Simulation of High Availability Internet Service Provider's Network

Abdullah Jameel Mahdi[1] and Anas Ali Hussain[2]
[1]Information and Communication department, Information Engineering Collage, Al-Nahrin University
[2]Computer department, Engineering Collage, Al-Nahrin University
Email: info_abdu2006@yahoo.com, anas78@yahoo.com

Received: 10/02/2013
Accepted: 1/04/2013

Abstract **-** The rapid increase of connection-demand to the internet application services and highly traffic network is the main reason behind the need to scale a reliable network. This paper presents the steps of how to make the network reliable by using *Redundancy scheme* and how to balance traffic load in order to reach optimal network.
The implemented network is based on IEEE 802 LAN standard in which the equipment used in the topology is 3745Cisco's routers module and 2960 Ether Switch.
Also the Hot Standby Redundancy Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and Virtual Redundancy Routing Protocol (VRRP) are implemented in this work. Many tests in this work in order to achieve the load balancing of the implemented protocols (test the redundancy scheme) and to test the network performance through CPU utilization, bandwidth consumption by protocols, and measure the convergence time of the implemented protocols in the network. This paper gives a guideline for Internet Service Provider's Network (ISP) in order to avoid loss of information and increase the productivity and revenue. The obtained results show that the GLBP has the best performance in terms of CPU utilization and convergence time, and also in link consumption in comparison with HSRP and VRRP protocols for the same conditions.

Keywords – HSRP, VRRP, GLBP, ISP.

.

1 Introduction

The companies and government offices depend in their business on the network that has high availability without interruption of the services.

High availability refers to a system or component that operates continuously for a desirably long length of time. Availability can be measured relative to "100% operational" or "never failing". A widely-held but difficult-to-achieve standard of availability for a system is known as "five 9s" (99.999 percent) availability.Table1 shows the downtime experienced by a network and how it translates to a high-availability metric in which DPM refers to Defect per Million [1].

Table 1 Network Down time Interval [1].

Availability	DPM	Downtime Per Year (24x365)		
99.000%	10000	3 Days	15 Hours	36 Minutes
99.500%	5000	1 Day	19 Hours	48 Minutes
99.900%	1000		8 Hours	46 Minutes
99.950%	500		4 Hours	23 Minutes
99.990%	100			53 Minutes
99.999%	10			5 Minutes
99.9999%	1			30 Seconds

"High Availability"

In order to reach high availability, the network design must include hardware redundancy, protocols that manage or achieve redundancy and quick recovery from failure.

1. Redundancy and its Challenges

Redundancy in computer networks means the duplication of critical components or function of a system with the intention of increasing the reliability of the system [2].

Figure 1 shows a single ISP network that feeds the hosts LAN with Internet services. When the single ISP link is down, the end users will not become reachable to internet service.

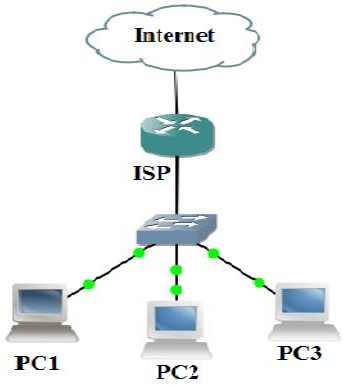


Figure 1. Single ISP Network

Any enterprise that requires consistently available access to and from the Internet should seriously consider using multiple ISPs connections into the enterprise network [3].

Redundant network design should satisfy the requirements for network availability by duplicating elements in a network such as router, switch, links, and internet connectivity and so on as shown in Fig. 2 [4].

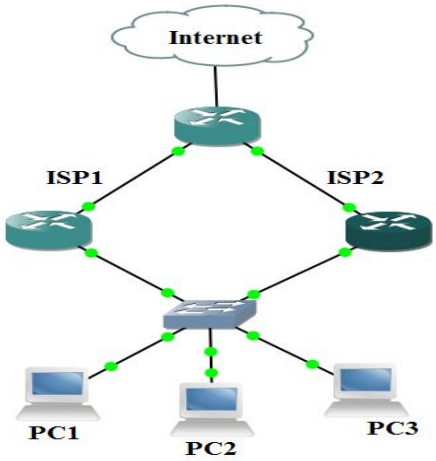


Figure 2. Multiple ISPs Network

In order to avoid outages and longtime of downtime caused by a single point of failure, parts of the network are repeated.

On a redundantly connected network if a device fails, then the connectivity would be preserved by routing traffic through a redundant connection.

One of the keys to make redundancy work for fault-tolerance problems is the mechanism for switching to the backup. The network redundancy should be the primary consideration for automated fault recovery. An important way of improving reliability in a certain network is particularly by the reliability against failures [5].

Even though redundant links are extremely helpful, they cause more problems than they solve. Because broadcast and multicast frames that do not have a destination hardware address specified where the source address will always be the hardware address of the device transmitting the frame, and the destination address will either be all 1s (broadcast), or with the network or subnet address specified and the host address all 1s (multicast) frames can be broadcast down all redundant links simultaneously, network loops can occur. The Spanning-Tree Protocol (STP) was developed to solve the loop problem. When a switch receives these types of frames, it then quickly floods out all of the switch's active ports by default, and this causes broadcast storm. To have broadcasts and multicasts only forwarding out a limited amount of administratively assigned ports, create Virtual Local Area Networks (VLANs) [6].

2. Virtual Local Area Network (VLAN)

A VLAN is a group of end stations in a switched network that is logically segmented by function, project team or application, without regard to the physical locations of the users [7].

The main benefit of VLAN is to create distinct broadcast domains. Devices within a VLAN can communicate with each other without the need for layer-3 routing, but devices in separate VLANs require a layer-3 routing device to communicate with one another. At first glance, using VLAN shows the need to a physical connection between network devices, but in practice the interfaces of the router are very limited. This problem can be overcome by using *sub-interfaces*, which are logical interfaces, created from one physical interface such as the physical interface f0/1,creating logical interfaces such as f0/1.1, f0/1.2…etc., and the router treats each sub-interface as a separate physical interface in routing decision [8].

3. Spanning Tree Protocol (STP)

STP is a link management protocol; standardized as IEEE 802.1D, that is a layer-2 protocol. The basic function of STP is to prevent bridge loops and the broadcast radiation. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

The spanning tree algorithm runs on a switch to activate or block redundant links if there are redundant links between nodes, then only one link is responsible for forwarding the traffic, this is done by creating a topology of all participating STP switches. The best loop free path through the switched network is then determined from this topology information.STP is implemented through the exchange of bridge protocol data unit (BPDU) messages between adjacent switches [9].

The slow convergence of spanning tree can cause major problems as the network grows. Also layer-2 switches cannot completely replace routers (layer-3 devices) in the internetwork [6].

Another drawback of the spanning- tree is the load balancing; STP does not provide load balancing [10].

4. First Hop Redundancy Protocols (FHRP)

Redundancy protocol is a computer networking protocol which is designed to protect the default gateway address used on a sub-network by allowing two or more routers to provide backup for that address [11].

Redundancy protocols work by giving a way to configure more than one router to appear as one single router. This makes client configuration and communication easier because it can configure a single default gateway and the host machine can use its standard protocols to talk [12].

There are a number of methods that an end-host can use to determine its first hop router towards a particular IP destination. These include running a dynamic routing protocol such as Routing Information Protocol (RIP) or OSPF version 2 (OSPF), running an Internet Control Message Protocol (ICMP) router discovery client (DISC), or using a statically configured default route. Running a dynamic routing protocol on every end-host may be infeasible for a number of reasons, including administrative overhead, processing overhead, security issues, or lack of a protocol implementation for some platforms. Neighbor or router discovery protocols may require active participation by all hosts on a network, leading to large timer values to reduce protocol overhead in the face of large numbers of hosts. This can result in a significant delay in the detection of a lost (i.e., dead) neighbor, that may introduce unacceptably long "black hole" periods. The use of a statically configured default route is quite popular; it minimizes configuration and processing overhead on the end-host and is supported by virtually every IP implementation. This mode of operation is likely to persist as Dynamic Host Configuration Protocols (DHCP) are deployed, which typically provide configuration for an end-host IP address and default gateway. However, this creates a single point of failure. Loss of the default router results in a catastrophic event, isolating all end-hosts that are unable to detect any alternate path that may be available [13].

The FHRP is designed to eliminate the single point of failure inherent in the static default routed environment by using an election algorithm.

4.1. Hot Standby Routing Protocol (HSRP)

HSRP is Cisco's standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address [14].

HSRP defines a standby group. Each of the standby groups defined include:

- Active router: higher router priority is elected to be an active router that physically forwards packets sent to the virtual router MAC address. This means that this active router responds to traffic. If an end-device sends an ARP request to the virtual router IP address, the active router

replies with the virtual router MAC Address.

- Standby router: a standby router that quickly assumes the packet-forwarding responsibility if the active router goes down.
- Virtual router: the virtual router is what the end-devices use for communicating with the "gateway", this is the IP and MAC Address configured on the end-devices. The virtual router processes no physical frames.
- Any other routers: that maybe attached to the subnet [12].

The benefits of using HSRP in redundancy network are:

- Redundancy**:** HSRP employs a redundancy scheme that is time proven and deployed extensively in large networks.
- Fast Failover: HSRP provides transparent fast failover of the first-hop router.
- Preemption: preemption allows a standby router to delay becoming active for a configurable amount of time.
- Authentication: HSRP message digest 5 (MD5) algorithm authentications protects against HSRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security [15].

While the drawbacks of using HSRP are:

- HSRP does not allow for efficient and total use of network resources when multiple available paths exist unless additional configuration steps are taken.
- Cisco proprietary protocol is implemented on Cisco devices only.
- Authentication used in HSRP is sent unencrypted. Just capturing a single hello message, it is fairly easy to know the entire HSRP configuration, like IDs, priorities, timers and virtual addresses [14, 16].

The configuration used in this paper is Multiple Hot Standby Redundancy Protocol (MHSRP), where MHSRP is an extension of HSRP that allows load sharing between two or more HSRP groups. This means one router is active for their group and at the same time standby for other group in HSRP group members [14].

4.2. Virtual Redundancy Routing Protocol (VRRP)

VRRP is an IETF standard; it is open standard that allows a group of routers to form a single virtual router used to increase the availability of default gateway servicing hosts on an IEEE 802 LAN. VRRP specifies an election protocol to provide the virtual router function [12].A VRRP group member consists of the following:

- Master router: the VRRP router that is assuming the responsibility of forwarding packets sent to IP address associated with the virtual router, and answering ARP requests for these IP addresses.
- Backup router(s): the set of VRRP routers available to assume forwarding responsibility for a virtual router should the current master fail [13].

Here are detailed the main strengths of VRRP as First Hop Redundancy protocol:

- Open source: can implement with different vendors including Cisco's devices [12].
- Redundancy: enables to configure multiple routers as the default gateway router, which reduces the possibility of a single point of failure in a network.
- Load Sharing: allows traffic to and from LAN clients to be shared by multiple routers. The traffic load is shared more equitably among available routers.
- Multiple VRRP groups: supports up to 255 VRRP groups on a router physical interface. Multiple VRRP groups enable to implement redundancy and load sharing in LAN topology.
- Preemption: enables to preempt a backup router that has taken over for a failing master with a higher priority backup router that has become available.
- VRRP Tracking: ensures that the best VRRP router is the master for the group by altering VRRP priorities based on interface states [17].

While the drawbacks of the VRRP are:

- VRRP does not allow for efficient and total use of network resources when multiple available paths exist unless additional configuration steps are taken.
- No security is used, as the offered authentication method is weak because the authentication used is plain text and sent unencrypted [16, 17].

4.3.Gateway Load Balancing Protocol (GLBP)[18]

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

GLBP performs a similar, but not identical, function for the user as the HSRP and the VRRP. 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 GLBP members.

GLBP consists of the following:

- One Active Virtual Gateway (AVG): the highest router priority becomes AVG. AVG assigns a virtual MAC addresses to each member of the GLBP group. The AVG is responsible for answering Address Resolution Protocol (ARP) requests for the virtual IP address. Load sharing is achieved by the AVG replying to the ARP requests with different virtual MAC addresses. The other routers in GLBP group members provide backup for the AVG in the event that the AVG becomes unavailable.
- Many Active Virtual Forwarders (AVF): each gateway assumes responsibilities for forwarding packets sent to the virtual MAC address assigned to it by the AVG. Gateways are assigned the next MAC address in sequence.
- Primary virtual forwarder: a virtual forwarder that is assigned a virtual MAC address by the AVG.
- Secondary virtual forwarder: other members of the GLBP group learn

the virtual MAC addresses from Hello messages.

4.3.1. Load balancing options [19]

- **None**: if no load-balance algorithm is specified then GLBP will operate in an identical fashion to HSRP, the AVG will only respond to Address Resolution Protocol (ARP) requests with its own Virtual Forwarder (VF) MAC address.
- **Weighted**: place a weight on each device when calculating the amount of load sharing that will occur through MAC assignment. Each GLBP router in the group will advertise its weighting and assignment; the AVG will act based on that value.
- **Host dependent**: the MAC address of a host is used to determine which VF MAC address the host is directed towards. This ensures that a host will be guaranteed to use the same virtual MAC address as long as the number of VFs in the GLBP group is constant
- **Round Robin**: with Round Robin each VF MAC address is used sequentially in ARP replies for the virtual IP address. Round robin is the default GLBP load balancing.

There is a negligible CPU difference in the operation of either of these options.

GLBP has important strengths; the most important are listed as follows:

- **Load Sharing:** the configuration of GLBP in such a way that traffic from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.
- **Multiple Virtual Routers:** GLBP supports up to 1,024 virtual routers (GLBP groups) on each physical interface of a router and up to four virtual forwarders per group.
- **Preemption:** the redundancy scheme of GLBP enables to preempt an AVG with a higher priority backup virtual gateway that has become available. Forwarder preemption works in a similar way, except that forwarder preemption uses weighting instead of priority and is enabled by default.
- **Efficient Resource Utilization:** GLBP makes it possible for any router in a group to serve as a backup, which eliminates the need for a dedicated backup router because all available routers can support network traffic [12].
- **Low Overhead**: the protocol uses minimal processor and bandwidth resources.
- **Fast Failover**: GLBP failover occurs immediately after the failure in a gateway is detected. End stations and applications continue as if no failure had occurred.
- **Flexibility**: several load-balancing algorithms are available for different network configurations and customer requirements.
- **Authentication and Security**: the protocol initially implements a very simple authentication scheme. An 8-character string carried in every packet is compared with a configured value, and only packets that match are accepted. MD5 authentication is planned for a future release [16].

While the drawbacks of the GLBP are:

- Cisco proprietary protocol.

- Weak security and authentication [16].

5. The Convergence Time of the Network [21]

The convergence time is very important in the stability of the network. Convergence occurs when the network topology changes, or when adding new equipment to the network. Each of the FHRP protocols have its convergence time that enters into four phases:

- Detection: detects the topology change.
- Propagation: propagates information about the change to neighbors.
- Computation: depends on the algorithm of the protocol and protocol itself.
- Update of routing table: all routing table, database table are updated.

Convergence time can be optimized with appropriate actions in every phase. Convergence is based on many parameters, so optimization is very complex process. Almost everything is an input to this process. The best results can be obtained, when optimization is done by starting on the physical layer and optimizing every other layer appropriately with consideration of the other layers, protocols and techniques used in the network. Optimization of configuration parameters is recommended and used.

6. Optimization Features for FHRP

FHRP offers optimizing options to make it possible to allow network optimizations, such feature as the following:

- **Tracking:** the tracking option monitor interface condition such as line-protocol and IP routing. If the interface changes its state, the interface priority is decremented by specified value. The default is 10.
- **Priority:** the priority value in FHRP group influencing in the choice of active and standby router in HSRP and GLBP group, and choice Master and Backup router in VRRP group. The default value for FHSR priority is 100.
- **Preempt:** preemption option provides the facility to the active router to become active after re-establishing the link (if active router fails) [20].
- **Weighting:** this option is used by GLBP to determine which router becomes the owner of the new AVF. Each gateway begins with a maximum weight value (range from 1 to 254, default 100), when tracked, interfaces go down, or when weight becomes up or down the specified threshold value, the weight decreases and increases when the interface come back [18].
- **Timers:** HSRP and GLBP have two important timers, hello time and hold time. Hello time is set for hello messages to send every specified interval; the default value is 3 seconds [18, 20].
- VRRP hello time is called advertise time. The default value is 1 second [13].
- **Hold time:** the time before the active or standby router is declared to be down. The defaults hold time for HSRP and GLBP is 10 second [19, 21]. The hold time for VRRP isn't default and calculated as declared in RFC 3768: skew time = (256-priority)/256. Master down interval= (3* advertisement time + skew time) [13].

For example, the priority set for ISP1 is 150, and the advertise set to default:
The skew time=256-150/256= 0.414 second.
Master down interval= (3*1+0.414) = 3.414 second.

8. Experiment Set-up with FHRP

8.1. Equipment

For implementation, the equipment used Cisco's devices (four Routers, one Ether Switch) as shown in table 2.

Table 2. Equipment for ISPs network

Cisco's Devices	Description	Quantity
Router	3745	4
Ether Switch	2960	1
Fast Ethernet	100 Mbps link	12

8.2. System Implementation and Results

The suggested network topology is dividing main ISP link to a triple ISPs branches to feed LAN hosts with Internet services as shown in Fig. 3.

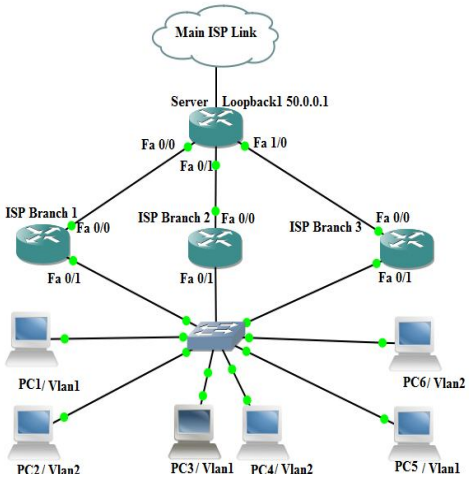


Figure 3. Triple ISPs Network Topology

This dividing is to increase the availability of the main ISP link in face of the failure. Every two PCs belong to a specific ISP branch as a way of theoretical load balancing done by the administrator. FHRP was applied to maintain redundancy topology and achieve load balancing between ISPs branches when one or two of the ISPs is unreachable. The simulator used in this paper is Graphical Network Simulator 3 (GNS3) that is emulated for real environment, and Wire shark network analyzer to analysis the network work and traffic.

8.2.1. HSRP Load Balancing

In this paper, Multiple Hot Standby Redundancy Protocol (MSRP) was used in the configuration. In the configuration process the command <**standby preempt**> must be entered in each HSRP interfaces [14].

Load balancing in MHSRP is achieved by election processes that depend on the priority values, as illustrated in Fig.4 that show the administrator balancing distribution.

```
ISP1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/1.1     1    150 P Active  local           192.168.1.10    192.168.1.254
Fa0/1.1     3    140 P Standby 192.168.1.10    local           192.168.1.224
Fa0/1.1     5    140 P Standby 192.168.1.20    local           192.168.1.234
Fa0/1.2     2    150 P Active  local           192.168.2.20    192.168.2.254
Fa0/1.2     4    130 P Listen  192.168.2.10    192.168.2.20    192.168.2.224
Fa0/1.2     6    140 P Listen  192.168.2.20    192.168.2.10    192.168.2.234
```

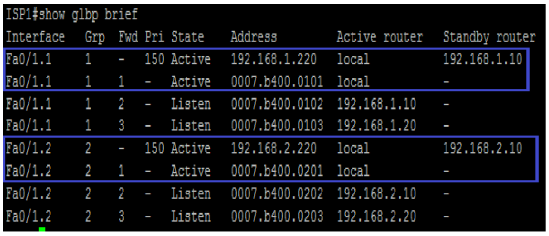
Figure 4. Configured MHSRP

For example, sub-interface f0/1.1 in router ISP branch1 with configured IP address 192.168.1.1 and virtual gateways 192.168.1.254is assigned to be active path for PC1.Sub-interface f0/1.1 in router ISP branch2 with configured IP address 192.168.1.10 and virtual gateway 192.168.1.224 is assigned to be active path for PC3 and standby path for PC1.To establish connection from PC1tointerface

loopback1 having IP address 50.0.0.1, the path for PC1 is through its active gateway 192.168.1.254 for normal operation as illustrated in Fig. 5.

Figure 5. Normal Route for PC1

In case that router ISP branch1 fail, PC1 will continue access to internet services through the standby path 192.168.1.224 (ISP branch2) that now becomes active for PC1 and it is originally active for PC3 as illustrated in Fig. 6.



ISP1#show glbp brief

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Fa0/1.1	1	-	150	Active	192.168.1.220	local	192.168.1.10
Fa0/1.1	1	1	-	Active	0007.b400.0101	local	-
Fa0/1.1	1	2	-	Listen	0007.b400.0102	192.168.1.10	-
Fa0/1.1	1	3	-	Listen	0007.b400.0103	192.168.1.20	-
Fa0/1.2	2	-	150	Active	192.168.2.220	local	192.168.2.10
Fa0/1.2	2	1	-	Active	0007.b400.0201	local	-
Fa0/1.2	2	2	-	Listen	0007.b400.0202	192.168.2.10	-
Fa0/1.2	2	3	-	Listen	0007.b400.0203	192.168.2.20	-

Figure 6. Backup Route for PC

8.2.2. VRRP Load Balancing

The election process in VRRP is similar to that in HSRP that depends on the priority, where the high priority configured value becomes the master and the other next higher priority becomes the backup for the master as illustrated in Fig.7 that show the administrator balancing distribution.

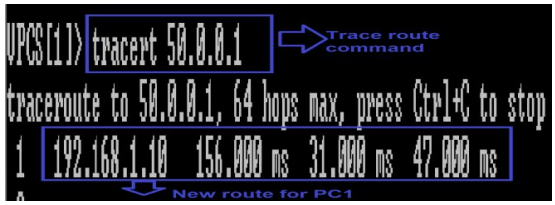


Figure 7. Configured VRRP

When applying the same scenario applied in HSRP, the results obtained illustrated in Fig. 8show the normal route for PC1 is through ISP branch1 sub-interface f0/1.1 ip address 192.168.1.1.

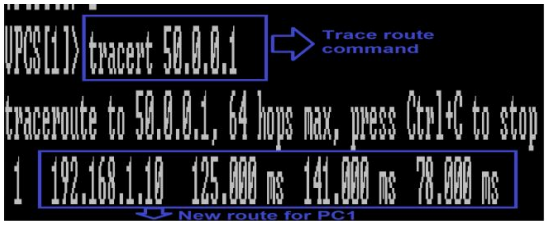
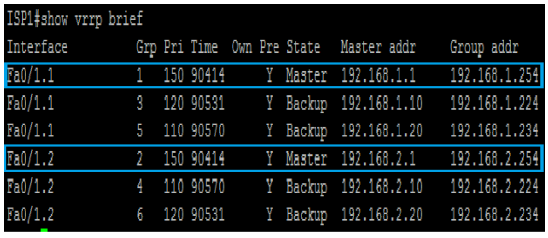


Figure 8. Normal Route for PC1

In case of ISP branch1 fail, the result in Fig. 9 show the new route for PC1 is through ISP branch2 sub-interface f0/1.1 ip address 192.168.1.10.



ISP1#show vrrp brief

Interface	Grp	Pri	Time	Own	Pre	State	Master addr	Group addr
Fa0/1.1	1	150	90414		Y	Master	192.168.1.1	192.168.1.254
Fa0/1.1	3	120	90531		Y	Backup	192.168.1.10	192.168.1.224
Fa0/1.1	5	110	90570		Y	Backup	192.168.1.20	192.168.1.234
Fa0/1.2	2	150	90414		Y	Master	192.168.2.1	192.168.2.254
Fa0/1.2	4	110	90570		Y	Backup	192.168.2.10	192.168.2.224
Fa0/1.2	6	120	90531		Y	Backup	192.168.2.20	192.168.2.234

Figure 9. Backup Route for PC1

8.2.3. GLBP Load Balancing

GLBP is different from HSRP and VRRP by adding basic load balancing functionality; also the election process is

different. GLBP elects an Active Virtual Gateway (AVG) and Active Virtual Forwarder (AVF). One AVG for GLBP group members and each gateway in GLBP group members is AVF for their hosts and responsible in forwarding host packets as illustrate in Fig. 10.

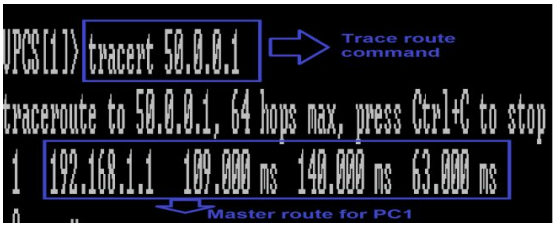


Figure 10.Configured GLBP Group Members

The configured load-balancing is round robin; this means that AVG assign VF MAC address sequentially. The same scenario applied in HSRP and VRRP is applied for GLBP. In the normal operation the route of PC1 is through ISP branch1 sub-interface f0/1.1 ip address 192.168.1.1 forwarder 1 as illustrated in Fig. 11.

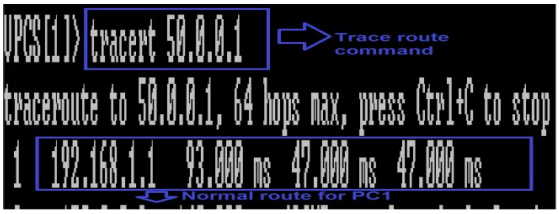


Figure 11. Normal PC1 Route

In case ISP branch1 forwarder 1 is unavailable, the new route for PC1 is through ISP branch2 forwarder 2 because it is the next higher weighting value for PC1 as illustrated in Fig. 12.

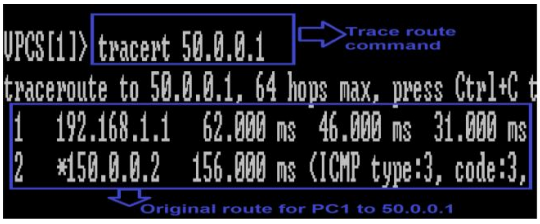


Figure 12. Backup Route for PC1

9. Calculation of CPU Utilization, Convergence Time, and Bandwidth Consumption

Two tests have been done to calculate CPU utilization, bandwidth consumptions, and convergence time that have an effect on network performance. The first test is to set the default values of hello time, hold time, priority, and preempt. The results are shown in the table 3.

Table 3. First Test-Default Parameters

Protocol	CPU [%]	BW [Kbps]	Convergence time [second]	Length of packet[Byte]
MHSRPv2	0.56	0-1	9.502	94
VRRP	0.98	0-1	10.388	60
GLBP	0.42	0~1	8.316	102

The second test is to optimize the parameters value by changing the hello time to 1 second, hold time to 3 seconds for HSRP and GLBP, increasing the priority value to 254 for VRRP and letting the preemption delay value to default (0 second).The results are as shown in the table 4.

Table 4. Test Two Results-Optimized Parameters

Protocol	CPU [%]	BW [Kbps]	Convergence time [second]	Length of packet[Byte]
MHSRPv2	1.49	0-2	2.521	94
VRRP	1.98	0-2	8.176	60
GLBP	1.24	0~2	2.312	102

When drawing the results in table 1 and 2 as a graphs in order to analysis the tested FHRP, the CPU utilization of GLBP is less than HSRP and VRRP before and after optimization features as illustrated in Fig.13.

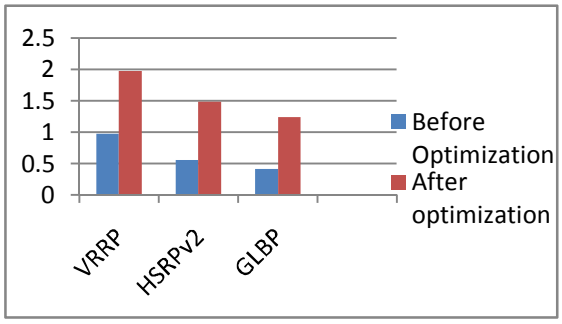


Figure 13. CPU Utilization

Also convergence time of GLBP is better than HSRP and VRRP before and after optimization features as illustrated in Fig. 14.

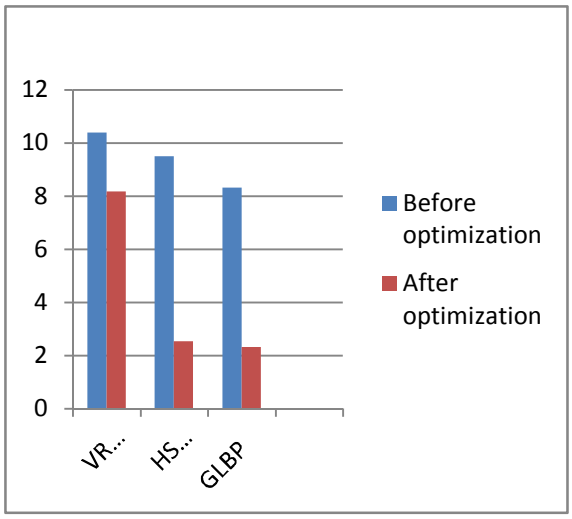


Figure 14. Convergence Time

There are two ways to increase the network bandwidth. One way is to reduce the affecting factor (cable attenuation, bridge tap, etc.) in the media. This method can save bandwidth and be utilized in the efficient way. The second way is to increase the amount of bandwidth available by changing network media. For example, if replace the 4 Mbps with 16 Mbps link, it will increase the available bandwidth by a factor of four. GLBP link bandwidth consumption is less than HSRP and VRRP as illustrated in Fig. 15.

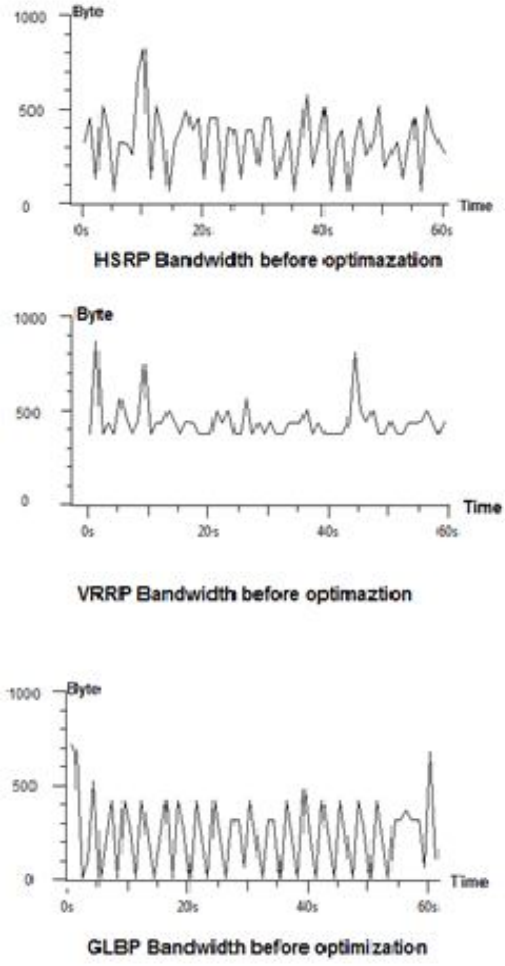


Figure 15. FHRP Bandwidth Consumption before Optimization

And after optimized the configurable parameters of FHRP, the bandwidth consumption by the protocol GLBP is still less than HSRP and VRRP as illustrated in Fig. 16.

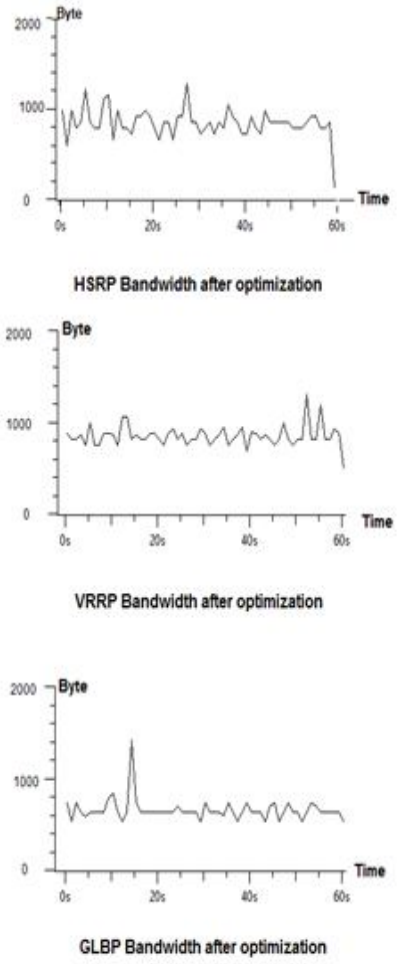


Figure 16. FHRP Bandwidth Consumption after Optimization

10. Conclusion

The paper studies and tests the FHRP load balancing and performance; the analysis highlights insightful features of redundancy protocols. Even in worst case when ISP branch1 and ISP branch2 become down, PCs on this branches will continuo access to internet services through ISP branch3.

After carefully examining the algorithm of redundancy of each of the protocols such as CPU utilization, link bandwidth consumption and convergence time and with taking into consideration the stability of the network when optimizing the FHRP features, the results showed that:

- GLBP has the best performance among HSRP and VRRP making GLBP an efficient protocol to be used in the generation of redundancy and backups.

- These results are so important especially when the network enlarges and becomes greater. Instead of changing the devices or links between devices because of the hug consuming of the CPU or link bandwidth due to the network growth, changing the type of protocol implemented in the network is cheaper than replacing the devices or links.

References

[1] Delivering High Availability in the Wiring Closet with Cisco Catalyst Switches white paper.http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns431/ns17/net_implementation_white_paper0900aecd804599e6.html.

[2] Redundancy Management Technique for Space Shuttle Computers (PDF), IBM Research.

[3] A Practical Guide to ISP Redundancy and Uninterrupted Internet Connectivity whitepaper. http://www.ithound.com/abstract/practical-guide-isp-redundancy-uninterrupted-internet-connectivity-2220.

[4] P. Oppenheimer, "Top-Down Network Design", Third Edition. 2010.

[5] "Experiencing network problems", Cisco Systems. http://www.cisco.com/en/US/products/ps9967/products_qanda_item09186a0080a 3698f.shtml.

[6] T. Lammle, "Cisco Certificate Network Associated (CCNA) study guide", second edition, Sybex Inc. 2000.

[7] "Configuring VLANs", Cisco Systems.http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/VLANs.html

[8] "Configuring Ethernet Settings and Sub interfaces", Cisco Systems. http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/intrface.html

[9] D. Hucaby, D. Donohue, and S. Wilkins, "CCNP SWITCH 642-813 Cert Kit", 1st edition, Jan 25, 2010.

[10] D. Levi, D. Harrington, "RFC 4318", Dec. 2005. http://www.apps.ietf.org/rfc/rfc 4318.html.

[11] "First Hop Redundancy protocol",http://en.wikipedia.org/wiki/First_Hop_Redundancy_Protocols.

[12]**Patrick J. Conlan**, "Cisco Network Professional's: Advanced Internetworking Guide", Pub. Date: May 11, 2009.

[13] "VRRP RFC 3768"http://tools.ietf.org/html/rfc3768

[14] "Configuring HSRP and Enhanced Object Tracking", Cisco Systms.http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_35_se/configuration/guide/swhsrp.pdf.

[15] "Configuring HSRP", Cisco Systems. http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1090733.

[16] "Gateway Load Balancing Protocol Overview" White paper, Cisco Systems. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6550/prod_presentation0900aecd801790a3_ps6600_Products_Presentation.html.

[17] "Configuring VRRP", Cisco Systems. http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_vrrp.html#wp1054588.

[18]"Gateway Load Balancing Protocol document", Cisco Systems. http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html.

[19] "Cisco Gateway Load Balancing Protocol options", Cisco Systems.http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6600/product_data_sheet0900aecd803a546c.html.

[20]T. Li, B. Cole, P. Morton, D. Li, "HSRP for optimization", RFC 2281, March 1998.

[21]Evans, J., Fils fils, C., "Engineering a multiservice IP backbone to support tight SLAs. Computer Networks", September 2002, vol. 40, no. 1, pp. 131-148