide backup for the

AVG if for some reason it is not available. The AVG assigns a virtual MAC address to each member of the GLBP group. These gateways become the Active Virtual Forwarder (AVF) for that virtual MAC address, which has the responsibility to forward the packets to other routers or to the destination [11].

b. Timers

There are four main timers that control GLBP operation.

- Hello time: The approximate period between the Hello messages sent by the GLBP gateway. The Hello time is normally learned from the AVG. If the hello time is not learned then manually configured hello time. The default value is 3 seconds and the range is 50 milliseconds to 60 seconds. The Hello time and Hold time can also be set using the commands.
- Hold time: Hold time is used to determine if action should be taken to takeover forwarding and/or the AVG function. Each time a hello is received, this timer is re-started. The Hold time should be at least three times the value of the Hello time and must be greater than it. The Hold time is normally learned from the AVG. If the Hold time is not learned, the manually configured time is used. The default value is 10 seconds, and the range is from 1 second to 180 seconds.
- Redirect time: The time for which the AVG continues to redirect hosts to an AVF. The Redirect time is normally learned from the AVG. If the time is not learned, the manually configured value is used. The default time is 5 minutes, and the range is from 1 second to 60 minutes.
- Secondary Hold Time: The period of time for which a Secondary Virtual Forwarder (SVF) remains valid after the Primary Virtual Forwarder becomes un-available.

Gateway Load Balancing Protocol Example

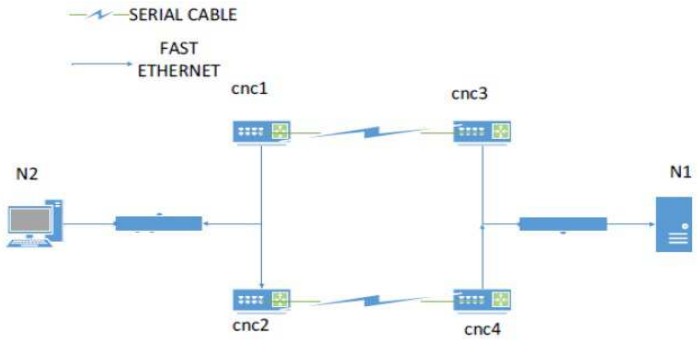

Figure 3: GLBP Example

In Figure 3 N2 system wants to communicate with N1. We configure the GLBP protocol on the cnc1 and cnc2 router. If the cnc1 router has the highest priority so this router will be the AVG and the cnc2 router will be the AVF. If N2 system wants to communicate with N1 system so the traffic will be forwarded through the AVG router that is through cnc1. If the N2 system again wants to communicate with N1 system so it will go through the AVF router that is through the cnc2 router because the GLBP protocol automatically balances load. If the traffic is passed through one router in one cycle so in the second cycle the traffic will be passed from the other router because the GLBP router is designed for the load balancing as well as for the FHRP [12].

3. METHODOLOGY

Use case is a number of steps that are used to communicate or to interact between the roles. Role is an actor in the Unified Modelling Language (UML).

Actor may be a human. Use case is the interaction between the user and the system [13]. The use case contains all the activities that are important to the users. The use cases are represented as ovals in the UML. The ovals contain the name of the use case. The advantage of the use case is that it provides a short summery of the system that what the system will do [14].

Use cases are extremely popular in Software Engineering. Steps in designing the use cases are:

- Identify the users
- Roles concerned with each user
- Goals associated with each role
- Create use case for each goal
- Structure the use cases

Advantages of Use cases

Use cases has the following Advantages:

- Use cases helps to ensure that the correct system is developed by capturing the requirements from the user's point of view.
- Use cases helps in the elicitation phase.
- They are easy to understand.
- Use cases helps to manage the complexity of the large projects.
- Use cases helps to make a project successful.

a. Use case of HSRP

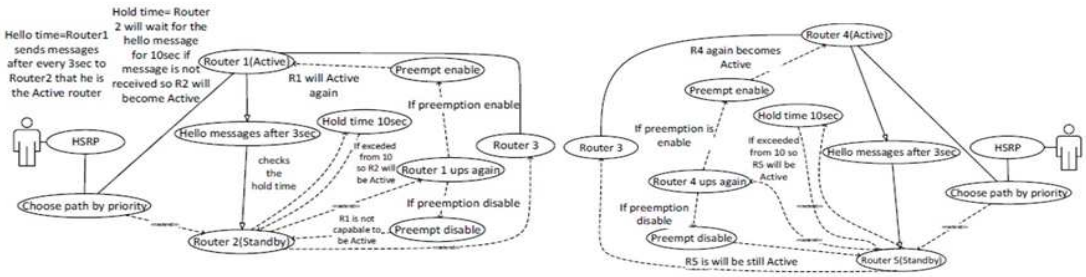

Figure 4: HSRP Use case

The Figure 4 defines the overall structure of the HSRP protocol. The use case diagram has an actor that communicates with the other actor through the network and in return the other actor gives reply or even send some messages. An actor that communicates through network has an HSRP protocol configured. Through HSRP there are two paths, one to be chosen for the transfer of the traffic. The HSRP protocol will choose that path which will have the highest priority and is active at that time. Say Router1 has the highest priority and is active so the traffic will go from Router1 to Router3. If the Router1 is not active at that time so the traffic will be forwarded through the standby router that is Router2. While Router1 is active so it will send a Hello messages after every 3sec to Router2 the sending of messages denotes that the Router1 is active if due some technical fault the Router1 goes down so the messages will not be received by the Router2 therefore it will check its hold time if it exceeds from 10 sec so Router2 will change its status from standby to active and then the traffic will go through Router2 [15-17]. When Router1 gets active so Router2 will check that the pre-emption on the Router1 is enabled or disabled if it is enabled so Router1 will be active if it is disabled so the active router is still Router2 as in HSRP the preemption should be configured manually. The Router3 will transfer traffic to Router4 and then to the actor eventually. Same procedure will be applied to receive the traffic.

b. Usecase of VRRP

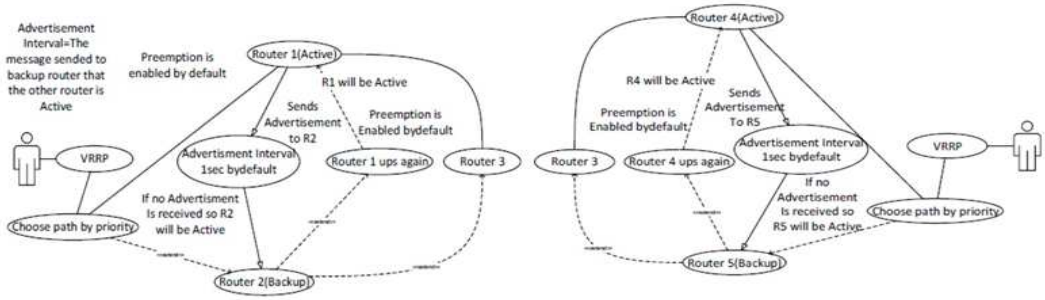

Figure 5: VRRP Use case

The Figure 5 shows the Usecase of VRRP that how this protocol works over the network. An actor wants to communicate with the other actor over the network on which VRRP is configured.

The VRRP protocol chooses the path from the available paths. Let be forwarded through this router to Router3. If the Router1 is not active at that time so the VRRP protocol will transfer the traffic through Router2. While the Router1 is active so it will send advertisement to Router2 after every sec that the active router is Router1. HSRP sends the hello messages whereas the VRRP sends the advertisement messages.

If no advertisement messages are received by Router2 so the status of the Router1 will change from active to backup and Router2 will change from backup to active.
Now the Router2 becomes active so the communication will be done through Router2. After some time if Router1 becomes active again so it has the capability of taking the responsibilities from Router2 because unlike HSRP VRRP does not require to enable the preemption manually rather preemption is enabled by default. The traffic forwards from Router1 to Router3 where Router3 sends it to Router5 and finally to the receiver that is to the other actor. The receiver than replies or send the message to the first actor in the same way that is through VRRP protocol.

c. Use case of GLBP

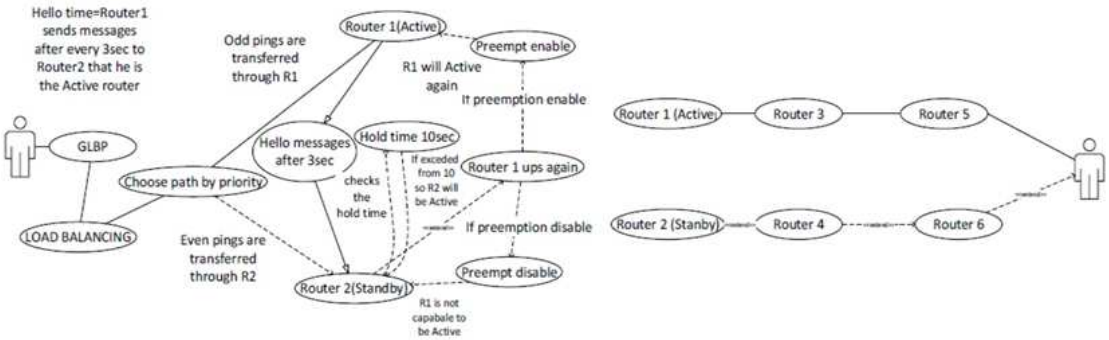

Figure 6: GLBP use case

The Figure 6 shows that how GLBP protocol is used for the FHRP and also for load balancing. The GLBP is configured on the network so if an actor wants to communicate with the other actor. The GLBP protocol first passes through the load balancing which chooses the path through priority the odd ping is passed through the Router 1 and the even pings are passed through the Router 2 so in this way GLBP achieve load balancing. Here Router 1 is active and Router 2 is the standby router however at the same time both the routers can send the traffic to achieve the load balancing. Router 1 sends hello messages to router 2 after every 3 sec which shows that Router 1 is the AVG. If Router 1 goes down so Router 2 will check its hold time if it exceeds from 10 sec so Router 2 will change its state from standby to active and then the transmission of data will be through Router 2. After some time if Router 1 ups again so Router 2 will check the preemption on the Router 1 if the preemption is disabled so Router 1 will not be able to active itself but if the preemption is enabled so the Router 1 will become active. Like HSRP GLBP also has to be configured to enable the preemption. The odd pings will be transferred through Router 1 then to Router 3 after that it will transfer to Router 5 and final to the actor. The even pings will be transferred through Router 2 then to Router 4 after that it will transfer to Router 6 and finally to the actor.

4. SIMULATION RESULTS

Topology of the network plays an important role in making a network. Topology shows overall design of the network that how many devices should be added.
The following topologies show the working of the FHRP.

a. HSRP topology
b. VRRP topology
c. GLBP topology

a. HSRP Topology

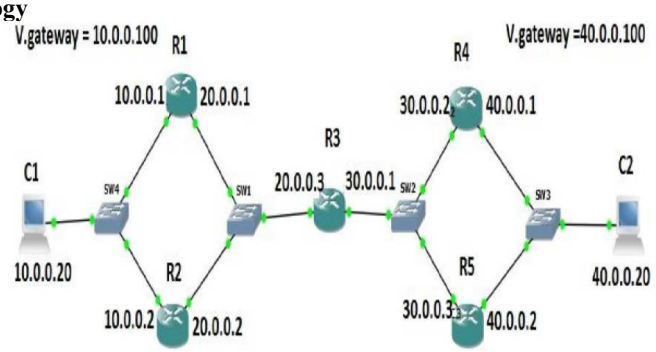

Figure 7: HSRP topology

The Figure 7 shows HSRP topology that how FHRP implements and how the data is transferred successfully even if the active router fails. To prevent the traffic to be lost hsrp is one of the protocol used. In case of transferring an important data there are chances for loss of data if the traffic transferring device fails. To avoid such kind of situation we use FHRP. In this C1 system wants to communicate with C2 with the help of HSRP. Here R1 is active router and standby router is R2. HSRP is configured on the R1 and R2. As an active router is R1 so the traffic will be forwarded through R1 then to R3 then to R4 and finally to C2. If the active router fails that is the R1 fails so HSRP provide the facility to use the standby router then traffic will be transferred through standby router that is through R2 then to R3 then R5 and finally to C2. When the active router transfers data so at that time the standby router does not transfer data. In the above figure C2 also communicates back with the C1 system by using HSRP because in the above topology HSRP is configured on both sides so that the response of C2 to C1 can successfully be transferred without the loss of data even when one router fails. While C2 replies to C1 so data will be transferred to R4 because it is active router than it will pass on to R3 then to R1 and finally to C1. When R4 router goes down so the standby router will take the responsibilities of transferring the data so the data will be send through R5 then to R3 then to R2 and finally to the destination system that is C1.

- **Packet Missing in HSRP**

The following Figure 8 shows the packet drop in HSRP.

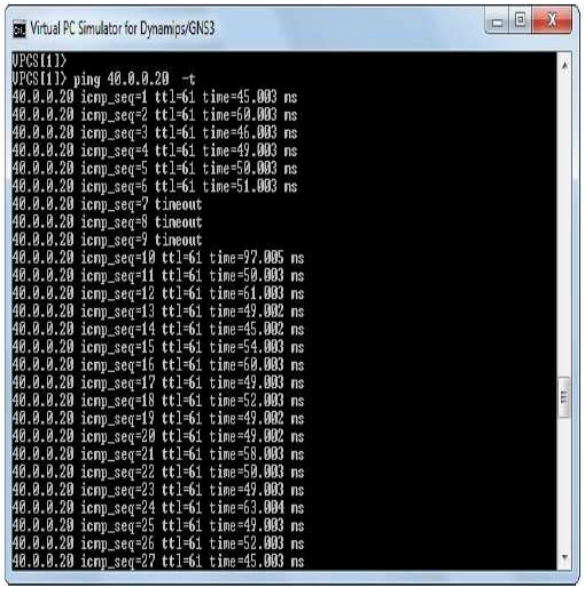

Figure 8: Packet missing in HSRP

b. VRRP topology

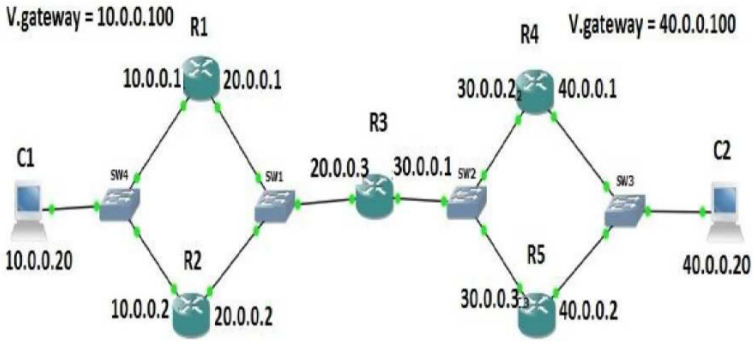

Figure 9: VRRP topology

The other protocol of FHRP is VRRP it is a non Cisco property. The working of the VRRP is same as that of the HSRP but differ in couple of ways. The VRRP also ensures that traffic should be passed even one of the device in a network fails. In figure 9 C1 system wants to communicate with C2 through VRRP. Here the Master router

is R1 and the backup router is R2. The VRRP is configured on R1 and R2. The traffic will pass through R1 because the R1 is the Master router than it will pass it to R3 then to R4 and finally to C2 but when due to some problem with R1 or R1 goes down so the backup router will take the charge and transfers the traffic so the traffic will pass through R2 then to R3 then to R5 and finally to C2. Here the C2 also replies to C1 through VRRP because in this topology the VRRP is configured on both sides that is multiple VRRP are configured. So R4 is the Master router and R5 is the backup router. The traffic will be forwarded through R4 then to R3 then R2 and finally to C1 but if R4 fails due to some reason then R5 that is the backup router will change its state from backup to active and then the data will be transferred through R5 then to R3 then to R2 and finally to C1. If the active router ups again so it will directly take the duty of forwarding the traffic because unlike HSRP, VRRP has the preemption enabled by default and there is no need to configure it manually.

Packet Missing in VRRP

The Figure 10 shows packet missing of VRRP. As GLBP misses no packet while the standby router gets active so this is the advantage of the GLBP over the HSRP and VRRP.

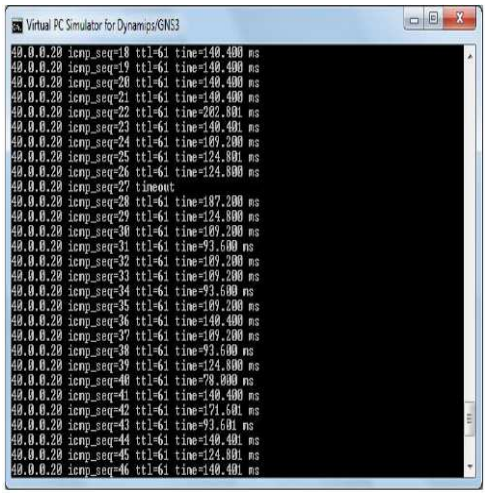

Figure 10: Packet missing in VRRP

c. GLBP topology

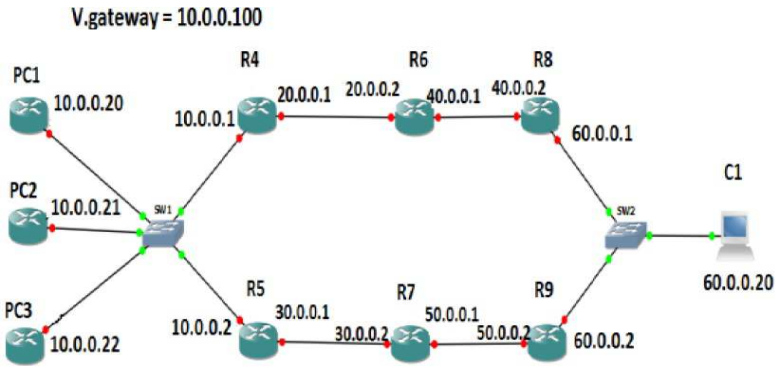

Figure 11: GLBP topology

In this Figure 11 PC1, PC2 and PC3 are connected from another network and the three paths are supposed to merge in two paths so as to manage the traffic load balancing protocol is needed. We implement the GLBP on the R4 and R5 so that the traffic is equally divided and can be transferred successfully. The first packet sending from PC1 will be transferred through R4, other packet sending from PC2 will be transferred through R5 and the packet sending from PC3 will be again transferred through R4 so in this way the load balancing is achieved. As GLBP is the FHRP so it also provides a backup if the network device fails. The GLBP is configured on R4 and R5 so R4 is the Active Virtual Gateway and R5 is the Active Virtual Forwarder so if during the transmission of data R4 goes down then R5 has the responsibility to transfer the data of all the three paths that is the data of PC1, PC2 and PC3. So from the figure it is clear that the GLBP is a new technology and can be used for multiple purposes that is for FHRP and also for the load balancing. GLBP has a hello time of 3 sec and the hold time of

10 sec this means that if R4 fails or does not transmit the data so R5 will wait up to 10 sec and after that R5 will be the master router. The preemption is disabled by default in GLBP and has to be configured manually.

Packet Missing in GLBP

The Figure 12 tells that there is no packet loss in GLBP. Packet missing in HSRP, VRRP and GLBP can also be shown through graph.

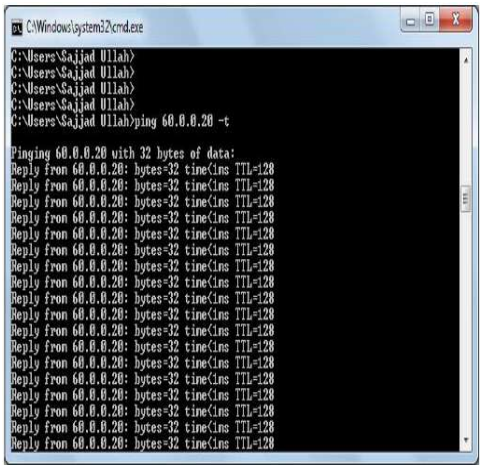

Figure 12: Packet missing in GLBP

5. CONCLUSIONS

Proficiencies and Constraints of First Hop Redundancy Protocol (FHRP).

Proficiencies

- The earliest First Hop Redundancy Protocol (FHRP).
- Provides backup to the network.
- Successful transmission from source to destination.

Constraints

- Does not provide the load balancing facility.
- It is Cisco propriety so works on only Cisco devices.
- Packet loss is more as compared to the other two.
- To enable the preemption it is to be configured manually every time.

REFERENCES

[1] Arregoces, Mauricio, and Maurizio Portolani. Data center fundamentals. Cisco Press, 2003.

[2] Long, James. Storage Networking Protocol Fundamentals. Pearson Education India, 2006.

[3] Hucaby, David. CCNP BCMSN exam certification guide: CCNP self-study. Cisco Press, 2004.

[4] Menga, Justin. CCNP practical studies: switching. Cisco Press, 2003.

[5] Membrey, Peter, Eelco Plugge, and David Hows. Practical Load Balancing: Ride the Performance Tiger. Apress, 2012..

[6] Odom, Ccie Routing And Switching Exam Certi cation Guide, 4/E. Cisco press, 2004.

[7] Kenyon, Tony. Data networks: routing, security, and performance optimization. Digital Press, 2002.

[8] R. Froom, B. Sivasubramanian, and E. Frahim, Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide. Cisco press.

[9] A. Cockburn, Writing Effective Use Cases. Pearson Education, 2001.

[10] Popovic, Miroslav. Communication protocol engineering. CRC press, 2016.

[11] S. Tim, Cisco Telepresence Fundamentals. Pearson Education India, 2010.

[12] Tate, Jon, et al. IBM Flex System and PureFlex System Network Implementation. IBM, International Technical Support Organization, 2013.

[13] P. Boger, BCMSN Exam Cram 2. Que Publishing, 2003.

[14] E. S. D, CCNP BCMSN Portable Command Guide. Cisco press.

[15] F. Dad et al., "Optimal Path Selection Using Dijkstra's Algorithm in Cluster-based LEACH Protocol," Journal of Applied Environmental and Biological Sciences, vol. 7, no. 2, pp. 194–198, Feb. 2017.

[16] Z. U. Rahman et al., "Investıgatıng the Pakıstan's Offshore Software Industry Infrastructure," Journal of Applied Environmental and Biological Sciences, vol. 7, no. 3, pp. 237–243, Mar. 2017

[17] Z. U. Rahman et al., "Magnetic Resonance Images Classification through Relevance Vector Machine," Journal of Applied Environmental and Biological Sciences, vol. 7, no. 1, pp. 213–217, Jan. 2017