Journal of Ubiquitous Systems & Pervasive Networks
Volume 19, No. 1 (2023) pp. 15-23

Performance Analysis and Functionality Comparison of First Hop Redundancy Protocol IPV6

Mahmud Mansour[a], Najia Ben Saud[b]

[a] *Department of Network, University of Tripoli, Tripoli, Libya*
[b] *Department of Network, University of Tripoli, Tripoli, Libya*

Abstract

High level of availability can be expensive to maintain, but lack of availability may also increase cost as it may damage the reputation of the business. Which led to the development of techniques that reduce downtime until it became transparent to the user.

First hop redundancy protocols (FHRP) are an essential tool for improving the availability of IP networks. The first hop redundancy protocols are protocols used to manage and maintain network default gateway routers by using one or more redundant routers that will take over in case of default router failure. Each protocol has its own purpose. FHRP was developed to reduce traffic loss. In this paper we present the first hop redundancy concept and the means for its realization in IPv6 network. We evaluate three FHRP protocols, namely, the Hot Standby Router Protocol (HSRPv2), Virtual Router Redundancy Protocol (VRRPv3), and Gateway Load Balancing (GLBP).

The First Hop Redundancy Protocols will be implemented, tested, optimized, and compared to one another in terms of convergence time, packet loss and CPU utilization, by using GNS3 simulator and Wireshark the results of comparison will be provided and analyzed. The performances of the three FHRP protocols are analyzed, and their functionalities are compared. The comparison results highlight which protocol performed the best in each scenario and which protocol can be considered as the best among the three FHRPs.

Keywords: *VRRP, FHRP, HSRP, GLBP*.

1. Introduction

In today's network, availability has become a major issue for corporations and businesses. Each minute of outage could cause a company hundred, if not thousands of dollarsThe availability can be expressed as a percent uptime per year, month, week, day, or hour compared to the total time in that period [1]. Service providers will typically include a specified network availability level in a service level agreement (SLA) [2]. To minimize outages, we aim to increase the network uptime by using redundant links and nodes. Although redundancy is good it is costly too, and there is no single way of achieving optimal network availability, it depends on the customer business' needs and how much it can tolerate the network downtime [3].

2. Availability

Availability refers to the amount of time a network is available to users and is often a critical goal for network design customers. The availability can be expressed as a percent uptime per year, month, week, day, or hour, compared to the total time in that period. Availability is linked to reliability but has a more specific meaning (percent uptime) than reliability. Reliability refers to a variety of issues, including accuracy, error rates, stability, and the amount of time between failures [3].

2.1 Measuring Availability

Network availability is measured as the percentage of time a system stays fully operational over a period of time, usually

* Corresponding author. Tel.: ++447542876286
E-mail: mah.mansour@uot.edu.ly

DOI: 10.5383/JUSPN.19.01.002

over a year. Service providers will typically include a specified level of network availability in a service level agreement (SLA).

Availability is also associated with resiliency, which is a word that is becoming more popular in the networking field. Resiliency means how much stress a network can handle and how quickly the network can rebound from problems including security breaches, natural and unnatural disasters, human error, and catastrophic software or hardware failures. A network that has good resiliency usually has good availability [2].

To calculate theoretical availability, the network is divided into each dependent unit, such as hardware, software, physical connections, power supplies etc. For most equipment, the manufacturer will supply information on availability expectations, often described as Mean Time Between Failure (MTBF).

For those parts of the network not having this data, such as a power source, statistical data and estimations have to be used. The expected time to repair each part of the network has to be estimated. This is normally referred to as Mean Time to Repair (MTTR). The availability for each unit is calculated by:

$$Availability = \frac{MTBF}{MTBF + MTTR}$$

The total availability for the network is then determined by combining the availability of the individual components. Theoretically, the availability of a redundant network should be higher than a serially connected one. However, the time taken to fail-over to the standby device should also be considered in the redundancy calculations [2].

Network redundancy is a procedure that involves including additional instances of network devices and equipment in a network as a way of ensuring network availability in the event that a network device or network path fails. Redundancy can be implemented at layer 2 using spanning tree protocol but this paper looks at redundancy options at the network layer using first hop redundancy protocol.

2.2 Cost of Network Downtime

Network downtime occurs when this digital network shuts down or becomes unavailable for use. Downtime can be either planned or unplanned.

Many organizations do not fully understand the impact of downtime on their business. Calculating the cost of this impact can be difficult because it requires an understanding of both tangible and intangible losses. Tangible losses are quantifiable, hard costs; they include lost revenue, the cost to recover lost information, disaster recovery, and business continuity costs. Intangible costs include damage to your company's reputation, lost customers, and employee productivity costs. In many ways, the damage associated with intangible costs can have a greater long-term impact on an organization than that of tangible costs.

In 2020, the information Technology intelligence consulting (ITIC) study showed Fig. 1. that since 2016 the average cost of downtime that lasts 1 hour has risen by 30%. In summary, 1,000 companies answered the poll questions, and the results were as follows [4].

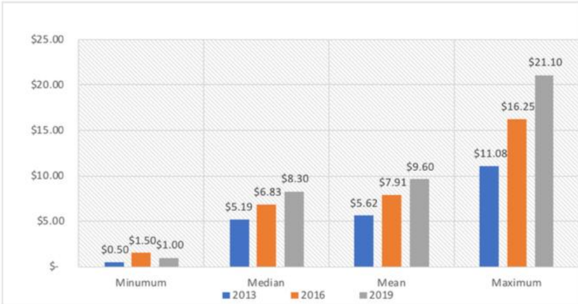

Fig. 1. ITIC Average Cost

More than 30% of the enterprises claimed that they spend from $1 to 5 million on 1 hour of downtime. Meanwhile, over $300,000 is the value of 1 hour of downtime for nearly 80% of organizations. Finally, 98% reported that 1 hour of downtime costs them almost $100,000 [5].

3. Related Work

Research [6] by Najia et (2023), compares and evaluates three different FHRPs in both IPv4 and IPv6 networks. From the result it could be seen that GLBP has performed the best for IPv4 and also IPv6. In IPv4, HSRP with optimized timers archived few numbers of packet loss but the cost was higher CPU consumption, n IPv6 VRRPv3 has the ability to switch fast during failures, thus convergence time and packet loss can be reduced.

In a previous study [7], M. Mansour, et al (2021) investigate the impact of Packet loss, CPU utilization, convergence time. It is clear to see from the result that GLBP has higher performance than HSRP and VRRP.

Research [8] conducted by Imelda et al (2020) which evaluates the three FHRP protocols, namely VRRP, HSRP, and GLBP and tests using parameters throughput, delay, packet loss, and downtime. But it is using one routing protocol that is EIGRP.

In a previous study [9], M. Mansour (2020) investigate the impact of convergence time, CPU utilization, Bandwidth consumption, Traffic flow. GLBP has higher performance than HSRP and VRRP. Also, the load balancing futures all make GLBP an efficient and reliable protocol used for redundancy and providing more availability to the network.

Besides, research [4] conducted by A. Zemtsov. (2019) investigate the impact of several factors such as convergence time, CPU utilization, Bandwidth consumption.

In addition, another paper [10] study by Usman et al (2019) investigates the impact of the bandwidth usage, CPU utilization and convergence time were measured.

Another study [11] by Rahman et al. (2017) where this study was conducted to evaluate the performance of HSRP, VRRP, and GLBP with only one parameter, namely packet loss.

Our study focused on the essential points which were packet loss, convergence time and CPU utilisation. Most of the studies performed were done in relation to IPv4, except for one study, research 6, which applied the newer IPv6. That study, however, only provided a comparison between IPv4 and IPv6.

The reason we chose to study these three protocols is because they are the more commonly applied protocols across companies, and knowing the difference between them helps in better application, which reduces network downtime.

4. First Hop Redundancy Protocols

First Hop Redundancy Protocol (FHRP) is a hop redundancy protocol designed to provide redundancy to the gateway router within the organization's network using a virtual IP address and virtual MAC address [12]. The virtual IP address will be the default gateway IP address for all the devices inside the organization's network [13]. One of the solutions to this problem is the First Hop Redundancy Protocols. The three main First Hop Redundancy Protocols are: HSRP - VRRP - GLBP [4]. First hop redundancy protocols such as HSRP and VRRP provide default gateway redundancy by one router acting as the active gateway router with one or more other routers are held in standby mode. While others like GLBP enables all available gateway routers to load share and be active at the same time [14][15].

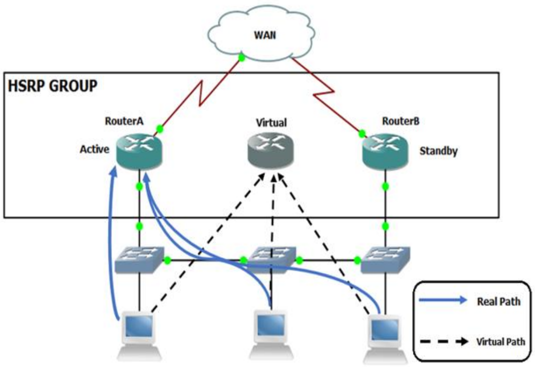

Fig. 2. HSRP Operation

4.1. Hot Standby Routing Protocol (HSRPv2)

HSRPv6 is Cisco proprietary FHRP, HSRP provides the same functionality, but it runs in an IPv6 environment. HSRPv2 hosts learn about IPv6 routers availability via IPv6 neighbor discovery route advertisement (RA) messages. These are either multicast periodically or solicited by hosts [16]. HSRP is designed to provide only a virtual first hop for IPv6 hosts.

HSRP virtual MAC address is derived from HSRP IPv6 group number, its virtual IPv6 link-local address is derived from the HSRP virtual MAC address. When HSRP group is active, it will send periodic router advertisement (RA) for the HSRP virtual IPv6 link-local addresses. HSRP uses a priority mechanism to determine which HSRP configured router is to be the default active router. HSRP router with the highest priority becomes the active router, the default priority is 100 [16]. By default, the active and standby routers HSRP sent hello messages once every 3 seconds group hello packets to the multicast address. If no hello message is received from the active router after 10 seconds, then the backup router becomes active. These timers are tunable and are tuned to obtain minimum convergence, thereby making a network highly available. However, to avoid unnecessary increase in CPU usage and standby state changes, we avoid setting the hello timer to 1 second or less, thus, keeping the timer set to 4 seconds or less.

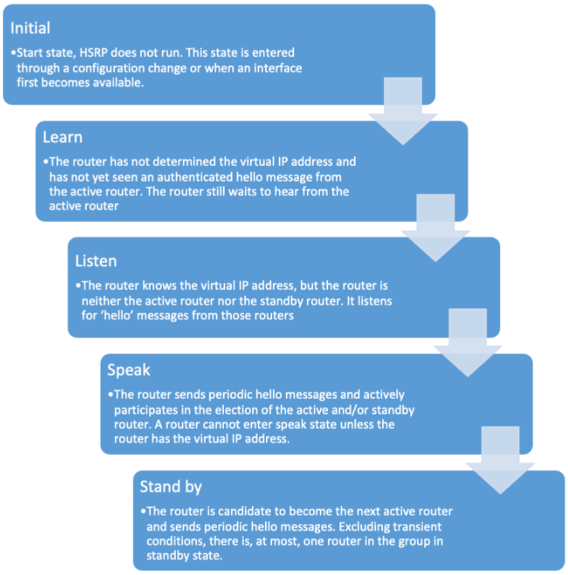

Fig. 3. HSRP Status

The HSRP operation process goes through numerous stages, starting with Initial status, where HSRP is not running and is only entered when a configuration update is made or when an interface first becomes operational, followed by Learn status; the router is still waiting to hear from the active router as it has not yet determined the virtual IP address or seen an authenticated Hello message from it, then Listen state, the router knows the virtual IP address, but the router is neither the active router nor the standby router, it just listens for 'Hello' messages from those routers, next Speak state, the router sends periodic Hello messages and actively participates in the election of the active and/or standby router, a router cannot enter speak state unless the router has the virtual IP address, in case the router considered as standby router it will operate at Stand by state, the router is candidate to become the next active router and sends periodic hello messages, excluding transient conditions, there is, at most, one router in the group in standby state.

4.2 Virtual Router Redundancy Protocol (VRRPv3)

Virtual Router Redundancy Protocol (VRRP) is an open standard redundancy protocol for establishing a fault-tolerant default gateway without changing the IP address or MAC [17]. VRRPv3 for IPv6 requires a primary virtual link-local IPv6 address configured to allow the group to operate. VRRP adds a group of routers that can act as network gateways that enable the traffic to pass through them. It uses the IPv6 multicast address of FF02::12 that is used to send hello messages. Routers in the VRRP group elect a master through the VRRP election mechanism to act as a gateway. Routers in a VRRP group determine their roles by priority [18]. VRRP version 3

(VRRPv3) introduces IPv6 address support for both standard VRRP and VRRP enhanced (VRRP-E) [18].

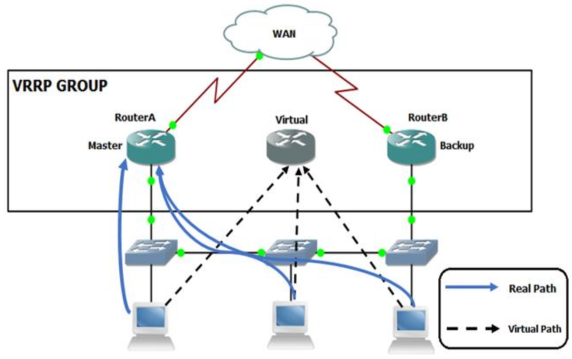

Fig. 4. VRRP Operation

There are three states defined by VRRP, initialize, master and backup, in initialize state the router waits for a startup event, routers in backup state monitors the state of the master router and router in master state forward packets for its virtual router MAC address. Respond to ARP requests for its virtual router IP addresses.

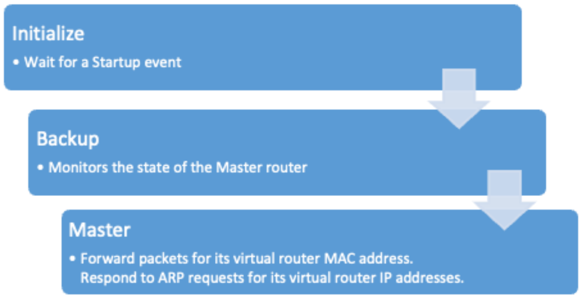

Fig. 5. VRRP Status

4.3 GLBP

GLBP performs a similar function as HSRP for the user. HSRP allows multiple routers to participate in a virtual router group configured with a virtual IPv6 address. One member is elected to be the active router to forward packets sent to the virtual IPv6 address for the group. The other routers in the group are redundant until the active router fails. The advantage of GLBP is that it additionally provides load balancing over multiple routers (gateways) using a single virtual IPv6 address and multiple virtual MAC addresses. The forwarding load is shared among all routers in a GLBP group rather than being handled by a single router while the other routers stand idle. Each host is configured with the same virtual IPv6 address, and all routers in the virtual router group participate in forwarding packets [19]. Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG in the event of the AVG becoming unavailable. The function of the AVG is that it assigns a virtual MAC address to each member of the GLBP group. Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as active virtual forwarders (AVFs) for their virtual MAC address. The AVG is also responsible for answering Address Resolution Protocol (ARP) requests for the virtual IPv6 address. Load sharing is achieved by the AVG replying to the ARP requests with different virtual MAC addresses.

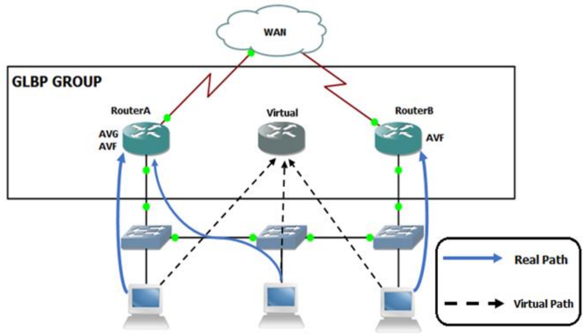

Fig. 6. GLBP Operation

The default timers in GLBP are similar to HSRP and tunable too. The hello time default value 3 seconds. While the Hold time default value 10 seconds. Tuning is used to obtain minimum convergence and therefore making a network highly available [19]. GLBP states are not the same for both AVG and AVFs, for AVG, the possible states are Disabled, Initial, Listen, Speak, Standby and Active, however for AVFs the possible states are Disabled, Initial, Listen and Active.

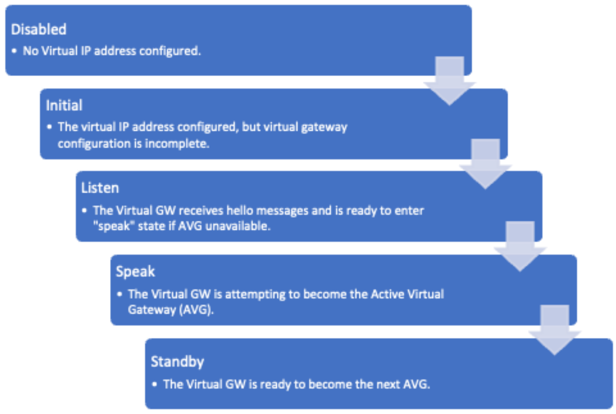

Fig. 7. GLBP States

5. Simulation and Configuration

The main objective of this paper is to implement different First Hop Redundancy Protocols on three sites and compare the performance of each one. GNS3 is a cross-platform graphical network simulator that runs on Windows, OS X, and Linux, it allows the combination of virtual and real devices, and is used to simulate complex networks without having dedicated network hardware such as routers and switches [20].

5.1 Network Design

The design used is a hierarchical design where each enterprise has two core layer routers and two access layer switches with partial mesh network topology to eliminate single points of failure in the enterprise network. The design, as shown in Fig. 1, consists of three enterprises, each of them is connected to two ISP to disrepute internet access to the enterprises, each enterprise consists of two routers inside that connect the internal network to the internet and two switches that provide layer 2 connectivity. For the network to work and provide connectivity between the network nodes with fast convergence time OSPFv6 routing protocol is used to forward packets between the ISPs and the enterprises [21].

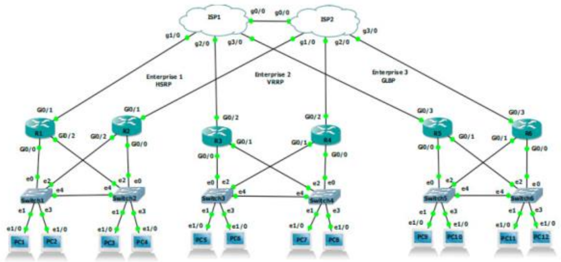

Fig. 8. Network Topology

5.2. Configuration

HSRP Hot standby router protocol is configured on the first enterprise that contains R1 and R2. The link-local address is generated by entering standby IPv6 command. A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10, and the interface identifier in the modified EUI-64 format. VRRP Virtual Router Redundancy Protocol is configured on the second enterprise that contains R3 and R4. GLBP for IPv6 Gateway Load Balancing Protocol is configured for the third enterprise that contains R5 and R6.

IP SLA is Configured on enterprise routers to check the reachability of the ISP. If the reachability goes down, it will report it back to the FHRP on the router using track object and bind it to the IP SLA when the ISP goes down. The track object will decrease the value of the priority of the router making it standby/backup while the other router becomes the active/master.

Table. 1 shows FHRP timer values before and after optimization.

Table 1. SIMULATION PARAMETER

Simulation Parameter	Value (Seconds)	
	Default	Optimized
HSRP Hello Time	3	1
HSRP Hold Time	10	3
VRRP Hello Time	1	0.5
VRRP Hold Time	3	1.656
GLBP Hello Time	3	1
GLBP Hold Time	10	3

6. Results

This section will present and discuss the measurements taken in order to measure the performance of FHRPv6 and provide and analyze the results of each FHRPv6 then compare them.

6.1. HSRPv2

6.1.1. Convergence Time and Packet loss

As seen on the diagram in Fig.9, the time taken for the router to detect ISP-1 interface going down is 6.177 seconds, making R2 an active router. During this time there are 4 ICMP packets lost. Following optimization Fig.10 shows that after timer's optimization number of packet loss has decreased because the hello packet timer and hold package time changed frequency from every 3 and 10 seconds to 1 and 3 seconds. Compared to the HSRP without optimization, the time taken for the router to detect the ISP-1 interface going down is 2.94 seconds, making R2 become an active router. During this time there are 2 ICMP packets lost. This provides much better convergence time than the results from HSRP without Optimizing timers.

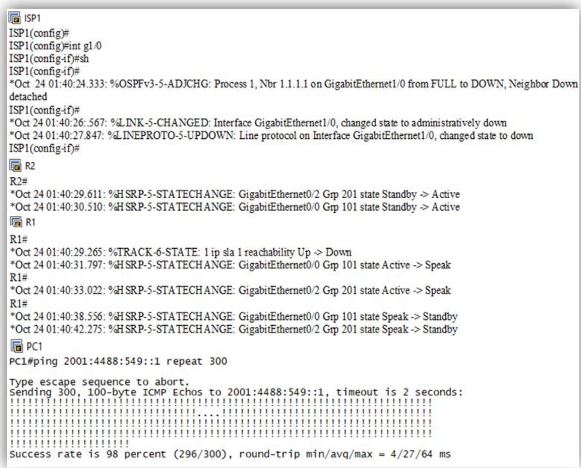

Fig.9. HSRP convergence Time without Optimization

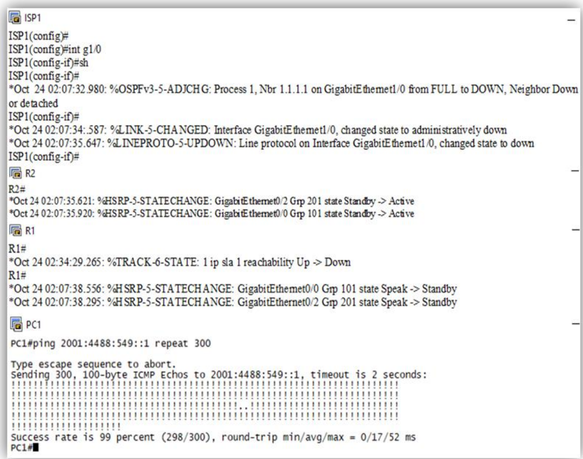

Fig. 10. HSRP convergence Time with Optimization

6.1.2 CPU Utilization

Without timers' optimization, HSRPv2 average CPU consumption is equal to 24.5%.

With timers' optimization, average CPU consumption is equal to 29%.

6.1.3 Hello Packet Consumption

Fig.11 shows the bandwidth consumption of HSRP hello packets in packets/sec over time.

We note that in the figure below the maximum consumption for HSRP hello packet is 4 packets/sec. for this reason HSRP without Optimization does not require to consume high bandwidth ، because it sends the hello packet every 3 seconds.

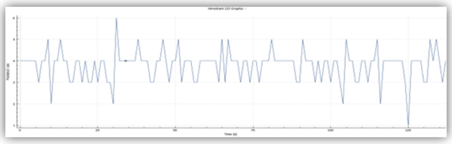

Fig. 11. HSRP Hello Packet Consumption without Optimization

After timer's optimization we notice in the following Fig.12 that the maximum consumption for HSRP hello packet reached is 6 packets/sec. In this case, HSRP with optimization needs to consume high bandwidth, because we reduced the hello packets to every 1 second and hold time every 3 second.

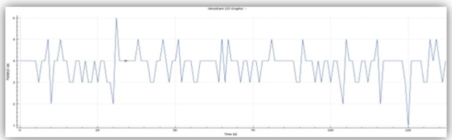

Fig. 12. HSRP Hello Packet Consumption with Optimization

6.2 VRRPv3

6.2.1 Convergence Time and Packet loss

VRRP took 2.392 m/s to converge from the time ISP-1 detects interface down at 09:55:19.946 till the state update of R4 that took over as the master router for the two VRRP groups at 09:55:22.338 as shown in Fig.13. For the hello Packet, the VRRP without Optimization does not need to consume too much bandwidth, because it sends the hello packet every 1000 msec.

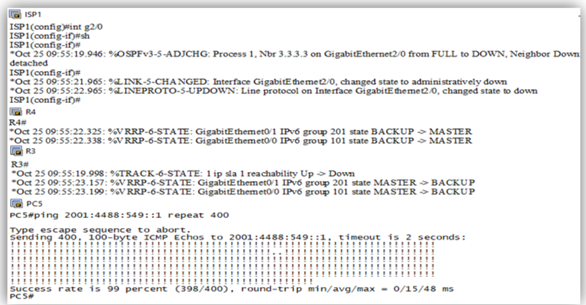

Fig. 13. VRRP Convergence without Optimization

After Optimizing the advertisement interval time in VRRP by changing the advertisement interval to 500 msec. VRRP took 1.801 milliseconds to converge from the time ISP-1 detects interface down at 11:10:9.200 till the state update of R4 that took over as the master router for the two VRRP groups at 11:10:11.001 as shown in Fig.14. During the convergence process, 1 ICMP packet was lost.

6.2.2 CPU Utilization

VRRPv3 average CPU consumption is equal to 37%.

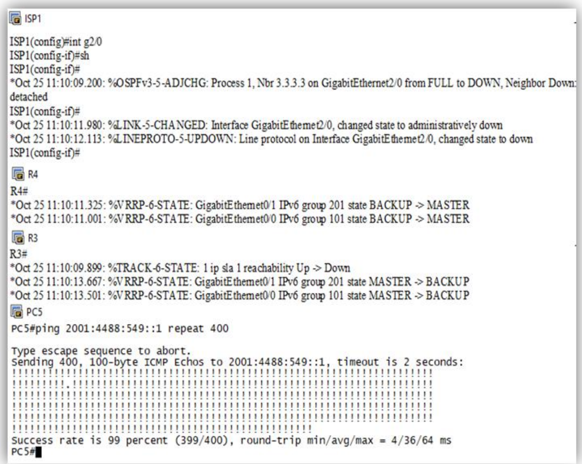

Fig. 14. VRRP Convergence with Optimization

6.2.3 Hello Packet Consumption

Fig.15 shows bandwidth consumption of VRRP hello packets in packets/sec over time.
We notice in the diagram below that maximum consumption for VRRP hello packets is 4 packets/sec. Therefore, VRRP without Optimization does not need to consume high bandwidth ، because it sends the hello packet every 1000 m/s.

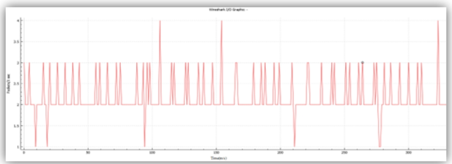

Fig. 15. VRRP Hello Packet Consumption without Optimization

Fig.16 shows bandwidth consumption of VRRP hello packets in packets/sec over time.
We note that in the figure below the maximum consumption for VRRP hello packet reached is 8 packets/sec. for this reason VRRP with Optimization will require to consume high bandwidth because we reduced the hello packet every 500 m/s.

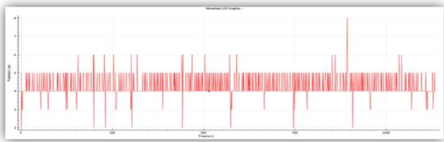

Fig. 16. VRRP Hello Packet Consumption with Optimization

6.3. GLBP

6.3.1 Convergence Time and Packet loss

GLBP convergence time without hello and hold timers' optimization is equal to 41 seconds, meanwhile 7 ICMP packets were lost, as shown in Fig. 17, the hello packet for the GLBP without Optimization does not require to consume high bandwidth, because it sends the hello packet every 3 seconds and hold time every 10 seconds. After optimizing the hello and hold timers in GLBP by changing the Hello packet time to 1 second and the hold packet time to 3 seconds.

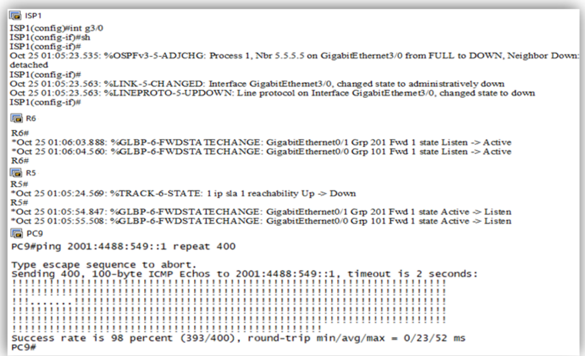

Fig. 17. GLBP Convergence without Optimization

GLBP took 2.044 seconds to converge from the time ISP-1 detects interface down at 23:21:04.831 until the state update of R6 that took over as the active router for the two GLBP groups at 23:21:06.875 as shown in Fig.18. This provides much better convergence time than the results from GLBP without optimizing timers.

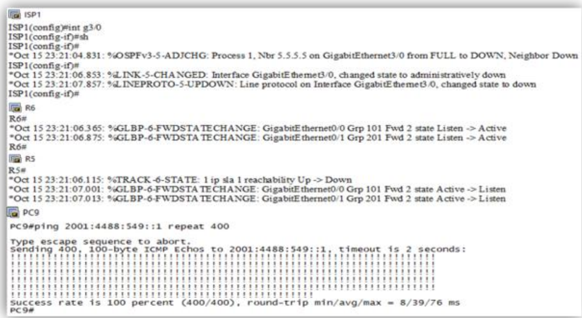

Fig. 18. GLBP Convergence with Optimization

During the convergence process, 0 ICMP packet loss as shown in Fig.18, after optimizing the hello and hold times in GLBP this will require to consume high bandwidth, because we reduced the hello packet to every 1 second and hold time every 3 seconds.

6.3.2 CPU Utilization

Without timers' optimization, GLBP average CPU consumption is equal to 25.5% of CPU usage.
With timers' optimization, HSRPv2 average CPU consumption is equal to 25% of CPU usage.

6.3.3 Hello Packet Consumption

Fig.19 shows bandwidth consumption of GLBP hello packets in packets/sec over time. We notice in the following figure that the longest time for GLBP hello packets is 3 packets/sec. For this reason, GLBP without Optimization does not require to consume high bandwidth, because it sends the hello packet every 3 seconds and hold time every 10 seconds.

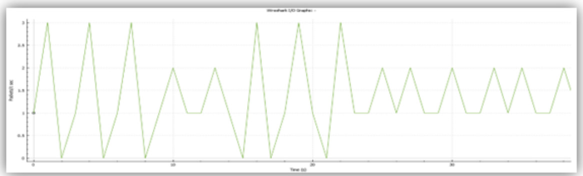

Fig. 19. GLBP Hello Packet Consumption without Optimization

After timer's optimization we note that in the figure below the longest time for GLBP hello packet reached is 39 packets/sec as shown in Fig.20, for this reason GLBP with Optimization will require to consume high bandwidth, because we reduced the hello packet to every 1 seconds and hold time every 3 sec.

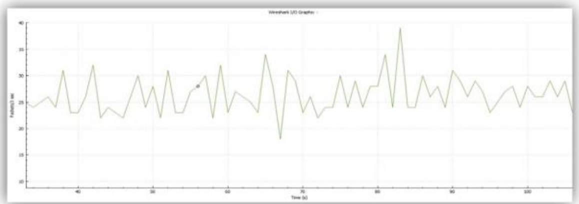

Fig. 20. GLBP Hello Packet Consumption with Optimization

7. Comparison

7.1 Convergence Time

Fig. 21 shows a convergence time comparison in seconds between FHRPv6. We can see from the following diagram that VRRP has the best convergence time of 1.801 s when optimized. This is because the VRRP Protocol sends the advertisement interval time in milliseconds, not seconds. For VRRP3, the advantage gained from using VRRP3 is that there's a faster switch over to back up routers than can be obtained with standard IPv6 Neighbor Discover mechanisms.

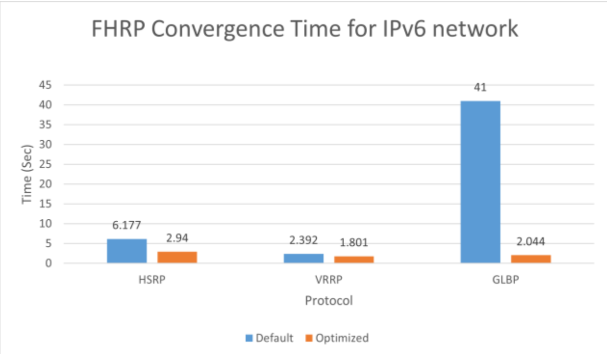

Fig. 21. FHRP Convergence Time Comparison

7.2 Packet loss

Fig.22 shows a comparison of packet loss in packets between FHRP during convergence time. GLBP has the lowest packet loss after optimization. The reason for this reduced packet loss is that the protocol uses load balancing that provides more network availability.

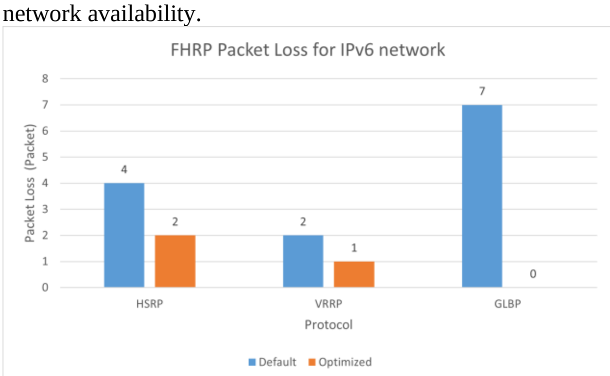

Fig. 22. FHRP Packet loss Comparison

7.3 CPU Utilization

Fig.23 shows a comparison of average percentage of CPU Utilization between FHRP.
Fig.10 illustrates that VRRP requires high CPU consumption because it sends the packet advertisement interval time every 1000msec, thus we can conclude that VRRP has the best utilization of CPU before optimization. Meanwhile GLBP has the best utilization of CPU after optimization because GLBP works on the principle of load balancing between routers, unlike HSRP and VRRP.

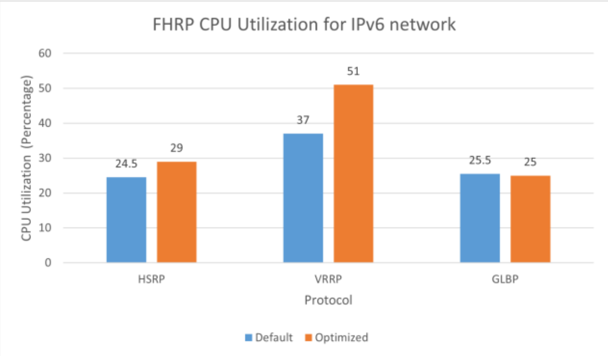

Fig. 23. FHRP CPU Utilization Comparison

7.4 Overall Performance Comparison

Following table summarize FHRP performance comparison:

Table 2. FHRP PERFORMANCE COMPARISON

FHRP	Measurement	Default	Optimized
HSRP	Convergence Time	6.177	2.94
	Packet Loss	4	2
	CPU Usage	24.5	29
VRRP	Convergence Time	2.392	1.801
	Packet Loss	2	1
	CPU Usage	37	51
GLBP	Convergence Time	41	2.044
	Packet Loss	7	0
	CPU Usage	25.5	25

Note that for the table above Convergence Time measured by seconds, Packet Loss by ICMP packet and CPU Usage as a percentage of usage.
It could be seen that GLBP after timer's optimization has the best convergence time and the lower number of packet loss among all protocols.

8. Conclusion

After implementing, optimizing, and testing different FHRP in IPv6 network, in terms of packet loss, conversion time, CPU utilization, and Hello packet consumption; the trade-off between performance and both CPU utilization and Hello packet consumption is clear.

For FHRP in IPv6 network, HSRP after optimization works well in terms of the number of packets lost, however, it requires more CPU utilization. VRRP is beneficial as it switches over faster to back up routers that can be obtained with standard IPv6 Neighbour Discover (RFC 4861) mechanisms; nevertheless, VRRP still presents with more packet loss compared to GLBP after optimization which achieved zero packet loss due to the use of load balancing in the latter protocol.

Although better results have been achieved after optimizing timers, higher bandwidth consumption is needed for Hello packet communication for all three FHRPs, GLBP had the highest consumption among all.

All the load balancing futures make GLBP an efficient and reliable protocol and provides more availability to the network. The only downside is GLBP is that it is a CISCO proprietary, so it only runs on CISCO devices.

To summarize, GLBP is a good choice in terms of performance and providing higher availability in the network as not only redundancy but also load balancing capabilities could be achieved.

References

[1] Chris Oggerino, "High Availability Network Fundamentals", Cisco Press, 1st edition, 2001.

[2] Richard Froom, "Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Foundation Learning for SWITCH

[3] Andy Sholomon, Tom Kunath, "Enterprise Network Testing", Cisco Press, 1st edition, 2011.

[4] A. Zemtsov "Performance Evaluation of First Hop Redundancy Protocols for a Computer Networks of an Industrial Enterprise" 2019 International Multi-Conference on Industrial Engineering and Modern Technologies. 1-4 Oct. 2019.

[5] R. Hinden, Ed, "Virtual Router Redundancy Protocol", Request for Comments: 3768, 2004.

[6] N. B. Saud and M. Mansour, "Performance Evaluation of First Hop Redundancy Protocols in IPv4 and IPv6 Networks," 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Benghazi, Libya, 2023, pp. 440-445, doi: 10.1109/MI-STA57575.2023.10169462.

[7] M. Mansour, A.Ghneimat, R.Alasem, F. Jarray, "Performance Analysis and Functionality Comparison of First Hop Redundancy Protocol", Journal of Ubiquitous Systems & Pervasive Networks. Volume 15, No. 1 (2021) pp. 49-58.

[8] Imelda Ristanti Julia et al, "Protocol (FHRP) on VRRP, HSRP, GLBP with Routing Protocol BGP and EIGRP", The 8th International Conference on Cyber and IT Service Management (CITSM 2020) On Virtual, October 23-24, 2020.

[9] M. Mansour "Performance Evaluation of First Hop Redundancy Protocols", The 11th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2020) November 2-5, 2020, Madeira, Portugal.

[10] Usman Anwar, Jing Teng; Hafiz Ahmad Umair; Ammar Sikander "Performance Analysis and Functionality Comparison of FHRP Protocols" IEEE 11th International Conference on Communication Software and Networks (ICCSN), 12-15 June 2019.

[11] Z. U. Rahman et al., "Performance Evaluation of First Hop Redundancy Protocols," J. Appl. Environ. Biol. Sci., vol. 7, no. 3, pp. 268–278, 2017.

[12] Priscilla Oppenheimer, "Top-Down Network Design", Cisco Press, 3ed edition, 2010.

[13] Rolf McClellan, Nick Lippis "Network-Level Redundancy/Resilience for High-Availability Campus LANs"," ZDTag white paper", 1999, pp6-8.

[14] Mike Miclot, John Mower, "Reducing the Risk, Cost and Frequency of Production Stoppages Using Network Redundancy", 2010.

[15] Priyanka Dubey, Shilpi Sharma, Aabha Sachdev, "Review of First Hop Redundancy Protocol and Their Functionalities", International Journal of Engineering Trends and Technology, 2013, pp 1085- 1088.

[16] T. Li, B. Cole, P. Morton, D. Li," Cisco Hot Standby Router Protocol", Request for Comments: 2281, 1998.

[17] S. Knight, D. Weaver, D. Whipple, R. Hinden, D. Mitzel, P. Hunt, P. Higginson, M. Shand, A. Lindem, "Virtual Router Redundancy Protocol", Request for Comments: 2338,1998.

[18] S. Nadas, "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", Request for Comments: 5798, 2010.

[19] Cisco Systems. "GLBP - Gateway Load Balancing Protocol."2006, [https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html]. Accessed 6 Oct. 2023.

[20] Jason C. Neumann, "The Book of GNS3", No Starch Press, 1st edition, 2015.

[21] M. Mansour, M.Agomati, M. Alsaid, M.berrish, R. Alasem, "Performance Analysis and Functionality Comparison of First Hop Redundancy Protocol IPv6", The 13th International Conference on Emerging Ubiquitous Systems and Pervasive Networks, October 26-28, 2022.