

Performance Analysis and Functionality Comparison of First Hop Redundancy Protocols

M. Mansour^a, A. Ghneimat^b, R. Alasem^c, F. Jarray^d *

^aDepartment of Network, University of Tripoli, Tripoli, Libya

^bPrince Sattam Ibn Abdulaziz University. Saudi Arabia

^cAl albayt University- Jordan

^dHigher institute of computer science, Medenine, Tunisia

Abstract

High levels of availability can be expensive to maintain, but a lack of availability may also increase costs as it may damage the reputation of the business. This has led to the development of techniques that reduce downtime until it became transparent to the user.

First hop redundancy protocols are an essential tool for improving the availability of IP networks. First hop redundancy protocols are protocols used to manage and maintain network default gateway router by using one or more redundant routers that will take over in case of default router failure. In this paper, we evaluate the three particular protocols of FHRPs, namely the Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing (GLBP) using GNS3 tools.

The First Hop Redundancy Protocols have been implemented, tested, optimized, and compared to one another in terms of convergence time, packet loss and CPU utilization. The comparison indicates which protocol is best in which scenario and which is best among the three protocols.

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

1. Introduction

The rapidly developing communication technology has led to an increase in demand for applications and high-speed networks. In today's network, availability became a major issue for corporations and businesses.

Each minute of outage could cost a company hundreds, if not thousands, of dollars. In order to minimize outages, we try to increase the uptime of the network by using redundant links and nodes. Although redundancy is good it is costly too. Additionally, there is no single way of achieving optimal availability for network, as it depends on the customer business needs and how much downtime of the network can be tolerated.

Availability can be measured according to factors such as almost 100% of operationality and zero points of failure. The most challenging standard of availability of a network is known as the five 9s (99.999%).

Availability also can be expressed as a percent uptime per year, month, week, day, or hour, compared to the total time in that period [1].

2. Availability

Normally the availability is expressed as the percentage of the time the network is working. It was from there the term "five-nines" came into use. Five-nines refer to the percentage 99.999%, which is a generalization that has for long been used for marketing and has been viewed as the desired goal for availability in many networks, at least at the core-level. Five-nines correspond to 5 minutes of downtime a year [2].

Table 1. Availability percentage in minutes

Nines	% Available	Downtime per year	Downtime per month	Downtime per week
One nine	90%	36.5 days	72 hours	16.8 hours
Two nines	99%	3.65 days	7.20 hours	1.68 hours
Three nines	99.9%	8.76 hours	43.2 minutes	10.1 minutes
Four nines	99.99%	52.56 minutes	4.32 minutes	1.01 minutes
Five nines	99.999%	5.26 minutes	25.9 seconds	6.05 seconds
Six nines	99.9999%	31.5 seconds	2.59 seconds	0.605 seconds

* Corresponding author. Tel.: +447542876286

E-mail: mansour30@hotmail.com

© 2011 International Association for Sharing Knowledge and Sustainability.

DOI: 10.5383/JUSPN.15.01.007

Availability is linked to reliability but has a more specific definition (percent uptime) than reliability. Reliability refers to a variety of issues, including accuracy, error rates, stability, and the amount of time between failures [3]. To calculate a 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:

$$Availability = \frac{MTBF}{MTBF + MTTR} \quad (1)$$

The total availability for the network is then determined by combining the availabilities 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.

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.

2.1. Cost of Network Downtime

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, cost of recovering 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.

According to Gartner Research, the losses associated with network downtime include:

- Productivity losses
- Revenue losses
- Damaged reputation
- Impaired financial performance

According to a July 2009 white paper titled "Navigating Network Infrastructure Expenditures during Business Transformations," written by Lippis Consulting, the cost of network downtime for a financial firm's brokerage service was calculated to be \$7.8 million per hour. A one-hour outage for a financial firm's credit card operation can cost upwards of \$3.1 million. A media firm could lose money on pay-per-view

revenues, an airline company in ticket sales, and a retail company in catalog sales [20].

3. Related Work

In a previous study [17], M. Mansour (2020) under the title "Performance Evaluation of First Hop Redundancy Protocols" investigate the impact of several factors such as convergence time, CPU utilization, Bandwidth consumption, Traffic flow.

In a previous study [15] T. Shakshuki, et al (2019) under the title "Performance Comparison of First Hop Redundancy Protocol", investigate the impact of several factors such as convergence time, CPU utilization, Bandwidth consumption.

In addition, another paper [16] study by Usman et al (2019) entitled "Performance Analysis and Functionality Comparison of FHRP Protocols" investigate the impact of the bandwidth usage, CPU utilization and convergence time were measured.

Besides, research [14] conducted by A. Zemtsov. (2019) entitled "Performance Evaluation of First Hop Redundancy Protocols for a Computer Networks of an Industrial Enterprise".

Research [19] conducted by Imelda et al (2020) with the title "Performance Analysis of VRRP, HSRP, and GLBP with EIGRP Routing Protocol" 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.

Another study [18] by Rahman et al. (2017) titled "Performance Evaluation of First Hop Redundancy Protocols (HSRP, VRRP & GLBP)" where this study was conducted to evaluate the performance of HSRP, VRRP, and GLBP with only one parameter, namely packet loss.

4. First Hop Redundancy Protocols

First, Hop Redundancy Protocol (FHRP) is a group of protocols that allow a router on a network to automatically take over if a primary default gateway router fails. The devices on a 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 will terminate [2]. One of the solutions to this problem is First Hop Redundancy Protocols. The three main First Hop Redundancy Protocols are HSRP - VRRP – GLBP [14].

- Hot Standby Router Protocol (HSRP; Cisco Proprietary)
- Virtual Router Redundancy Protocol (VRRP; Open Standard)
- Gateway Load Balancing Protocol (GLBP; Cisco Proprietary).

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. While others, like GLBP, enable all available gateway routers to load share and be active at the same time [4].

4.1. Hot Standby Routing Protocol

Hot Standby Routing Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway. The Hot Standby Redundancy Protocol (HSRP) supports two versions.

4.1.1 Hot Standby Routing Protocol operation

HSRP provides a set of routers work in concert to present the illusion of a single virtual router to the hosts on the LAN. This set is known as an HSRP group or a standby group. A single router elected from the group is responsible for forwarding the packets that hosts send to the virtual router. This router is known as the active router while another router is elected as the standby router. In the event that the active router fails, the standby assumes the packet forwarding duties of the active router. This process is transparent to users. Although an arbitrary number of routers may run HSRP, only the active router forwards the packets sent to the virtual router. Devices in an HSRP group select the active router based on device priorities [7].

To minimize network traffic, only the active and the standby routers send periodic HSRP messages once the protocol has completed the election process [9].

Multiple hot standby groups may coexist and overlap. Each standby group emulates a single virtual router. For each standby group, a single well-known virtual MAC and IP address are allocated. The IP address should belong to the primary subnet in use on the LAN but must differ from the addresses allocated as interface addresses on all routers and hosts on the LAN, including virtual IP addresses assigned to other HSRP groups. If multiple groups are used on a single LAN, load splitting can be achieved by distributing hosts among different standby groups. In the case of multiple groups, each group operates independently of other groups and individual routers that participate in multiple groups maintains separate state and timers for each group [8].

4.2. Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) is an open standard redundancy protocol for establishing a fault-tolerant default gateway. VRRP is a protocol that provides redundancy to routers within a LAN. It provides an alternate route path for hosts without changing the IP address or MAC that the host knows. VRRP follows the same concept of cisco's HSRP with some differences [11].

4.2.1 VRRP Operation

VRRP provides a set of routers work in concert to present the illusion of a single virtual router to the hosts on the LAN. This set is known as a VRRP group. A single router elected from the group is responsible for forwarding the packets that hosts send to the virtual router. This router is known as the 'Master' router while another router is elected as the 'Backup' router. In the event that the master router fails, the backup assumes the packet forwarding duties of the master router. This process is

transparent to users. Although an arbitrary number of routers may run VRRP, only the master router forwards the packets sent to the virtual router. Devices in a VRRP group select the master based on device priorities [6] [4]. The master periodically sends VRRP Advertisement packets to all backups in the VRRP group to advertise its configuration and running status [5].

4.3. Gateway Load Balancing Protocol

Gateway Load Balancing Protocol (GLBP) is a Cisco proprietary protocol that attempts to overcome the limitations of existing redundant router protocols by adding basic load balancing functionality.

GLBP provides load balancing over multiple routers (gateways) using a single virtual IP address and multiple virtual MAC addresses. Each host is configured with the same virtual IP address, and all routers in the virtual router group participate in forwarding packets [9].

4.3.1 GLBP Operation

GLBP works by making use of a single virtual IP address, which is configured as the default gateway on the hosts. When the routers are configured to a GLBP group, they first elect one gateway to be the Active Virtual Gateway (AVG) for that group. The election is based on the priority of each gateway (highest priority wins). If all of them have the same priority, then the gateway with the highest real IP address becomes the AVG [12]. A GLBP group only has a maximum of four AVFs. If there are more than 4 gateways in a GLBP group, then the rest will become Standby Virtual Forwarder (SVF) which will take the place of an AVF in the case of failure [12].

5. Simulation and Results

This paper focuses on implementing first hop redundancy protocols in a network to increase the availability and reduce network downtime. The main objective is to implement different First hop redundancy protocols on three sites and compare the performance of each one. Each site connects to two different ISP to provide high availability, and if one of the links fails the other will take over, this will provide a way to minimize network downtime, which is one of the most important goals of corporations in today's network.

5.1 Simulation Tool

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 [13].

In GNS3 VPCS can provide Traffic Flow by using ICMP, TCP or UDP data flow. Simulating network fails IP Service Level Agreements (SLA) will be using and track object to help with failover process. IP SLAs is a network performance measurement and diagnostics tool that uses active monitoring. It is beneficial in the sense that it checks the reachability of a specific IP address and reports it back. Finally, results obtained are analyzed using Wireshark.

5.2 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 in order to eliminate single points of failure in the enterprise network.

The design consists of three enterprises (Tripoli, Sabha, and Benghazi), each of which is connected to two ISP to disrepute internet access to the enterprises. Each enterprise consists of two routers inside that connect internal network to the internet and two switches that provide layer 2 connectivity as shown in Fig. 1. In order for the network to work and provide connectivity between the network nodes with fast convergence time, EIGRP routing protocol is used to forward packets between the ISPs and the enterprises.

Each router has to track an object that is used to verify connection to ISP in case the connection goes down the track object decrements a value to the priority of active/master router which will make it have less priority than the standby/backup and it will result in making the standby/backup to become active/master router.

In the network design topology shown in Fig.1, routers on the left side in each enterprise (R1, R3, and R5) have been configured with higher priority than the routers on the right side of each enterprise.

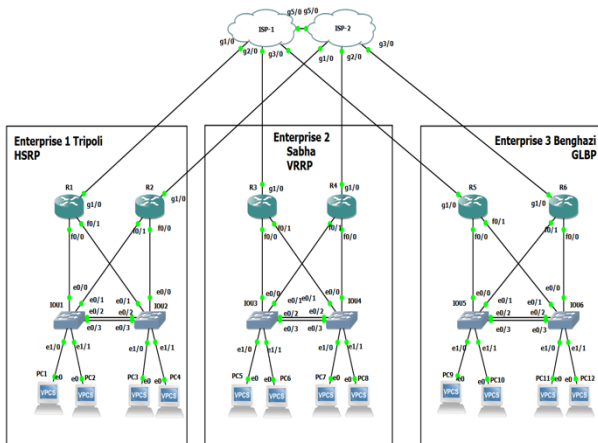


Fig. 1. Network Topology Used

5.3 Configuration

HSRP Hot standby router protocol is configured on the first enterprise that contains R1 and R2, the following is a sample of the configuration used to enable HSRP on the routers, the configuration needs to be the same on both routers in order to connect and exchange hello packets.

VRRP Virtual Router Redundancy Protocol is configured on the second enterprise that contains R3 and R4. The following is a sample of the configuration used to enable VRRP on routers. The configuration needs to be the same on both routers in order to connect and exchange hello packets.

Table 2. Simulation Parameters

Simulation parameter	Value
Simulator	GNS3
Number of ISP	2 ISP (ISP1- ISP2)
Number of Routers	6 Routers
Number of Switches	6 Switches
PCs Numbers	12 PCs
Traffic generator	Constant bit rate
Bandwidth	2Mbps
Packet rate	10 packet per second
ISP-1	Lo0 8.8.8.8/30
ISP-2	Lo0 8.8.4.4/30
HSRP- Hello –Hold time	Without optimization 3 10 With optimization 1 3
GLBP- Hello –Hold time	Without optimization 3 10 With optimization 1 3
VRRP - Hello –Hold time	With optimization 1 3

GLBP Gateway Load Balancing Protocol is configured for the third enterprise that contains R5 and R6. The following is a sample of the configuration used to enable GLBP on routers. The configuration needs to be the same on both routers in order to connect and exchange hello packets.

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 decrement a value of the priority of the router making it do to standby/backup while the other router becomes the active/master.

6. Results

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

6.1 HSRP Result

6.1.1. Convergence Time

HSRP without Optimization

This contains the results of HSRP without the optimization of the hello and hold timers.

HSRP took 7.25 seconds to converge from the time ISP-1 detects interface down at 01:10:04.243 till the state update of R2 that took over as the active router for the two HSRP groups at 01:10:11.493 as shown in Fig. 2. During the convergence process, 4 ICMP packets were lost.

```

PC1
84 bytes from 8.8.8.8 icmp_seq=11 ttl=254 time=17.154 ms
84 bytes from 8.8.8.8 icmp_seq=12 ttl=254 time=11.898 ms
84 bytes from 8.8.8.8 icmp_seq=13 ttl=254 time=14.439 ms
8.8.8.8 icmp_seq=14 timeout
8.8.8.8 icmp_seq=15 timeout
8.8.8.8 icmp_seq=16 timeout
8.8.8.8 icmp_seq=17 timeout
84 bytes from 8.8.8.8 icmp_seq=18 ttl=253 time=27.954 ms
84 bytes from 8.8.8.8 icmp_seq=19 ttl=253 time=35.418 ms
84 bytes from 8.8.8.8 icmp_seq=20 ttl=253 time=35.991 ms
    
```

Fig. 2. HSRP Conversion without Optimization

HSRP with Optimization

This are the results after optimizing the hello and hold timers in HSRP by changing the Hello packet time to 1 second and the hold packet time to 3 seconds. Using the commands:

```

#standby 1 timers 1 3
#standby 2 timers 1 3
    
```

After optimization, HSRP took 3.271 seconds to converge from the time ISP-1 detects interface down at 01:31:12.151 until the state update of R2 that took over as the active router for the two HSRP groups at 01:31:15.422 as shown in Fig. 3. This provides much a better convergence time than the results from HSRP without optimizing timers. During the convergence process, 1 ICMP packet was lost.

```

PC1
84 bytes from 8.8.8.8 icmp_seq=202 ttl=253 time=24.767 ms
84 bytes from 8.8.8.8 icmp_seq=203 ttl=253 time=24.865 ms
84 bytes from 8.8.8.8 icmp_seq=204 ttl=253 time=22.500 ms
84 bytes from 8.8.8.8 icmp_seq=205 ttl=253 time=24.172 ms
84 bytes from 8.8.8.8 icmp_seq=206 ttl=253 time=27.962 ms
84 bytes from 8.8.8.8 icmp_seq=207 ttl=253 time=23.032 ms
8.8.8.8 icmp_seq=208 timeout
84 bytes from 8.8.8.8 icmp_seq=209 ttl=253 time=25.449 ms
    
```

Fig. 3. HSRP Conversion with Optimization

6.1.2. CPU Utilization

Before optimization, HSRP consumed an average of 0.15% of CPU usages for R1 and R2 while both routers CPU utilization at average 6%.

```

R2#sh processes cpu sorted
CPU utilization for five seconds: 6%/0%; one minute: 6%; five minutes: 6%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
262      82580      890947      92  4.55%  3.71%  3.68%  0 IP SLAs XOS Even
 3       1192        284       4197  1.03%  0.08%  0.01%  0 Exec
245       5984       8569       698  0.31%  0.16%  0.15%  0 HSRP IPv4
268       7740        733      10539  0.31%  0.25%  0.21%  0 Compute load avg
269        316        123      2569  0.23%  0.01%  0.00%  0 Per-minute Jobs
160        512      227302        2  0.23%  0.23%  0.23%  0 HSRP Common

R1#sh processes cpu sorted
CPU utilization for five seconds: 6%/100%; one minute: 7%; five minutes: 6%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
262      80708      909864      88  3.91%  4.10%  3.66%  0 IP SLAs XOS Even
239       5544      233114      23  0.23%  0.37%  0.38%  0 ISG MIB jobs Man
145       6004       5588      1074  0.23%  0.14%  0.14%  0 CEF: IPv4 proces
 83      11464      18497      587  0.15%  0.21%  0.18%  0 IP Input
245       6092       8962       679  0.15%  0.13%  0.13%  0 HSRP IPv4
112       2888      116287        24  0.15%  0.18%  0.17%  0 IPAM Manager
160        542      232165        2  0.15%  0.23%  0.23%  0 HSRP Common
    
```

Fig. 4. HSRP CPU Utilization without Optimization

After optimization, HSRP took an average of 0.32% of CPU usages for R1 and R2 due to the change of timers while both routers CPU utilization still at average 7%.

6.1.3. Hello Packet Bandwidth Consumption

Fig. 5 shows bandwidth consumption of HSRP hello packets in bytes/sec. HSRP hello packet size is 62 Byte. Fig. 6 shows the bandwidth consumption of HSRP hello packets in bytes/sec.

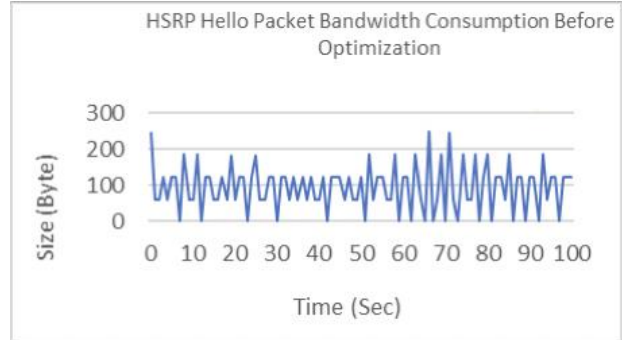


Fig. 5. HSRP Hello Packet Consumption without Optimization

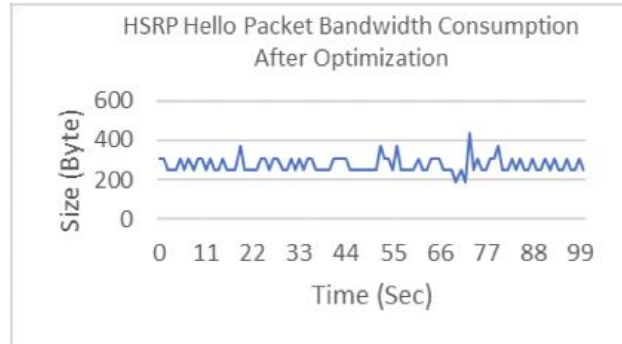


Fig. 6. HSRP Hello Packet Consumption with Optimization

6.1.4. Traffic Flow

Fig. 7. shows data traffic flow in HSRP network throw R1. This shows major drops in bandwidth after reaching 5000 byte/sec. Fig. 8. shows data traffic flow in HSRP network through R1, this shows major drops in bandwidth after reaching 5000 byte/sec.

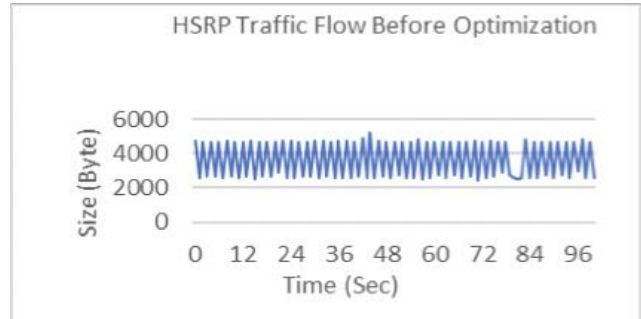


Fig. 7. HSRP Traffic Before Optimization

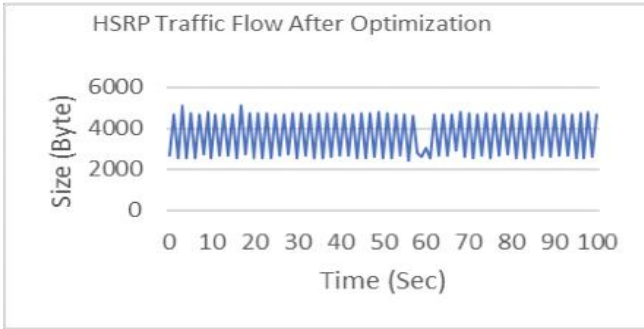


Fig. 8. HSRP Traffic After Optimization.

6.2. VRRP Result

6.2.1. Convergence Time

VRRP took 4.861 seconds to converge from the time ISP-1 detects interface down at 00:19:28.103 till the state update of R4 that took over as the master router for the two VRRP groups at 00:19:32.964 as shown in Fig. 9. During the convergence process, 3 ICMP packets lost.

```

PC#
34 bytes from 8.8.8.8 icmp_seq=14 ttl=254 time=15.536 ms
34 bytes from 8.8.8.8 icmp_seq=15 ttl=254 time=13.771 ms
34 bytes from 8.8.8.8 icmp_seq=16 ttl=254 time=13.752 ms
34 bytes from 8.8.8.8 icmp_seq=17 ttl=254 time=72.859 ms
3.8.8.8 icmp_seq=18 timeout
3.8.8.8 icmp_seq=19 timeout
3.8.8.8 icmp_seq=20 timeout
34 bytes from 8.8.8.8 icmp_seq=21 ttl=253 time=50.510 ms
34 bytes from 8.8.8.8 icmp_seq=22 ttl=253 time=34.590 ms
34 bytes from 8.8.8.8 icmp_seq=23 ttl=253 time=34.361 ms
34 bytes from 8.8.8.8 icmp_seq=24 ttl=253 time=35.083 ms
34 bytes from 8.8.8.8 icmp_seq=25 ttl=253 time=35.048 ms
34 bytes from 8.8.8.8 icmp_seq=26 ttl=253 time=35.207 ms
    
```

Fig. 9. VRRP Conversion Time

6.2.2. CPU Utilization

VRRP took an average of 0.10% of CPU usage for R3 and R4 while both routers CPU utilization at average 6% as shown in Fig. 10.

```

R4#show processes cpu sort
CPU utilization for five seconds: 7%/100%; one minute: 7%; five minutes: 6%
PID Runtime(ms)   Invoked    uSecs  5Sec  1Min   5Min  ITY Process
252      86032      1040033      82   3.19%  3.55%  3.61%  0 IP SLAs XOS Even
3         4856         637      6995  1.43%  0.63%  0.30%  0 Exec
83       30876      19914      1550  0.71%  0.61%  0.54%  0 IP Input
239      6952      265845      26   0.31%  0.36%  0.36%  0 ISG MIB Jobs Man
82       3272      132888      24   0.15%  0.16%  0.15%  0 IP ARP Retry Age
268      10352      856      12093  0.15%  0.21%  0.21%  0 Compute load avg
112      3768      132590      28   0.15%  0.16%  0.16%  0 IPAM Manager
174       764      42610      17   0.15%  0.08%  0.08%  0 RBSCP Background
2         3152         855      3686  0.07%  0.05%  0.05%  0 Load Meter
53       4620      1283      3600  0.07%  0.11%  0.08%  0 HC Counter Timer
160      7768      12445      624  0.07%  0.13%  0.13%  0 VRRP

R3#show processes cpu sort
CPU utilization for five seconds: 5%/100%; one minute: 6%; five minutes: 6%
PID Runtime(ms)   Invoked    uSecs  5Sec  1Min   5Min  ITY Process
252      88760      1046559      84   3.27%  3.66%  3.46%  0 IP SLAs XOS Even
3         1196         420      2847  0.63%  0.61%  0.23%  0 Exec
239      4876      266720      18   0.23%  0.30%  0.32%  0 ISG MIB Jobs Man
83      13336      14755      903  0.23%  0.19%  0.22%  0 IP Input
82       2836      133117      21   0.15%  0.12%  0.14%  0 IP ARP Retry Age
112      2492      133117      18   0.15%  0.18%  0.17%  0 IPAM Manager
2         3144         855      3664  0.07%  0.07%  0.07%  0 Load Meter
53       4624      1283      3600  0.07%  0.11%  0.08%  0 HC Counter Timer
160      2716      18450      147  0.07%  0.06%  0.07%  0 VRRP
189      1808      42777      329  0.07%  0.05%  0.05%  0 PER BR LEARN
    
```

Fig. 10. VRRP CPU without Utilization

6.2.3. Packet Bandwidth Consumption

Fig. 11. shows bandwidth consumption of VRRP hello packets in bytes/sec. HSRP hello packet size is 60 Byte.

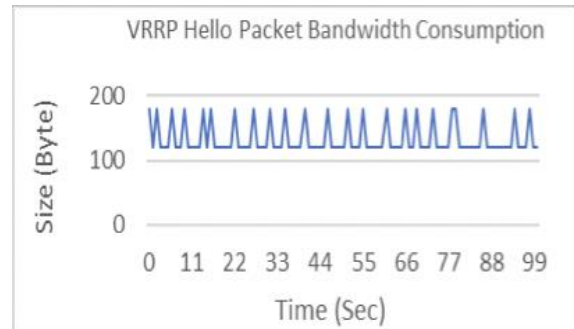


Fig. 11. VRRP Hello Packet Bandwidth Consumption

6.2.4. Traffic Flow

Fig. 12. shows data traffic flow in VRRP network throw R3. This provides similar results to that of HSRP.

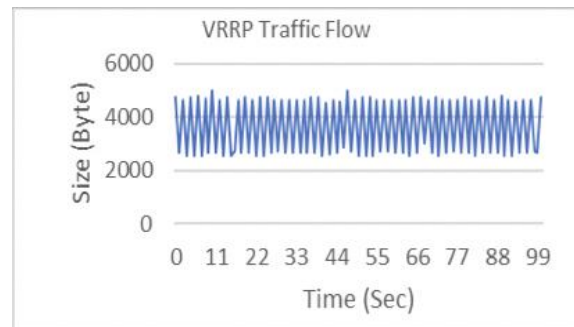


Fig. 12. VRRP Traffic Flow

6.3. GLBP Result

6.3.1. Convergence Time

GLBP without Optimization

This contains the results of GLBP without the optimization of the hello and hold timers.

Before optimization, GLBP took 39 seconds to converge from the time ISP-1 detects interface down at 02:37:26.655 until the state update of R6 that took over as the active router for the two GLBP groups at 02:38:05.607 as shown in Fig. 13. This is caused by the pre-emption delay that is set by default on the AVF and its value is 30 seconds pre-emption delay. During the convergence process, more than 10 ICMP packets were lost

```

PC3
*192.168.5.2 icmp_seq=54 ttl=255 time=11.006 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.5.2 icmp_seq=55 ttl=255 time=3.000 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.5.2 icmp_seq=56 ttl=255 time=9.271 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.5.2 icmp_seq=57 ttl=255 time=11.804 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.5.2 icmp_seq=58 ttl=255 time=10.962 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.5.2 icmp_seq=59 ttl=255 time=10.109 ms (ICMP type:3, code:1, Destination host unreachable)
84 bytes from 8.8.8.8 icmp_seq=60 ttl=253 time=31.186 ms
84 bytes from 8.8.8.8 icmp_seq=61 ttl=253 time=40.381 ms
84 bytes from 8.8.8.8 icmp_seq=62 ttl=253 time=49.729 ms
84 bytes from 8.8.8.8 icmp_seq=63 ttl=253 time=40.462 ms
    
```

Fig. 13. GLBP Conversion without Optimization

GLBP after Optimization

These are the results after optimizing the hello and hold timers in HSRP by changing the Hello packet time to 1 second and the hold packet time to 3 seconds. Using the commands:

```

#glbp 1 timers 1 3
#glbp 2 timers 1 3
And changing the AVF preemption to 0 using the commands:
#glbp 1 forwarder preempt delay minimum 0
#glbp 1 forwarder preempt delay minimum 0
On both GLBP routers
    
```

After optimization GLBP took 2.372 seconds to converge from the time ISP-1 detects interface down at 00:25:54.411. until the state update of R6 that took over as the active router for the two GLBP groups at 00:25:56.783 as shown in Fig.14. This provides a much better convergence time than the results from GLBP without optimizing timers. During the convergence process, 0 ICMP packets lost.

```

PC3
84 bytes from 8.8.8.8 icmp_seq=67 ttl=253 time=34.027 ms
84 bytes from 8.8.8.8 icmp_seq=68 ttl=253 time=39.364 ms
84 bytes from 8.8.8.8 icmp_seq=69 ttl=253 time=37.845 ms
84 bytes from 8.8.8.8 icmp_seq=70 ttl=253 time=36.331 ms
84 bytes from 8.8.8.8 icmp_seq=71 ttl=253 time=40.112 ms
84 bytes from 8.8.8.8 icmp_seq=72 ttl=253 time=29.519 ms
84 bytes from 8.8.8.8 icmp_seq=73 ttl=253 time=26.488 ms
84 bytes from 8.8.8.8 icmp_seq=74 ttl=253 time=26.490 ms
84 bytes from 8.8.8.8 icmp_seq=75 ttl=253 time=30.281 ms
    
```

Fig. 14. GLBP Conversion with Optimization

6.3.2 CPU Utilization

Before optimization GLBP took an average of 0.13% of CPU usages for R5 and R6 while both routers CPU utilization at 6%. After optimization GLBP took an average of 0.13% of CPU usages for R5 and R6 while both routers CPU utilization at an average 6 %.

```

R5
R5#sh processes cpu sorted
CPU utilization for five seconds: 8%/100%; one minute: 6%; five minutes: 6%
PID Runtime(ms)   Invoked  uSecs  SSec  lMin  SMin TTY Process
262   267040     2565522  104   4.31%  3.60%  3.44%  0 IP SLAs XOS Even
3      4672        790     5913   1.91%  0.15%  0.19%  0 Exec
239   19484     659978   29    0.39%  0.46%  0.44%  0 ISG MIB jobs Man
83    65752    125238   525   0.23%  0.18%  0.21%  0 IP Input
145   14956    15826    945   0.23%  0.11%  0.13%  0 CEF: IPv4 proces
112   8436    329060   25    0.15%  0.16%  0.15%  0 IPAM Manager
82    8496    329057   25    0.15%  0.16%  0.16%  0 IP ARP Retry Age
160   1936    329852   5     0.15%  0.12%  0.13%  0 GLBP
53    832    10573    78    0.15%  0.02%  0.00%  0 TTY Background
    
```

Fig. 15. GLBP CPU Utilization without Optimization

```

R6#sh processes cpu sorted
CPU utilization for five seconds: 6%/100%; one minute: 5%; five minutes: 6%
PID Runtime(ms)   Invoked  uSecs  SSec  lMin  SMin TTY Process
262   264992     2581995  102   3.27%  3.32%  3.47%  0 IP SLAs XOS Even
3      1748        557     3138   0.87%  0.11%  0.08%  0 Exec
82    8048    330605   24    0.31%  0.18%  0.16%  0 IP ARP Retry Age
268   22756    2128    10693   0.31%  0.25%  0.22%  0 Compute load avg
239   18684    663450   28    0.31%  0.32%  0.32%  0 ISG MIB jobs Man
59    10988    3191    3443   0.15%  0.11%  0.10%  0 HC Counter Timer
145   15288    15907    961   0.15%  0.12%  0.13%  0 CEF: IPv4 proces
112   9124    330605   27    0.15%  0.16%  0.17%  0 IPAM Manager
160   3668    10623    345   0.15%  0.07%  0.04%  0 PBR BR Learn
    
```

Fig. 16. GLBP CPU Utilization without Optimization

6.3.3. Hello Packet Bandwidth Consumption

Before optimization, Fig. 17. shows bandwidth consumption of GLBP hello packets in bytes/sec. GLBP hello packet size is 102 Byte. After optimization Fig. 18. shows bandwidth consumption of GLBP hello packets in bytes/sec.

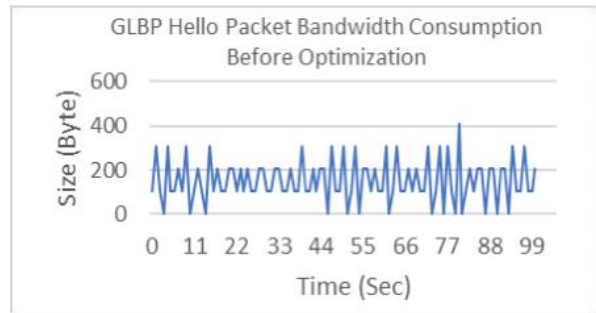


Fig. 17. GLBP Hello Packet Consumption Before Optimization

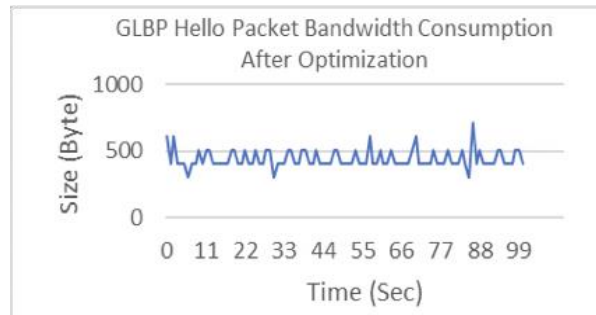


Fig. 18. GLBP Hello Packet Consumption After Optimization

6.3.4. Traffic Flow

Before optimization Fig. 19. data traffic flow in GLBP network throw R5 and R6, because of the default load balancing of GLBP each router became a forwarder. This makes the flow load balance between those two routers. This also provides more reliable flow without much drops like the HSRP and VRRP.

After optimization Fig. 20. shows the average data traffic flow in GLBP network throw R5 and R6. It provides a similar result to GLBP without the optimization.

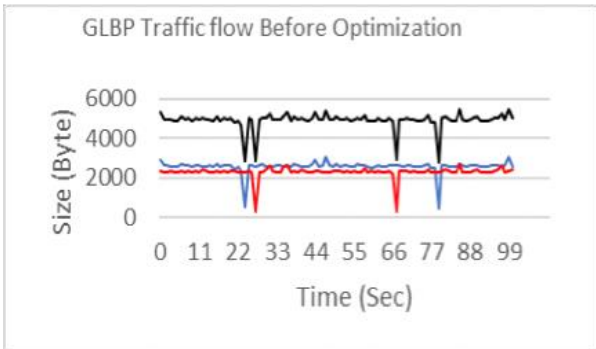


Fig. 19. GLBP Traffic Flow without Optimization

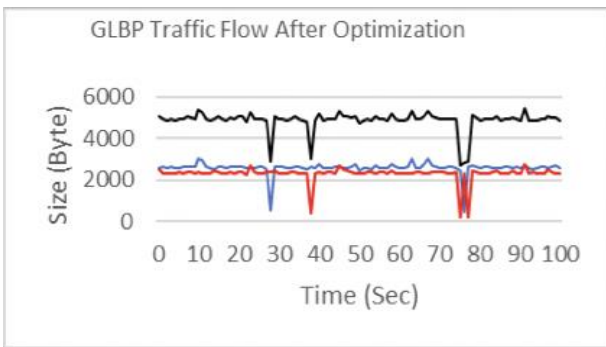


Fig. 20. GLBP Traffic Flow with Optimization

7. Comparison

7.1. CPU Utilization

Fig. 21 shows the CPU Utilization comparison between FHRP. VRRP has the best utilization of CPU then the GLBP.

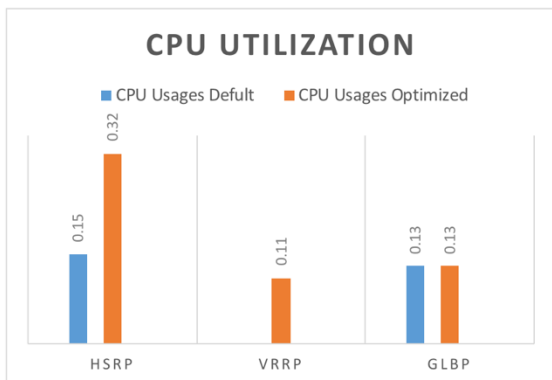


Fig. 21. FHRP CPU Utilization Comparison

7.2. Convergence Time

GLBP has the best convergence time at 2.372 seconds when optimized compared to HSRP at time 3.271 second, and VRRP at 4.861second.

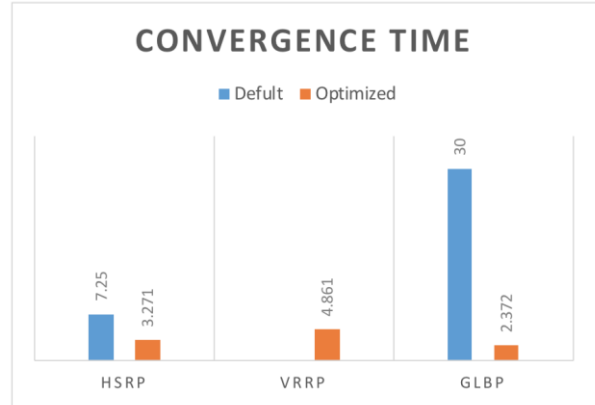


Fig. 22. FHRP Convergence Time Comparison

7.3. Packets Loss

Fig. 23 show Packet loss comparison between FHRP during convergence time. GLBP has the lowest packet loss after optimization.

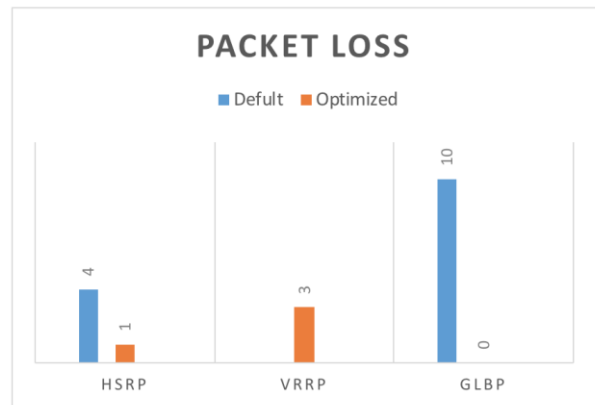


Fig. 23. FHRP Packet Loss Comparison

8. Conclusion

After implementing, optimizing and testing different FHRP and studying and analyzing their output of the conversion time, CPU utilization, and traffic flow, it is clear to see that GLBP has higher performance than HSRP and VRRP. Furthermore, the load balancing futures all make GLBP an efficient and reliable protocol to use for redundancy as it provides more network availability. The only downside is GLBP is CISCO proprietary.

References

- [1] Chris Oggerino, "High Availability Network Fundamentals", Cisco Press, 1st edition, 2001.
- [2] Priscilla Oppenheimer, "Top-Down Network Design", Cisco Press, 3ed edition, 2010.

- [3] Richard Froom, "Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Foundation Learning for SWITCH 642- 813", Cisco Press, 1st edition, 2010.
- [4] Rolf McClellan, Nick Lippis "Network-Level Redundancy/Resilience for High-Availability Campus LANs", ZDTag white paper", 1999, pp 6-8.
- [5] Mike Miclot, John Mower, "Reducing the Risk, Cost and Frequency of Production Stoppages Using Network Redundancy", 2010.
- [6] 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.
- [7] T. Li, B. Cole, P. Morton, D. Li," Cisco Hot Standby Router Protocol", Request for Comments: 2281, 1998.
- [8] cisco.com: Hot Standby Router Protocol Features and Functionality, <http://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>, 2006.
- [9] 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.
- [10] R. Hinden, Ed, "Virtual Router Redundancy Protocol", Request for Comments: 3768, 2004.
- [11] S. Nadas, "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", Request for Comments: 5798, 2010.
- [12] cisco.com: GLBP - Gateway Load Balancing Protocol , http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glb.html, 2016.
- [13] Jason C. Neumann, "The Book of GNS3", No Starch Press, 1st edition, 2015
- [14] 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.
- [15] M. Mansour, T. Shakshuki, "Performance Comparison of First Hop Redundancy Protocol", International Conference on Technical science, ICTS, March 2019 Tripoli- Libya.
- [16] 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.
- [17] 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.
- [18] 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.
- [19] 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.
- [20] Andy Sholomon, Tom Kunath, "Enterprise Network Testing", Cisco Press, 1st edition, 2011.