Winter 2-2014

ANALIZING PROTOCOLS FOR LAYER THREE NETWORK REDUNDANCY

Taulant Galimuna

University for Business and Technology
School of Computer Sciences and Engineering

ANALIZING PROTOCOLS FOR LAYER THREE NETWORK REDUNDANCY

Bachelor Degree

Taulant Galimuna

February 2014
Prishtinë

University for Business and Technology
School of Computer Sciences and Engineering

Bachelor Thesis
Academic year 2010 – 2013

Student:
Taulant Galimuna

ANALIZING PROTOCOLS FOR LAYER THREE NETWORK REDUNDANCY

Mentors: Mr. Selman Haxhijaha
Dr. Petrit Shala

February 2014

This thesis is submitted in partial fulfillment of the requirements for a Bachelor Degree

Abstract

This thesis will analyze FHRP (First Hop Redundancy Protocols) which are three redundancy protocols of the IP Layer (layer 3). Protocols of the default gateway redundancy or FHRP are HSRP (Hot Standby Router Protocol) which is a Cisco proprietary and is an active/standby redundancy protocol, GLBP (Gateway Load Balancing Protocol) which is an active/active redundancy protocol and also it does Load Balancing, and the last VRRP (Virtual Redundant Routing Protocol) which is typically used with non-Cisco routers (such as Juniper) and is an extension of GLBP. Basically what FHRP protocols do is; they allow multiple redundant routers on the same subnet to act as a single default router (first-hop router). Layer 3 redundancy protocols were designed to keep networks 100% up and running.

The focus of this thesis is the difference between the three protocols and the way they use to keep the network up and running.

Acknowledgement

I would never have been able to finish my thesis without the guidance of my professor, help from friends, and support from my family and wife.

Foremost, I would like to express my sincere gratitude to my advisor Prof. Mr. Selman Haxhijaha for the continuous support of my BCs study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis and other projects related to networking. I could not have imagined having a better advisor and mentor for my BCs study.

Besides my advisor, I would like to thank Prof. Dr. Petrit Shala, for his encouragement, insightful comments, and hard questions☺.

Last but not the least; I would like to thank my family, my wife, my parents, my brother and sister for supporting me spiritually throughout my life.

Prishtine, 10 January 2014

Taulant Galimuna

Table of content

LIST OF FIGURES 7

LIST OF TABLES 8

LIST OF ABBREVIATIONS.. 9

1 INTRODUCTION.. 10

1.1 Problem Statement 10

1.2 Research Questions 10

1.3 First Hop Redundancy Protocol Concept 10

1.3.1 The need of Redundancy in networks 11

1.3.2 The three solutions for First Hop Redundancy.......................... 14

2 LITERATURE REVIEW 15

2.1 Hot Standby Router Protocol (HSRP) 15

2.1.1 HSRP Background and Operations 15

2.1.2 Dynamic Router Discovery Mechanisms 17

2.1.3 HSRP Operation 18

2.1.4 HSRP Addressing 19

2.1.5 HSRP Load Balancing 20

2.1.6 HSRP Features 21

2.1.7 Interface Tracking 22

2.1.8 Configuring and Verifying HSRP 23

2.2 Gateway Load Balancing Protocol 26

2.2.1 GLBP Concepts 26

2.2.2 Configuring and Verifying GLBP 28

2.3 Virtual Router Redundancy Protocol 32

2.3.1 Introduction 32

2.3.2 VRRP Operation.. 33

2.3.3 VRRP Benefits 35

2.3.4 VRRP Router Priority and Preemption 37

2.3.5 VRRP Advertisements... 37

2.3.6 VRRP Object Tracking 38

2.3.7 How VRRP Object Tracking Affects the Priority of a Device 38

3 METHODOLOGY 39

4 CASE STUDY 40

5 EXPERIMENTAL DESIGN 41

5.1 Experimental Setup A (HSRP) 41

5.2 Experimental Setup B (GLBP) 42

5.3 Experimental Setup C (VRRP) 43

6 RESULTS 44

6.1 Testing results of HSRP 44

6.2 Testing results of GLBP 45

6.3 Testing results of VRRP 46

7 CONCLUSIONS 47

8 REFERENCES 49

9 APPENDIX 50

9.1.1 Basic configuration of HSRP 50

9.1.2 Basic configuration of GLBP 52

9.1.3 Basic configuration of VRRP 53

9.1.4 Router configs of ISP and L3PR_CR1 54

9.1.5 Router configs of HSRP Routers 57

9.1.6 Router configs of GLBP Routers 60

9.1.7 Router configs of VRRP Routers 63

LIST OF FIGURES

Figure 1. First Hop Redundancy Protocol [3] 11
Figure 2. Single point of failure [1]........ 12
Figure 3. Redundant Network [1]........ 12
Figure 4. Balancing Traffic by Assigning Different Default Routers to Different Clients [1]........ 13
Figure 5. All Traffic goes to 192.168.0.1 (R1, Which is Active); R3 is Standby [1] 16
Figure 6. Packets Sent Through R3 (New Active) Once it Takes over for Failed R1 [1]17
Figure 7. Load Balancing with HSRP by Using Different Active Routers per Subnet [1] 21
Figure 8. GLBP Directs Host A by Sending Back ARP Reply with R1's MAC1 [3] 27
Figure 9. GLBP Directs Host B by Sending Back ARP Reply with R2's VMAC2 [3].... 28
Figure 10. Basic VRRP topology [4] 34
Figure 11. Load Sharing and Redundancy VRRP Topology [8] 35
Figure 12. Adding redundancy protocols to the network 40
Figure 13. HSRP using network 41
Figure 14. GLBP using network........ 42
Figure 15. VRRP using network 43
Figure 16. HSRP Active elected router 44
Figure 17. Pinging from L3PR_CR1 to ISP Loopback 44
Figure 18. Interface shutdown on L3PR_L1 (HSRP Active router)........ 45
Figure 19. L3PR_L2 (standby router) changing from standby to Active........ 45
Figure 20. GLBP Active elected router 45
Figure 21. Pinging from L3PR_CR1 to ISP Loopback (GLBP)........ 45
Figure 22. Interface shutdown on L3PR_L1 (GLBP Active router)........ 46
Figure 23. (standby router) changing from standby to Active (GLBP)........ 46
Figure 24. VRRP Master elected router 46
Figure 25. Pinging from L3PR_CR1 to ISP Loopback (VRRP)........ 46
Figure 26. Interface shutdown on L3PR_L1 (VRRP Master router) 47
Figure 27. (backup router) changing from Backup to Master (VRRP)........ 47

LIST OF TABLES

Table 1. List of the three FHRP Options [3] 14
Table 2. Comparing Local State in show glbp brief Commands [2] 31
Table 3. Difference between features of HSRP, VRRP, GLBP [8] 48

LIST OF ABBREVIATIONS

FHRP	First Hop Redundancy Protocol
HSRP	Hot Standby Router Protocol
GLBP	Gateway Load Balancing Protocol
VRRP	Virtual Redundant Routing Protocol
WAN	Wide Area Network
LAN	Local Area Network
VLAN	Virtual Local Area Network
IP	Internet Protocol
ARP	Address Resolution Protocol
IETF	Internet Engineering Task Force
RFC #	Request for Comments #
VIP	Virtual IP
MAC	Media Access Control Address
VMAC	Virtual MAC
SRB	Source-Route Bridging
RIF	Routing Information Field
USE-BIA	Use Burned-In Address
Cisco IOS	Cisco Internetwork Operating System
AVG	Active Virtual Gateway
AVF	Active Virtual Forwarder
RIP	Routing Information Protocol
OSPF	Open Shortest Path First
DHCP	Dynamic Host Configuration Protocol
IRDP	ICMP Router Discovery Protocol

1 INTRODUCTION

1.1 Problem Statement

Businesses rely on their networks to get their work done. Some businesses rely more on the network than others, with a direct connection between network outages and lost revenue. For instance, when the network is down, some companies lose customers, or lose sales, or they cannot ship their goods to market, affecting sales volume in the future. Companies can design their networks to use redundancy - extra devices and extra links - so that when a device fails, or a link fails, the network still works. The extra devices may cost more money, but the cost may be justified, given the cost of an outage. Networks that have redundant devices and links sometimes require additional protocols to deal with changes to how the network functions with the added redundancy. This chapter discusses one such class of protocols, called First Hop Redundancy Protocol (FHRP). FHRPs allow network engineers to install multiple routers in a subnet, which collectively act as a single default router. The FHRP makes the routers appear like a single default router to the hosts, letting the hosts be completely unaware of the redundant routers while receiving the benefits of that redundancy. The routers exchange messages to coordinate which router does the work and how to recognize a router problem and take over the function of the other router when needed. [1]

1.2 Research Questions

To get a clear understanding of what has to be researched and analyzed in the thesis we have defined two research questions:

- What is the advantage of using Layer three (3) redundancy protocols in a big company?
- Describe and compare FHRP (First Hop Redundancy Protocols)?

1.3 First Hop Redundancy Protocol Concept

Default Gateway Redundancy also known as (First Hop Redundancy Protocol) allows a highly available network to recover from the failure of the device acting as the default

gateway for the end stations on a physical segment (See Figure 1) [2]. It is a computer networking protocol which is designed to protect the default gateway used on a sub-network by allowing two or more routers to provide backup for that address. In the event of failure of the active router, the backup router will take over the address, usually within a few seconds.
When networks use a design that includes redundant routers, switches, LAN links, and WAN links, in some cases other protocols are required to both take advantage of that redundancy and to prevent problems caused by it. For instance, imagine a WAN with many remote branch offices. If each remote branch has two WAN links connecting it to the rest of the network, those routers can use an IP routing protocol to pick the best routes. When one WAN link fails, the routing protocol can learn routes that all happen to use the one remaining WAN link, taking advantage of the redundant link. [2]

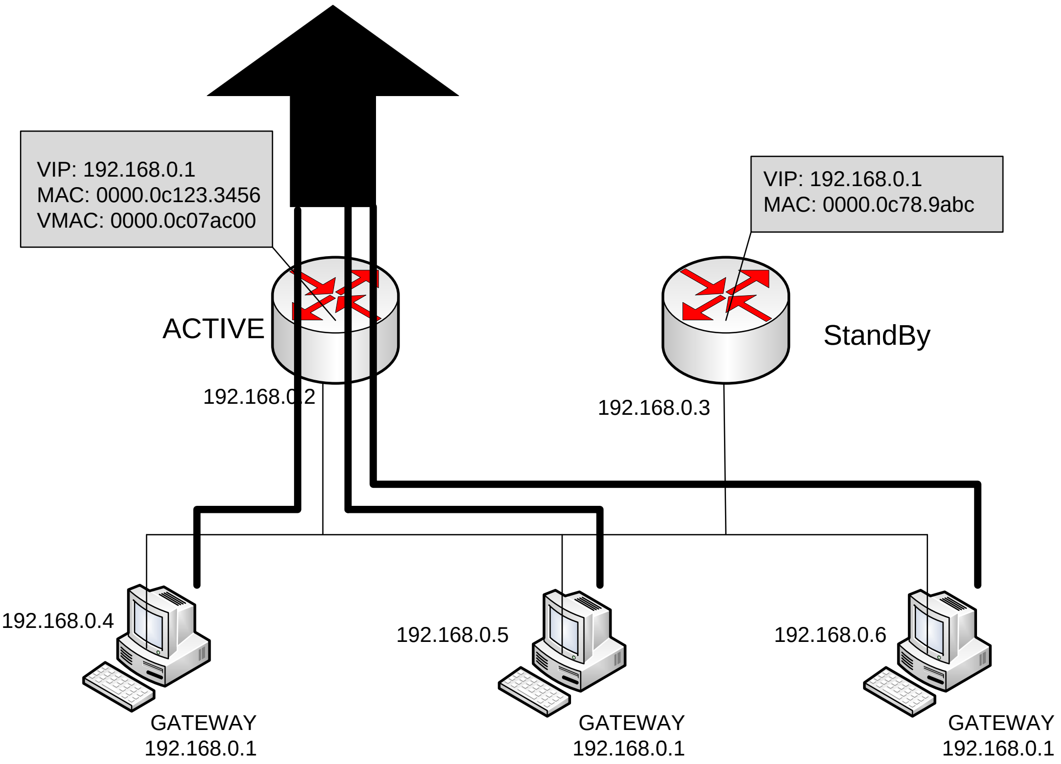


Figure 1. First Hop Redundancy Protocol [3]

1.3.1 The need of Redundancy in networks

Network needs redundant links to guarantee availability between one point and the other. The goal of redundant topologies is to eliminate network downtime caused by a single point of failure (see Figure 2). Every network needs redundancy for enhanced reliability. The Network reliability is achieved through reliable equipment and network designs that are tolerant to failures and faults. [2]

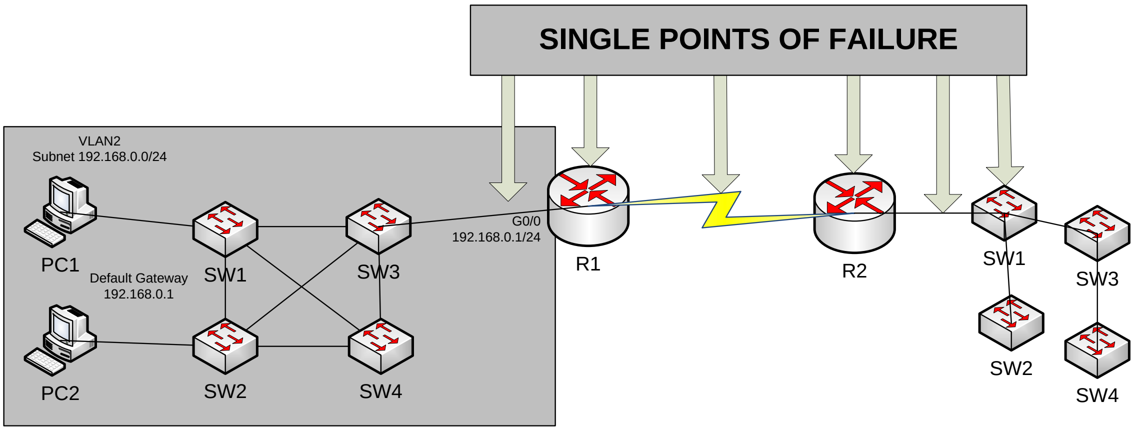


Figure 2. Single point of failure [1]

The figure notes several components as a single point of failure. If any one of the noted parts of the network fails, packets cannot flow from the left side of the network to the right. To improve the network and make it fully redundant the next step in higher availability for that remote site is to protect against those catastrophic routers and switch failures. In this particular design, adding one router on the left side and one to the right of the network in Figure 2 removes all the single points of failure that had been noted earlier. Figure 3 shows the design with a second router, which connects to a different LAN switch so that SW1 is also no longer a single point of failure. [1]

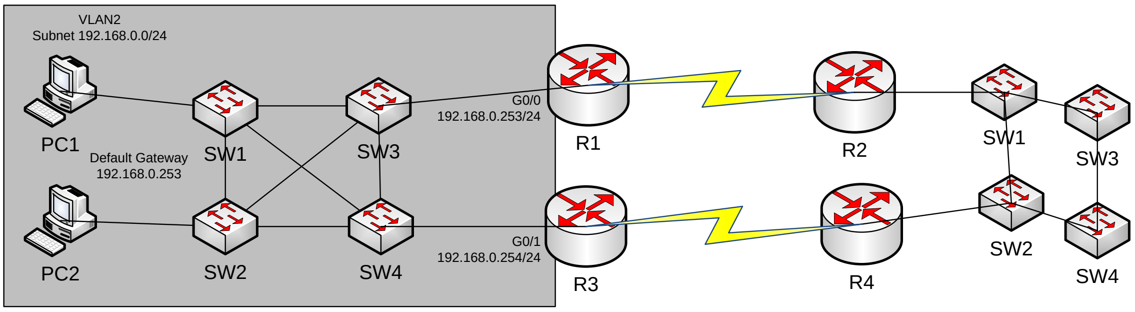


Figure 3. Redundant Network [1]

Of the designs shown so far in this chapter, only Figure 3's design has two routers on the LAN of the left side of the figure, specifically the same VLAN and subnet. While having the redundant routers on the same subnet helps, the network needs to use an FHRP when these redundant routers exist. [1]

To see the need and benefit of using an FHRP, first think about how these redundant routers could be used as default routers by the hosts in VLAN 2/subnet 192.168.0.0/24. The host logic will remain unchanged, so each host has a single default router setting. So, some design options for default router settings include the following:
• All hosts in the subnet use R1 (192.168.0.253) as their default router, and they statically reconfigure their default router setting to R3's 192.168.0.254 if R1 fails.
• All hosts in the subnet use R3 (192.168.0.254) as their default router, and they statically reconfigure their default router setting to R1's 192.168.0.253 if R3 fails.
• Half the hosts use R1, and half use R3, as default router, and if either router fails, that half of the users statically reconfigure their default router setting. [1] [2]

To make sure the concept is clear, Figure 4 shows this third option, with half the hosts using R1, and the other half using R3. The figure removes all the LAN switches just to uncluttered the figure. Hosts A and B use R1 as default router, and hosts C and D use R3 as default router. [1]

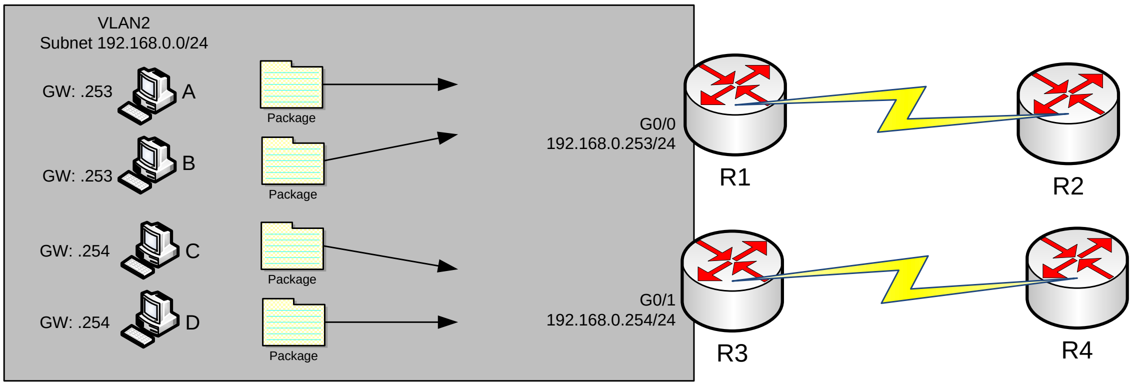


Figure 4. Balancing Traffic by Assigning Different Default Routers to Different Clients [1]

All of these options have a problem: The users have to take action. They have to know an outage occurred. They have to know how to reconfigure their default router setting. And they have to know when to change it back to the original setting. FHRPs make this design work better. The two routers appear to be a single default router. The users never have to do anything: Their default router setting remains the same, and their ARP table even remains the same. To allow the hosts to remain unchanged, the routers have to do some more work, as defined by one of the FHRP protocols. Generically, each FHRP makes the following happen:

1. All hosts act like they always have, with one default router setting that never has to change.

2. The default routers share a virtual IP address in the subnet, defined by the FHRP.
3. Hosts use the FHRP virtual IP address as their default router address.
4. The routers exchange FHRP protocol messages, so that both agree as to which router what works at any point in time.
5. When a router fails, or has some other problem, the routers use the FHRP to choose which router takes over responsibilities from the failed router. [1] [3]

1.3.2 The three solutions for First Hop Redundancy

The term First Hop Redundancy Protocol does not name any one protocol. Instead, it names a family of protocols that fill the same role. For a given network, like the left side of Figure 4, the engineer would pick one of the protocols from the FHRP family.

Cisco first introduced the proprietary Hot Standby Router Protocol (HSRP), and it worked well for many of their customers. Later, the IETF developed an RFC for a very similar protocol, Virtual Router Redundancy Protocol (VRRP). Finally, Cisco developed a more robust option, Gateway Load Balancing Protocol (GLBP). [1]

Acronym	**Full Name**	**Origin**	**Redundancy Approach**	**Load Balancing**
HSRP	Hot Standby Router Protocol	Cisco	Active/Standby	Per Subnet
VRRP	Virtual Router Redundancy Protocol	IETF (RFC 5798)	Active/Standby	Per Subnet
GLBP	Gateway Load Balancing Protocol	Cisco	Active/Active	Per Host

Table 1. List of the three FHRP Options **[3]**

2 Literature Review

2.1 Hot Standby Router Protocol (HSRP)

2.1.1 HSRP Background and Operations

The goal of the protocol is to allow hosts to appear to use a single router and to maintain connectivity even if the actual first hop router they are using fails. Multiple routers participate in this protocol and in concert create the illusion of a single virtual router. The protocol insures that one and only one of the routers is forwarding packets on behalf of the virtual router. End hosts forward their packets to the virtual router.

The router forwarding packets is known as the active router. A standby router is selected to replace the active router should it fail. The protocol provides a mechanism for determining active and standby routers, using the IP addresses on the participating routers. If an active router fails a standby router can take over without a major interruption in the host's connectivity. [3] [5]

- Definitions

Active Router the router that is currently forwarding packets for the virtual router.

Standby Router the primary backup router.

Standby Group the set of routers participating in HSRP that jointly emulate a virtual router.

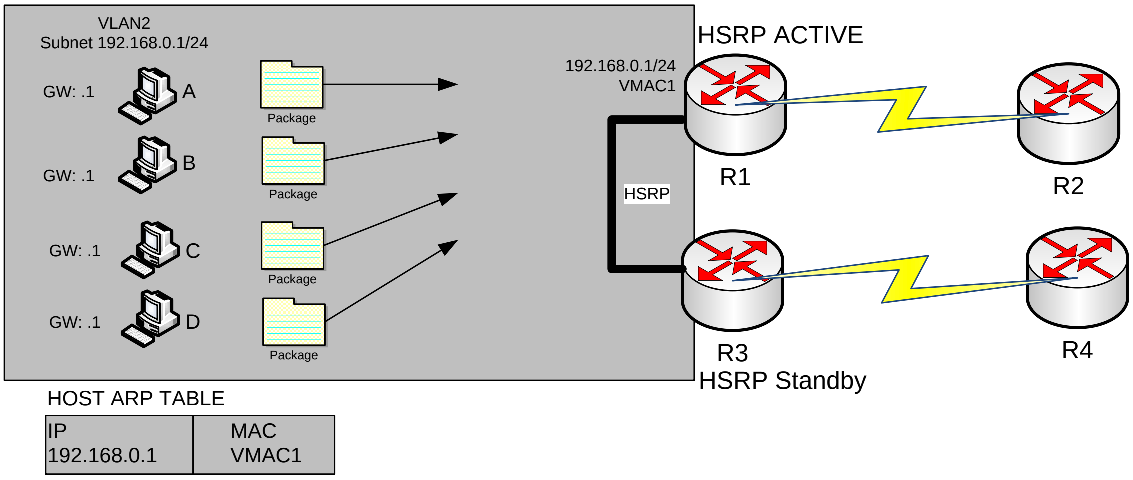
Hello Time the interval between successive HSRP Hello messages from a given router.

Hold Time the interval between the receipt of a Hello message and the presumption that the sending router has failed. [3]

HSRP operates with an active/standby model (also more generally called active/passive). HSRP allows two (or more) routers to cooperate, all being willing to act as the default router. However, at any one time, only one router actively supports the end-user traffic. The packets sent by hosts to their default router flow to that one active router. Then, the other routers, with an HSRP standby state, sit there patiently waiting to take over should the active HSRP router have a problem. [1] [6]

The HSRP active router implements a virtual IP address and matching virtual MAC address. This virtual IP address exists as part of the HSRP configuration, which is an additional configuration item compared to the usual IP address interface subcommand. This virtual IP address is in the same subnet as the interface IP address, but it is a different IP address. The router then automatically creates the virtual MAC address. All the cooperating HSRP routers know these virtual addresses, but only the HSRP active router uses these addresses at any one point in time. [6]

Hosts refer to the virtual IP address as their default router address, instead of any one router's interface IP address. For instance, in Figure 5, R1 and R3 use HSRP. The HSRP virtual IP address is 192.168.0.1, with the virtual MAC address referenced as VMAC1 for simplicity's sake. [1]



IP	MAC
192.168.0.1	VMAC1

Figure 5. All Traffic goes to 192.168.0.1 (R1, Which is Active); R3 is Standby [1]

HSRP on each router has some work to do to make the network function as shown in Figure 5. The two routers need HSRP configuration, including the virtual IP address. The two routers send HSRP messages to each other to negotiate and decide which router should currently be active, and which should be standby. Then, the two routers continue to send messages to each other so that the standby router knows when the active router fails so that it can take over as the new active router. Figure 6 shows the result when the R1, the HSRP active router in Figure 5, fails. R1 quits using the virtual IP and MAC address, while R3, the new active router, starts using these addresses. The hosts do not need to change their default router settings at all, with traffic now flowing to R3 instead of R1.

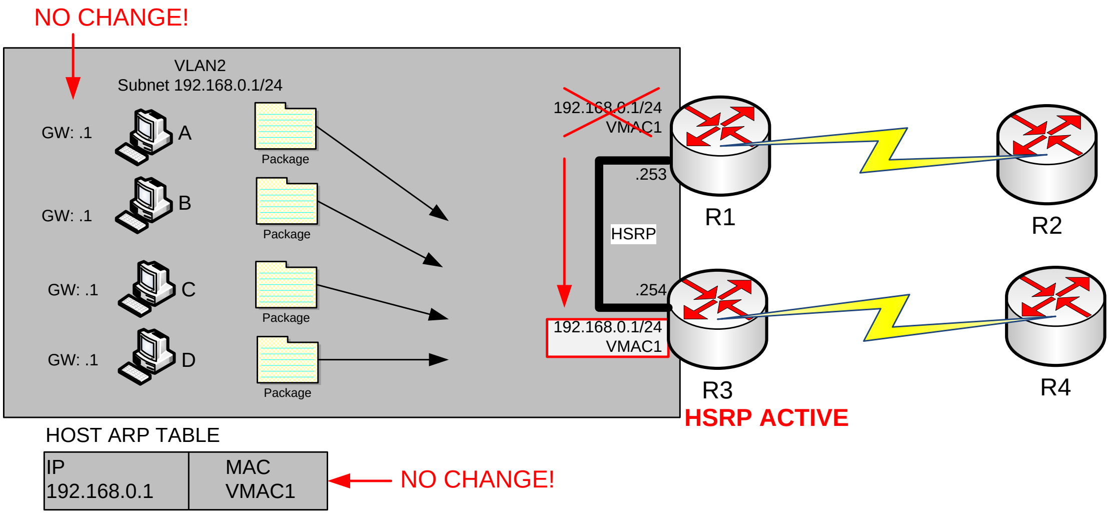


Figure 6. Packets Sent Through R3 (New Active) Once it Takes over for Failed R1 [1]

When the failover happens, some changes do happen, but none of those changes happen on the hosts. The host keeps the same default router setting, set to the virtual IP address (192.168.0.1 in this case). The host's ARP table does not have to change either, with the HSRP virtual MAC being listed as the MAC address of the virtual router.

When the failover occurs, changes happen on both the routers and the LAN switches. Clearly, the new active router has to be ready to receive packets (encapsulated inside frames) using the virtual IP and MAC addresses. However, the LAN switches, hidden in the last few figures, used to forward frames destined for VMAC1 to router R1. Now the switches must know to send the frames to the new active router, R3. [1]

2.1.2 Dynamic Router Discovery Mechanisms

Below are descriptions of dynamic router discovery mechanisms that are available to hosts. Many of these mechanisms don't provide the network resiliency required by network administrators. This may be because the protocol wasn't initially intended to provide network resiliency or because it isn't feasible for every host on a network to be running the protocol. In addition to what is listed below, it is important to note that many hosts only allow you to configure a default-gateway. [5] [2]

- Proxy Address Resolution Protocol

Some IP hosts use proxy Address Resolution Protocol (ARP) to select a router. When a host runs proxy ARP, it sends an ARP request for the IP address of the remote host it wants to contact. A router, Router A, on the network replies on behalf of the remote host and provides its own MAC address. With proxy ARP, the host behaves as if the remote host were connected to the same segment of the network. If Router A fails, the host continues to send packets destined for the remote host to the MAC address of Router A even though those packets have nowhere to go and are lost. You can either wait for ARP to acquire the MAC address of another router, Router B, on the local segment by sending another ARP request, or reboot the host to force it to send an ARP request. In either case, for a significant period of time, the host can't communicate with the remote host, even though the routing protocol has converged, and Router B is prepared to transfer packets that would otherwise go through Router A. [4]

- Dynamic Routing Protocol

Some IP hosts run (or snoop) a dynamic routing protocol such as the Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) to discover routers. The drawback of using RIP is that it is slow to adapt to changes in the topology. Running a dynamic routing protocol on every host may not be feasible for a number of reasons, including administrative overhead, processing overhead, security issues, or lack of a protocol implementation for some platforms. [4]

- ICMP Router Discovery Protocol

Some newer IP hosts use ICMP Router Discovery Protocol (IRDP) to find a new router when a route becomes unavailable. A host that runs IRDP listens for hello multicast messages from its configured router and uses an alternate router when it no longer receives those hello messages. The default timer values of IRDP mean that it's not suitable for detection of failure of the first hop. The default advertisement rate is once every 7 to 10 minutes, and the default lifetime is 30 minutes. [4]

- Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) provides a mechanism for passing configuration information to hosts on a TCP/IP network. A host that runs a DHCP client requests configuration information from a DHCP server when it boots onto the network. This configuration information typically comprises an IP address and a default gateway. There is no mechanism for switching to an alternative router if the default gateway fails. [6] [5]

2.1.3 HSRP Operation

A large class of legacy host implementations that don't support dynamic discovery are capable of configuring a default router. Running a dynamic router discovery mechanism on every host may not be feasible for a number of reasons, including administrative overhead, processing overhead, security issues, or lack of a protocol implementation for some platforms. HSRP provides failover services to these hosts. [2]

Using HSRP, a set of routers works 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. 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. Although an arbitrary number of routers may run HSRP, only the Active router forwards the packets sent to the virtual router. [1]

To minimize network traffic, only the Active and Standby routers send periodic HSRP messages once the protocol has completed the election process. If the Active router fails, the Standby router takes over as the Active router. If the Standby router fails or becomes the Active Router, then another router is elected as the Standby router. [1]

On a particular LAN, multiple hot standby groups may coexist and overlap. Each standby group emulates a single virtual router. The individual routers may participate in multiple groups. In this case, the router maintains separate state and timers for each group. [1]

Each standby group has a single, well-known MAC address, as well as an IP address. [6]

2.1.4 HSRP Addressing

In most cases when you configure routers to be part of an HSRP group, they listen for the HSRP MAC address for that group as well as their own burned-in MAC address. The exception is routers whose Ethernet controllers only recognize a single MAC address (for example, the Lance controller on the Cisco 2500 and Cisco 4500 routers). These routers use the HSRP MAC address when they are the Active Router and their burned-in address when they are not. [1]

HSRP uses the following MAC address on all media except Token Ring: 0000.0c07.ac** (where ** is the HSRP group number)
Token Ring interfaces use functional addresses for the HSRP MAC address. Functional addresses are the only general multicast mechanism available. There are a limited number of Token Ring functional addresses available and many of them are reserved for other functions. You can use the following three addresses with HSRP:

c000.0001.0000	(group 0)
c000.0002.0000	(group 1)
c000.0004.0000	(group 2)

Note: When HSRP runs in a multiple-ring source-route bridging (SRB) environment and the HSRP routers reside on different rings, using the functional addresses can cause Routing Information Field (RIF) confusion. For example, in an SRB environment, it is possible that an HSRP standby router resides on a different ring than the active router. When this standby router becomes active, stations on the same ring as the old active router need a new RIF in order to send packets to the new active router. However, since the standby (new active) router is using the same functional address as the previous active router the stations are not aware that they must send explorers for a new RIF. For this reason, the use-bia command was introduced. [2] [6]

2.1.5 HSRP Load Balancing

The active/standby model of HSRP means that in one subnet all hosts send their off-subnet packets through only one router. In other words, the routers do not share the workload, with one router handling all the packets. For instance, back in Figure 5, R1 was the active router, so all hosts in the subnet sent their packets through R1, and none of the hosts in the subnet sent their packets through R3. HSRP does support load balancing by preferring different routers to be the active router in different subnets. Most sites that require a second router for redundancy are also big enough to use several VLANs and subnets and the site. The two routers will likely connect to all the VLANs, acting as the default router in each VLAN. HSRP then can be configured to prefer one router as active in one VLAN and another router as active in another VLAN, balancing the traffic. [1] [5]

For instance, Figure 7 shows a redesigned LAN, now with two hosts in VLAN 1 and two hosts in VLAN 2. Both R1 and R2 connect to the LAN, and both use a VLAN trunking and router-on-a-stick (ROAS) configuration. Both routers use HSRP in each of the two subnets, supporting each other. However, on purpose, R1 has been configured so that it wins the negotiation to become HSRP active in VLAN 1, and R2 has been configured to win in VLAN 2.

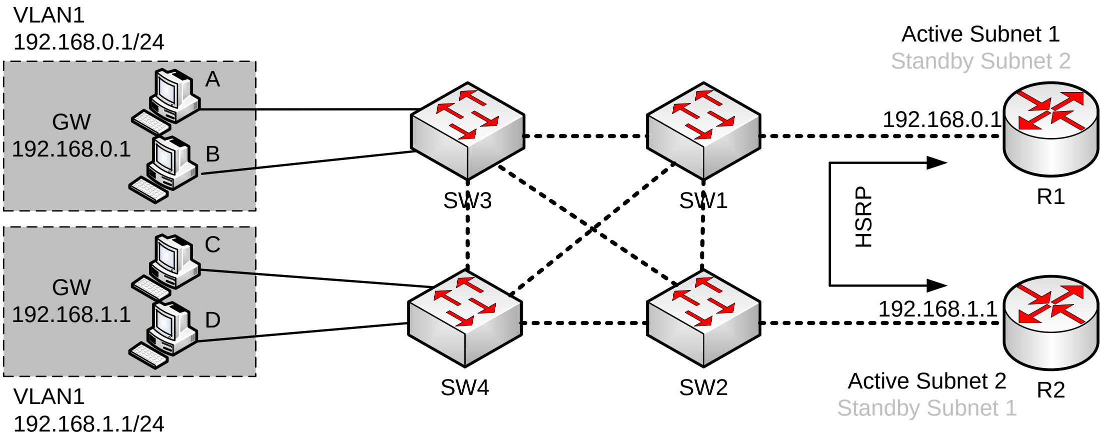


Figure 7. Load Balancing with HSRP by Using Different Active Routers per Subnet [1]

Note that by having each router act as the HSRP active router in some subnets, the design makes use of both routers and both WAN links. [1]

2.1.6 HSRP Features

- Preemption

The HSRP preemption feature enables the router with highest priority to immediately become the Active router. Priority is determined first by the priority value that you configure, and then by the IP address. In each case a higher value is of greater priority. When a higher priority router preempts a lower priority router, it sends a coup message. When a lower priority active router receives a coup message or hello message from a higher priority active router, it changes to the speak state and sends a resign message. [6]

- Preempt Delay

The preempt delay feature allows preemption to be delayed for a configurable time period, allowing the router to populate its routing table before becoming the active router. Before Cisco IOS Software release 12.0(9), the delay started when the router reloaded. In Cisco IOS release 12.0(9) the delay starts when preemption is first attempted. [6] [4]

To configure HSRP priority and preemption, use the standby [group] [priority number] [preempt [delay [minimum] seconds] [sync seconds]] command. [6]

2.1.7 Interface Tracking

Interface tracking allows you to specify another interface on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group. If the specified interface's line protocol goes down, the HSRP priority of this router is reduced, allowing another HSRP router with higher priority can become active (if it has preemption enabled). To configure HSRP interface tracking, use the standby [group] track interface [priority] command. When multiple tracked interfaces are down, the priority is reduced by a cumulative amount. If you explicitly set the decrement value, then the value is decreased by that amount if that interface is down, and decrements are cumulative. If you do not set an explicit decrement value, then the value is decreased by 10 for each interface that goes down, and decrements are cumulative.

The following example uses the following configuration, with the default decrement value of 10.

Note: When an HSRP group number is not specified, the default group number is group 0.

```
interface ethernet0
        ip address 10.1.1.1 255.255.255.0
        standby ip 10.1.1.3
        standby priority 110
        standby track serial0
        standby track serial1
```

The HSRP behavior with this configuration is:

- 0 interfaces down = no decrease (priority is 110)
- 1 interface down = decrease by 10 (priority becomes100)
- interfaces down = decrease by 10 (priority becomes 90)

The above HSRP behavior is true even if the decrement values are configured explicitly as below.

```
interface ethernet0
        ip address 10.1.1.1 255.255.255.0
        standby ip 10.1.1.3
        standby priority 110
        standby track serial0 10
        standby track serial1 10
```

Before Cisco IOS release 12.1, if you start a router with a down interface, HSRP interface tracking regards the interface as up.

This defect has Cisco bug ID CSCdp32289 (registered customers only). [6]

2.1.8 Configuring and Verifying HSRP

HSRP configuration requires only one command on the two (or more) routers that want to share default router responsibilities with HSRP: the **standby** *group* **ip** *virtual-ip* interface subcommand. The first value defines the HSRP group number, which must match on both routers. The group number lets one router support multiple HSRP groups at a time, and it allows the routers identify each other based on the group. The command also configures the virtual IP address shared by the routers in the same group.

Example 2.1.1 shows a configuration example, matching the HSRP examples related to Figures 5 and 6. Both routers use group 1, with virtual IP address 192.168.0.1, with the standby 1 ip 192.168.0.1 interface subcommand.

Example 2.1.1 of HSRP Configuration on R1 and R2, Sharing IP Address 192.168.0.1:

```
R1# show running-config
! Lines omitted for brevity
interface GigabitEthernet0/0
        ip address 192.168.0.253 255.255.255.0
        standby version 2
        standby 1 ip 192.168.0.1
        standby 1 priority 110
        standby 1 name HSRP-group-for-UBT
----------------------------------------------------------------------------------------
! The following configuration, on R2, is identical except for the priority,
! the interface IP address, and the HSRP priority
R2# show running-config
! Lines omitted for brevity
        interface GigabitEthernet0/0
        ip address 192.168.0.254 255.255.255.0
        standby version 2
        standby 1 ip 192.168.0.1
        standby 1 name HSRP-group-for-UBT
```

The configuration shows other optional parameters, as well. For instance, R1 has a priority of 110 in this group, and R2 defaults to 100. With HSRP, if the two routers are brought up at the same time, the router with the higher priority wins the election to become the active router. The configuration also shows a name that can be assigned to the group (when using show commands) and a choice to use HSRP Version 2. Once configured, the two routers negotiate the HSRP settings and choose which router will currently be active and which will be standby. With the configuration as shown, R1 will win the election and become active because of its higher (better) priority. Both routers reach the same conclusion, as confirmed with the output of the show standby brief command on both R1 and R2 in Example 2.1.2 [1]

Example 2.1.2 HSRP Status on R1 and R2 with show standby brief

```
! First, the group status as seen from R1
R1# show standby brief
                         P indicates configured to preempt.
                         |
Interface    Grp    Pri    P  State      Active        Standby        Virtual IP
Gi0/0        1      110       Active      local        192.168.0.254  192.168.0.1
```

```
! The output here on R2 shows that R2 agrees with R1.
R2# show standby brief
                        P indicates configured to preempt.
                        |
Interface    Grp    Pri    P  State      Active         Standby       Virtual IP
Gi0/0        1      100       Standby    192.168.0.253  local         192.168.0.1
```

First, look at the Grp column for each command. This lists the HSRP group number, so when looking at output from multiple routers, you need to look at the lines with the same group number to make sure
the data relates to that one HSRP group. In this case, both routers have only one group number (1), so it is easy to find the information.
Each line of output lists the local router's view of the HSRP status for that group. In particular, based on the headings, the show standby brief command identifies the following: [1] [8]

Interface: The local router's interface on which the HSRP group is configured
Grp: The HSRP group number
Pri: The local router's HSRP priority
State: The local router's current HSRP state
Active: The interface IP address of the currently-active HSRP router (or "local" if the local router is HSRP active)

Standby: The interface IP address of the currently-standby HSRP router (or “local” if the local router is HSRP standby)

Virtual IP: The virtual IP address defined by this group [4] [1]

For instance, following the highlighted text in Example 2.1.2, R2 believes that its own current state is standby, that the router with interface address 192.168.0.253 is active, with a confirmation that the “local” router (R2, on which this command was issued) is the standby router. [1] [3]
As you can see, the **show standby brief** command actually packs a lot of detail in a single line of output. In comparison, the **show standby** command lists a more detailed description of the current state, while repeating many of the facts from the **show standby brief** command. Example 2.1.3 shows an example of the new information with the **show standby** command, listing several counters and timers about the HSRP protocol itself, plus the virtual MAC address 0000.0c9f.f001.

Example 2.1.3 HSRP Status on R1 and R2 with show standby

```
R1# show standby
GigabitEthernet0/0 - Group 1 (version 2)
        State is Active
                6 state changes, last state change 00:12:53
        Virtual IP address is 192.168.0.1
        Active virtual MAC address is 0000.0c9f.f001
                Local virtual MAC address is 0000.0c9f.f001 (v2 default)
        Hello time 3 sec, hold time 10 sec
                Next hello sent in 1.696 secs
        Preemption disabled
        Active router is local
        Standby router is 192.168.0.254, priority 100 (expires in 8.096 sec)
        Priority 110 (configured 110)
        Group name is "HSRP-group-for-UBT" (cfgd)

--------------------------------------------------------------------------------

! The output here on R2 shows that R2 agrees with R1.
R2# show standby
GigabitEthernet0/0 - Group 1 (version 2)
        State is Standby
                4 state changes, last state change 00:12:05
        Virtual IP address is 192.168.0.1
        Active virtual MAC address is 0000.0c9f.f001
                Local virtual MAC address is 0000.0c9f.f001 (v2 default)
        Hello time 3 sec, hold time 10 sec
                Next hello sent in 0.352 secs
        Preemption disabled
```

```
    Active router is 192.168.0.253, priority 110 (expires in 9.136 sec)
    MAC address is 0200.0101.0101
    Standby router is local
    Priority 100 (default 100)
  Group name is "HSRP-group-for-UBT" (cfgd)
```

2.2 Gateway Load Balancing Protocol

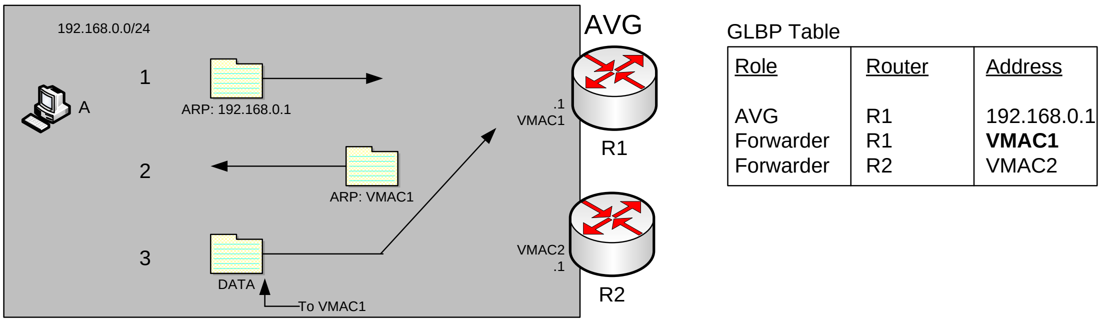
2.2.1 GLBP Concepts

HSRP and VRRP, which were introduced before Gateway Load Balancing Protocol (GLBP), balanced the packet load per subnet, as shown in Figure 7. However, because traffic loads vary unpredictably from subnet to subnet, Cisco wanted an FHRP option with better load-balancing options than just the per-subnet load balancing of HSRP and VRRP. To meet that need, Cisco introduced GLBP.

GLBP balances the packet load per host by using an active/active model in each subnet. Each GLBP router in a subnet receives off-subnet packets from some of the hosts in the subnet. Each host still remains unaware of the FHRP, allowing the hosts to configure the same default gateway/router setting and for the hosts to make no changes when a router fails. GLBP creates a world that at first glance looks like HSRP, but with a few twists that let GLBP balance the traffic. Like HSRP, all the routers configure a virtual IP address, which is the IP address used by hosts as their default router. Like with HSRP, hosts use a default router setting that points to the virtual IP address, and that setting does not need to change. GLBP differs from HSRP with regard to the MAC addresses it uses and the ARP process, because GLBP actually uses ARP Reply messages to balance traffic from different hosts through different routers.

With GLBP, one router acts in a special role called the active virtual gateway (AVG). The AVG replies to all ARP requests for the virtual IP address. Each router has a unique virtual MAC address so that the AVG can reply to some ARP Requests with one virtual MAC and some with the other. As a result, some hosts in the subnet send frames to the Ethernet MAC address of one of the routers, with other hosts sending their frames to the MAC address of the second router.

As an example, Figure 8 shows the process by which a GLBP balances traffic for host A based on the Address Resolution Protocol (ARP) Reply sent by the AVG (R1). The figure uses the same IP addresses as earlier HSRP examples with Figures 5 and 6. The two routers support virtual IP address 192.168.0.1, with the hosts using that address as their default router setting. [1]



GLBP Table

Role	Router	Address
AVG	R1	192.168.0.1
Forwarder	R1	**VMAC1**
Forwarder	R2	VMAC2

Figure 8. GLBP Directs Host A by Sending Back ARP Reply with R1's MAC1 [3]

The figure shows three messages, top to bottom, with the following action:

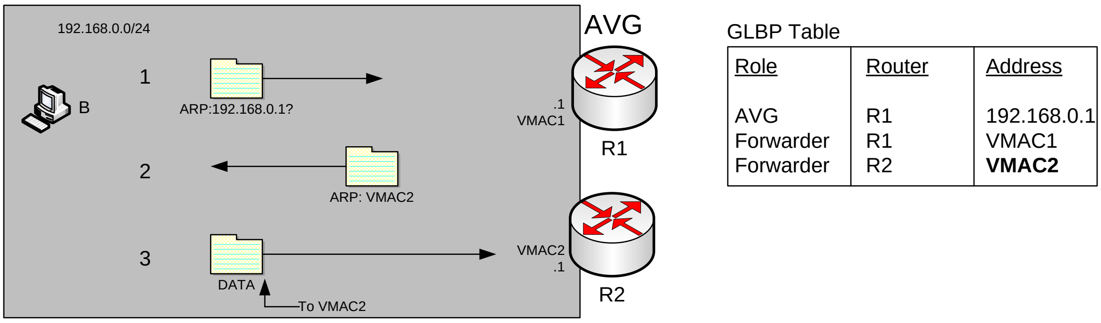
1. Host A has no ARP table entry for its default router, 192.168.0.1, so host A sends an ARP Request to learn 192.168.0.1's MAC address.

2. The GLBP AVG, R1 in this case, sends back an ARP Reply. The AVG chooses to include its own virtual MAC address in the ARP Reply, VMAC1.

3. Future IP packets sent by host A are encapsulated in Ethernet frames, destined to VMAC1, so that they arrive at R1.

From now on, host A sends off-subnet packets to R1 due to host A's ARP table entry for its default gateway (192.168.0.1). Host A's ARP table entry for 192.168.0.1 now refers to a MAC address on R1 (VMAC1), so packets host A sends off-subnet flow through R1.

To balance the load, the AVG answers each new ARP Request with the MAC addresses of alternating routers. Figure 9 continues the load-balancing effect with the ARP Request for 192.168.0.1 coming from host B. The router acting as AVG (R1) still sends the ARP Reply, but this time with R2's virtual MAC (VMAC2). [1] [3]



GLBP Table

Role	Router	Address
AVG	R1	192.168.0.1
Forwarder	R1	VMAC1
Forwarder	R2	**VMAC2**

Figure 9. GLBP Directs Host B by Sending Back ARP Reply with R2's VMAC2 [3]

Here are the steps in the figure:

1. Host B sends an ARP Request to learn 192.168.0.1's MAC address.

2. The GLBP AVG (R1) sends back an ARP Reply, listing VMAC2, R2's virtual MAC address.

3. For future packets sent off-subnet, host B encapsulates the packets in Ethernet frames, destined to VMAC2, so that they arrive at R2.

The process shown in Figures 8 and 9 balances the traffic, per host, but the routers must also be ready to take over for the other router if it fails. GLBP refers to each router as a forwarder. When all is well, each router acts as forwarder for their own virtual MAC address, but it listens to GLBP messages to make sure the other forwarders are still working. If another forwarder fails, the still working forwarder takes over the failed forwarder's virtual MAC address role and continues to forward traffic. [6] [1]

2.2.2 Configuring and Verifying GLBP

GLBP configuration mimics HSRP configuration to a great degree. In fact, if you took the configuration in Example 2.1.1, removed the standby version 2 command (which applies only to HSRP) and replaced each standby with glbp, the result would be a completely valid GLBP configuration.

GLBP requires only a single interface subcommand on each router: the glbp group ip virtual-ip interface subcommand. The ideas behind this one command work just like HSRP as well: All routers use the same group number, and all routers configure the same virtual IP address.

Example 2.2.1 shows a GLBP configuration that would be typical if migrating from using HSRP, as shown in Example 2.1.1, to the equivalent GLBP configuration. Both routers use GLBP group 1, with virtual IP address 192.168.0.1, with the **glbp 1 ip 192.168.0.1** interface subcommand. [1] [6]

Example 2.2.1. GLBP Configuration on R1 and R2, Sharing IP Address 192.168.0.1

```
! First, the configuration on R1
R1# show running-config
! Lines omitted for brevity
interface GigabitEthernet0/0
        ip address 192.168.0.253 255.255.255.0
        glbp 1 ip 192.168.0.1
        glbp 1 priority 110
        glbp 1 name GLBP-group-for-UBT
-----------------------------------------------------
! The following configuration, on R2, is identical except for
! the interface IP address, and the GLBP priority
R2# show running-config
! Lines omitted for brevity
interface GigabitEthernet0/0
      ip address 192.168.0.254 255.255.255.0
      glbp 1 ip 192.168.0.1
      glbp 1 name HSRP-group-for-UBT
```

Once configured, the two routers negotiate as to which will be the AVG. As with HSRP, if both come up at the same time, R1 will win, with a priority set to 110 with the glbp 1 priority 110 command versus R2's default priority of 100. However, if either router comes up before the other, that router goes ahead and takes on the AVG role.

Sifting through the GLBP show command output takes a little more work with HSRP, in particular because of the added detail in how GLBP works. First, consider the show glbp brief command on router R1, as shown in Example 2.2.2. (Note that many show glbp commands have the same options as equivalent HSRP show standby commands.) [1]

Example 2.2.2. GLBP Status on R1 with show glbp brief

```
R1# show glbp brief
Interface   Grp Fwd  Pri   State    Address          Active router   Standby router
Gi0/0        1   -   110  Active   192.168.0.1          local        192.168.0.254
Gi0/0        1   1    -   Listen   0007.b400.0101   192.168.0.254          -
Gi0/0        1   2    -   Active   0007.b400.0102       local              -
```

Before looking at the right side of the output, first consider the context for a moment. This example lists a heading line and three rows of data. These rows data rows are identified by the Grp and Fwd headings, short for Group and Forwarder. With only one GLBP group configured, R1 lists lines only for group 1. More important, each row defines details about a different part of what GLBP does, as follows:

Fwd is -: This line refers to none of the forwarders, and instead describes the AVG.

Fwd is 1: This line describes GLBP forwarder (router) 1.

Fwd is 2: This line describes GLBP forwarder (router) 2.

The output usually lists the line about the AVG first, as noted with a dash in the Forwarder column.

Now looking at the highlighted portions on the right of Example 2.2.2. This line will list the virtual IP address and identify the active AVG and the standby AVG. This particular command, from router R1, lists R1 itself (“local”) as the active router. So, R1 is the current AVG.

Each of the next two lines lists status information about one of the forwarder roles; that is, a router that uses a virtual MAC address, receives frames sent to that address, and routes the packets encapsulated in those frames. To that end, the Address column lists MAC addresses, specifically the virtual MAC addresses used by GLBP, and not the interface MAC addresses.

Each forwarder row also identifies the router that currently uses the listed virtual MAC in the Active Router column. In Example 2.2.2, 0007.b400.0101 is used by the router with interface IP address 192.168.0.254 (which happens to be R2). 0007.b400.0102 is supported by the local router (the router on which the show command was issued), which is R1.

The brief output of the show glbp brief lists many details, but with some effort to learn how to sift through it all. For more perspective on the output, Example 2.2.3 lists this same show glbp brief command, this time on R2. Note that the Fwd column again identifies the first line of output as being about the AVG, with the next two lines about the two forwarders. [1]

Example 2.2.3. GLBP Status on R2 with show standby brief

```
R1# show glbp brief
Interface  Grp Fwd  Pri   State     Address         Active router   Standby router
Gi0/0       1   -   100  Standby   192.168.0.1     192.168.0.253      local
Gi0/0       1   1    -   Active    0007.b400.0101       local            -
Gi0/0       1   2    -   Listen    0007.b400.0102  192.168.0.253         -
```

Take a moment to compare the output in Example 2.2.3 to Example 2.2.2, focusing on the State column. This column lists the local router’s state. In other words, the command in Example 2.2.3, taken from R2, lists R2’s state for each item. Comparing these two column gives some great insight into linking the concepts behind GLBP to the details in the show command output. The key concepts are as follows:

AVG: One router should be the active AVG, with the other acting as standby, ready to take over the AVG role if the AVG fails.

Each forwarder: One router should be active, while the other should be listening, ready to take over that virtual MAC address if that forwarder fails.

Table 2 collects the values of the State column from Example 2.2.2 and 2.2.3 for easier reference side by side. Note that, indeed, each line has either an active/standby pair (for the AVG) or an active/listen pair (for the forwarder function). [6] [1]

Row is about…	Fwd column value	R1 State	R2 State
AVG	-	Active	Standby
Forwarder 1	1	Listen	Active
Forwarder 2	2	Active	Listen

Table 2. Comparing Local State in ***show glbp brief*** *Commands* **[2]**

Finally, the show glbp command lists a more detailed view of the current GLBP status. Example 2.2.4 shows a sample from router R1. Note that the first half of the output has similar informtion compared to HSRP’s show standby command, plus it lists the IP and MAC addresss of the routers in the GLBP group. Then, the end of the output lists a group of messages per GLBP forwarder.

Example 2.2.4. GLBP Status on R1 with show glbp

```
R1# show glbp
GigabitEthernet0/0 - Group 1
     State is Active
        2 state changes, last state change 00:20:59
     Virtual IP address is 192.168.0.1
     Hello time 3 sec, hold time 10 sec
        Next hello sent in 2.112 secs
Redirect time 600 sec, forwarder timeout 14400 sec
Preemption disabled
Active is local
Standby is 192.168.0.254, priority 100 (expires in 8.256 sec)
Priority 110 (configured)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
IP redundancy name is "GLBP-group-for-book"
Group members:
     0200.0101.0101 (192.168.0.253) local
     0200.0202.0202 (192.168.0.254)
There are 2 forwarders (1 active)
Forwarder 1
     State is Listen
```

```
       2 state changes, last state change 00:20:34
    MAC address is 0007.b400.0101 (learnt)
    Owner ID is 0200.0202.0202
    Redirection enabled, 598.272 sec remaining (maximum 600 sec)
    Time to live: 14398.272 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.0.254 (primary), weighting 100 (expires in 8.352 sec)
    Client selection count: 1
Forwarder 2
    State is Active
       1 state change, last state change 00:24:25
    MAC address is 0007.b400.0102 (default)
    Owner ID is 0200.0101.0101
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
    Client selection count: 1
```

2.3 Virtual Router Redundancy Protocol

2.3.1 Introduction

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 (or snooping) a dynamic routing protocol such as Routing Information Protocol (RIP) or OSPF version 2, running an ICMP router discovery client 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. [3] [4] 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. [4]
The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

VRRP provides a function similar to the proprietary protocols "Hot Standby Router Protocol (HSRP)" and "IP Standby Protocol". [3] [1]

2.3.2 VRRP Operation

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

Proxy ARP - The client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router will respond to the ARP request with its own MAC address.

Routing protocol - The client listens to dynamic routing protocol updates (for example, from Routing Information Protocol) and forms its own routing table.

ICMP Router Discovery Protocol (IRDP) client - The client runs an Internet Control Message Protocol (ICMP) router discovery client.

The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow. [8] [1] [3]
An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network. [4]

VRRP can solve the static configuration problem. VRRP enables a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group. [4]

VRRP is supported on Ethernet, Fast Ethernet, BVI, and Gigabit Ethernet interfaces, and on MPLS VPNs, VRF-aware MPLS VPNs, and VLANs.

The figure below shows a LAN topology in which VRRP is configured. In this example, Routers A, B, and C are VRRP routers (routers running VRRP) that comprise a virtual router. The IP address of the virtual router is the same as that configured for the Ethernet interface of Router A (192.168.0.1). [8]

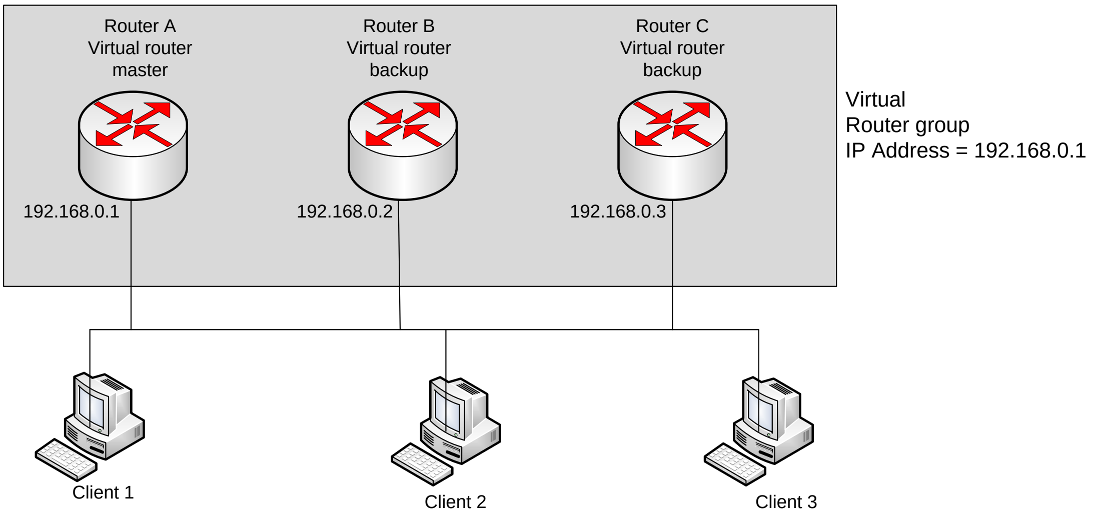


Figure 10. Basic VRRP topology [4]

Because the virtual router uses the IP address of the physical Ethernet interface of Router A, Router A assumes the role of the virtual router master and is also known as the IP address owner. As the virtual router master, Router A controls the IP address of the virtual router and is responsible for forwarding packets sent to this IP address. Clients 1 through 3 are configured with the default gateway IP address of 192.168.0.1. Routers B and C function as virtual router backups. If the virtual router master fails, the router configured with the higher priority will become the virtual router master and provide uninterrupted service for the LAN hosts. When Router A recovers, it becomes the virtual router master again. For more detail on the roles that VRRP routers play and what happens if the virtual router master fails, see the VRRP Router Priority and Preemption section.

The figure below shows a LAN topology in which VRRP is configured so that Routers

A and B share the traffic to and from clients 1 through 4 and that Routers A and B act as virtual router backups to each other if either router fails. [6] [8]

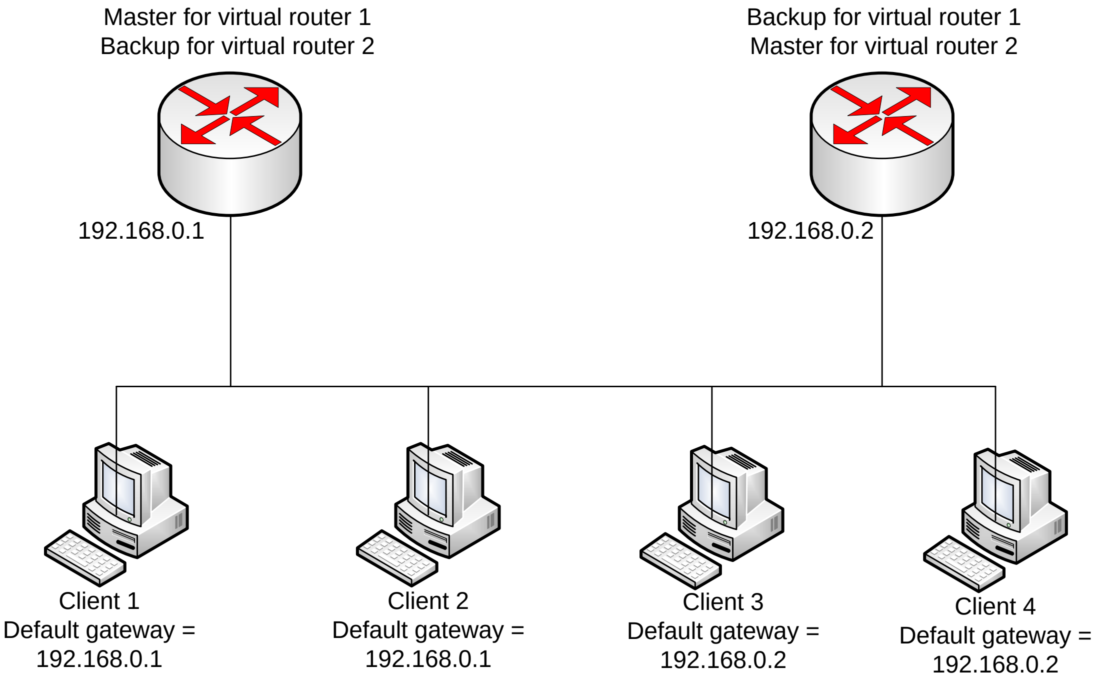


Figure 11. Load Sharing and Redundancy VRRP Topology [8]

In this topology, two virtual routers are configured. For virtual router 1, Router A is the owner of IP address 192.168.0.1 and virtual router master, and Router B is the virtual router backup to Router A. Clients 1 and 2 are configured with the default gateway IP address of 192.168.0.1.
For virtual router 2, Router B is the owner of IP address 192.168.0.2 and virtual router master, and Router A is the virtual router backup to Router B. Clients 3 and 4 are configured with the default gateway IP address of 192.168.0.2. [8]

2.3.3 VRRP Benefits

Redundancy

VRRP enables you to configure multiple routers as the default gateway router, which reduces the possibility of a single point of failure in a network.

Load Sharing

You can configure VRRP in such a way that traffic to and from LAN clients can be shared by multiple routers, thereby sharing the traffic load more equitably among available routers.

Multiple Virtual Routers

VRRP supports up to 255 virtual routers (VRRP groups) on a router physical interface, subject to the platform supporting multiple MAC addresses. Multiple virtual router support enables you to implement redundancy and load sharing in your LAN topology.

Multiple IP Addresses

The virtual router can manage multiple IP addresses, including secondary IP addresses. Therefore, if you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.

Preemption

The redundancy scheme of VRRP enables you to preempt a virtual router backup that has taken over for a failing virtual router master with a higher priority virtual router backup that has become available.

Authentication

VRRP message digest 5 (MD5) algorithm authentication protects against VRRP-spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

Advertisement Protocol

VRRP uses a dedicated Internet Assigned Numbers Authority (IANA) standard multicast address (224.0.0.18) for VRRP advertisements. This addressing scheme minimizes the number of routers that must service the multicasts and allows test equipment to accurately identify VRRP packets on a segment. The IANA assigned VRRP the IP protocol number 112.

VRRP Object Tracking

VRRP object tracking provides a way to ensure the best VRRP router is the virtual router master for the group by altering VRRP priorities to the status of tracked objects such as the interface or IP route states. [3] [6]

2.3.4 VRRP Router Priority and Preemption

An important aspect of the VRRP redundancy scheme is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the virtual router master fails.

If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router will function as a virtual router master.

Priority also determines if a VRRP router functions as a virtual router backup and the order of ascendancy to becoming a virtual router master if the virtual router master fails.

You can configure the priority of each virtual router backup with a value of 1 through 254 using the vrrp priority command.

For example, if Router A, the virtual router master in a LAN topology, fails, an election process takes place to determine if virtual router backups B or C should take over. If Routers B and C are configured with the priorities of 101 and 100, respectively, Router B is elected to become virtual router master because it has the higher priority. If Routers B and C are both configured with the priority of 100, the virtual router backup with the higher IP address is elected to become the virtual router master.

By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become virtual router master. You can disable this preemptive scheme using the no vrrp preempt command. If preemption is disabled, the virtual router backup that is elected to become virtual router master remains the master until the original virtual router master recovers and becomes master again. [4] [8]

2.3.5 VRRP Advertisements

The virtual router master sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the virtual router master. The VRRP advertisements are encapsulated in IP packets and sent to the IP Version 4 multicast address assigned to the VRRP group. The advertisements are sent every second by default; the interval is configurable. [4]

Although the VRRP protocol as per RFC 3768 does not support millisecond timers, Cisco routers allow you to configure millisecond timers. You need to manually configure the millisecond timer values on both the primary and the backup routers. The master advertisement value displayed in the show vrrp command output on the backup routers is always 1 second because the packets on the backup routers do not accept millisecond values.

You must use millisecond timers where absolutely necessary and with careful consideration and testing. Millisecond values work only under favorable circumstances, and you must be aware that the use of the millisecond timer values restricts VRRP operation to Cisco devices only. [4] [3]

2.3.6 VRRP Object Tracking

Object tracking is an independent process that manages creating, monitoring, and removing tracked objects such as the state of the line protocol of an interface. Clients such as the Hot Standby Router Protocol (HSRP), Gateway Load Balancing Protocol (GLBP), and VRRP register their interest with specific tracked objects and act when the state of an object changes. [4]

Each tracked object is identified by a unique number that is specified on the tracking CLI. Client processes such as VRRP use this number to track a specific object. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to interested client processes, either immediately or after a specified delay. The object values are reported as either up or down. [4]

VRRP object tracking gives VRRP access to all the objects available through the tracking process. The tracking process allows you to track individual objects such as a the state of an interface line protocol, state of an IP route, or the reach ability of a route. VRRP provides an interface to the tracking process. Each VRRP group can track multiple objects that may affect the priority of the VRRP router. You specify the object number to be tracked and VRRP is notified of any change to the object. VRRP increments (or decrements) the priority of the virtual router based on the state of the object being tracked. [4] [1] [3]

2.3.7 How VRRP Object Tracking Affects the Priority of a Device

The priority of a device can change dynamically if it has been configured for object tracking and the object that is being tracked goes down. The tracking process periodically polls the tracked objects and notes any change of value. The changes in the tracked object are communicated to VRRP, either immediately or after a specified delay. The object values are reported as either up or down. Examples of objects that can be tracked are the line protocol state of an interface or the reach ability of an IP route. If the specified object goes down, the VRRP priority is reduced. The VRRP router with the higher priority can now become the virtual router master if it has the vrrp preempt command configured. See the “VRRP Object Tracking” section for more information on object tracking. [4]

3 METHODOLOGY

For the research of this thesis, the case study methodology is most suited methodology. The information gathering phase of the case studies will be completed through document study and a literature review.

The main part of the research for the thesis will be based on the Case Study. In the thesis we have also used comparatives methodology for the purpose of analyzing the redundancy protocols.

Extensive secondary research will be conducted. Acknowledged texts, standards documents, industry periodicals and white papers, analysts’ reports and conference journals will be referenced.

4 CASE STUDY

Level 3 Telecommunication Company as a leading company in the world is seeking for small Telecom Companies to join them.

As part of our study was integrating a RIP (Routing Protocol) using company to the Level 3 OSPF network, which was recently bought by Level 3. After integrating the small company in Level 3 OSPF network, the board decided to add an additional link to the ISP to have a more stable and reliable network. To execute the request, Level 3 we decided on using a layer three redundancy protocol. To know which the best choice was, they had to run some tests.

Below there is a logical diagram of the project.

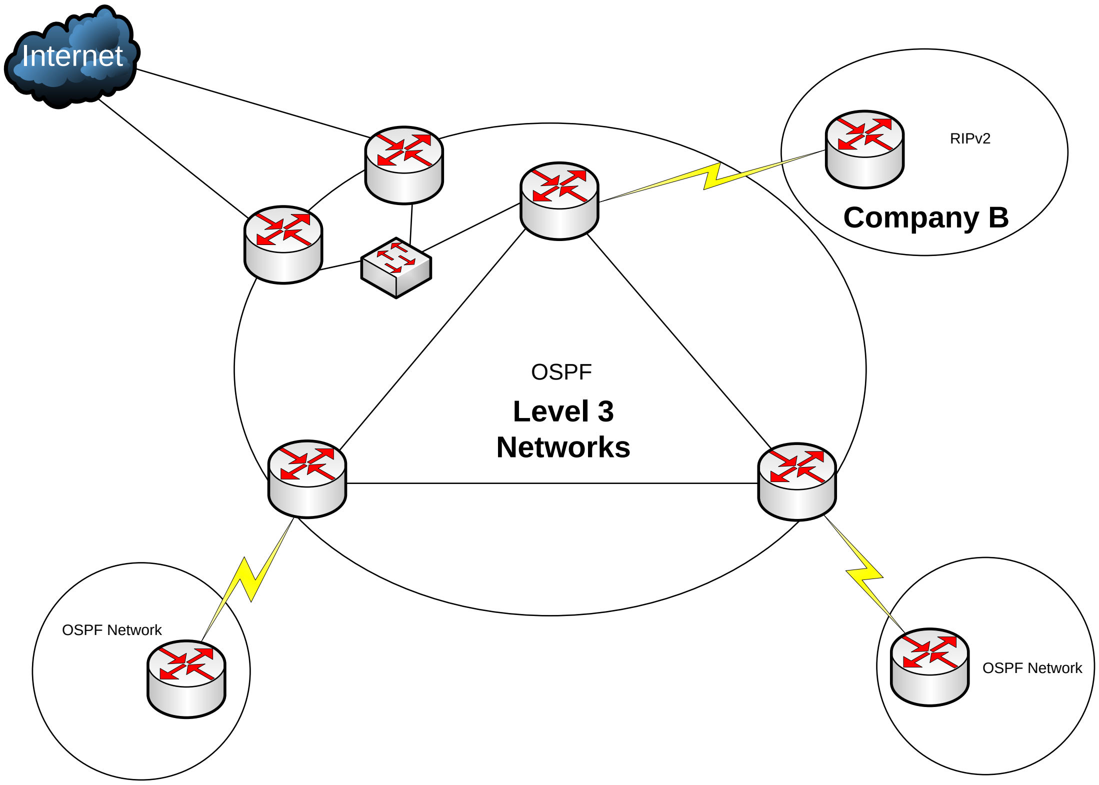


Figure 122. Adding redundancy protocols to the network

5 EXPERIMENTAL DESIGN

Based on our Case study, we tested all three redundancy protocols and their features.

5.1 Experimental Setup A (HSRP)

Diagram below explains the connection to the internet, using HSRP redundancy protocol. Routers L3PR_L1 and L3PR_L2 are configured to use HSRP and they are acting as one router with Virtual IP address 192.168.0.1.

The IP addresses configured on interfaces of the Link routers are:

L3PR_L1:	192.168.0.253/24
L3PR_L2:	192.168.0.254/24

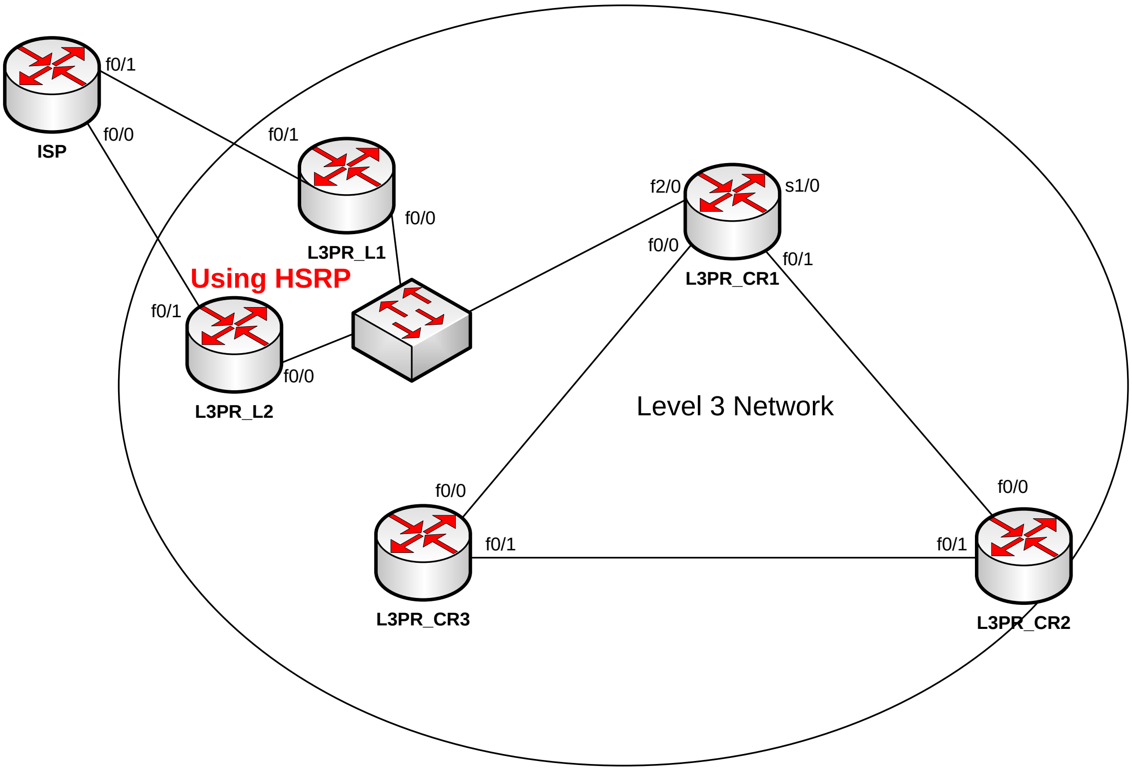


Figure 133. HSRP using network

5.2 Experimental Setup B (GLBP)

Diagram below explains the connection to the internet, using GLBP redundancy protocol.
Routers L3PR_L1 and L3PR_L2 are configured to use GLBP and they are acting as one router with Virtual IP address 192.168.0.1.

The IP addresses configured on interfaces of the Link routers are:

L3PR_L1:	192.168.0.253/24
L3PR_L2:	192.168.0.254/24

GLBP does also load balancing.

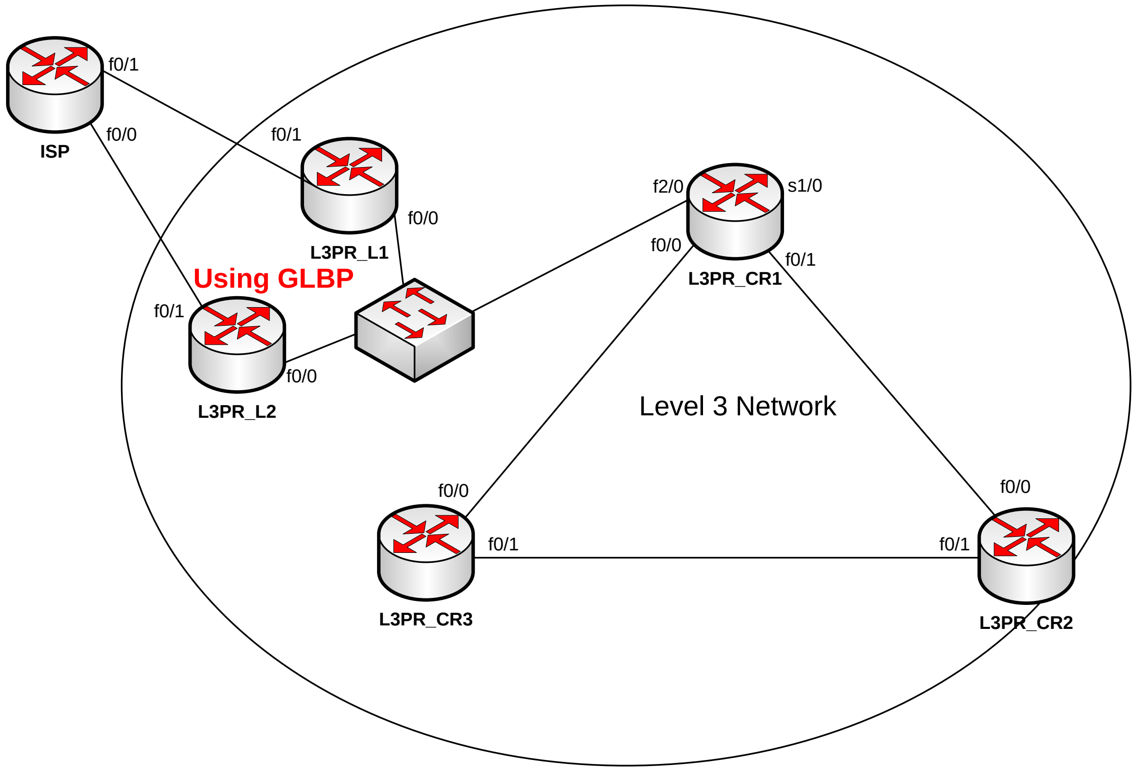


Figure 144. GLBP using network

5.3 Experimental Setup C (VRRP)

Diagram below explains the connection to the internet, using VRRP redundancy protocol.
Routers L3PR_L1 and L3PR_L2 are configured to use VRRP and they are acting as one router with Virtual IP address 192.168.0.1.

The IP addresses configured on interfaces of the Link routers are:

L3PR_L1:	192.168.0.253/24
L3PR_L2:	192.168.0.254/24

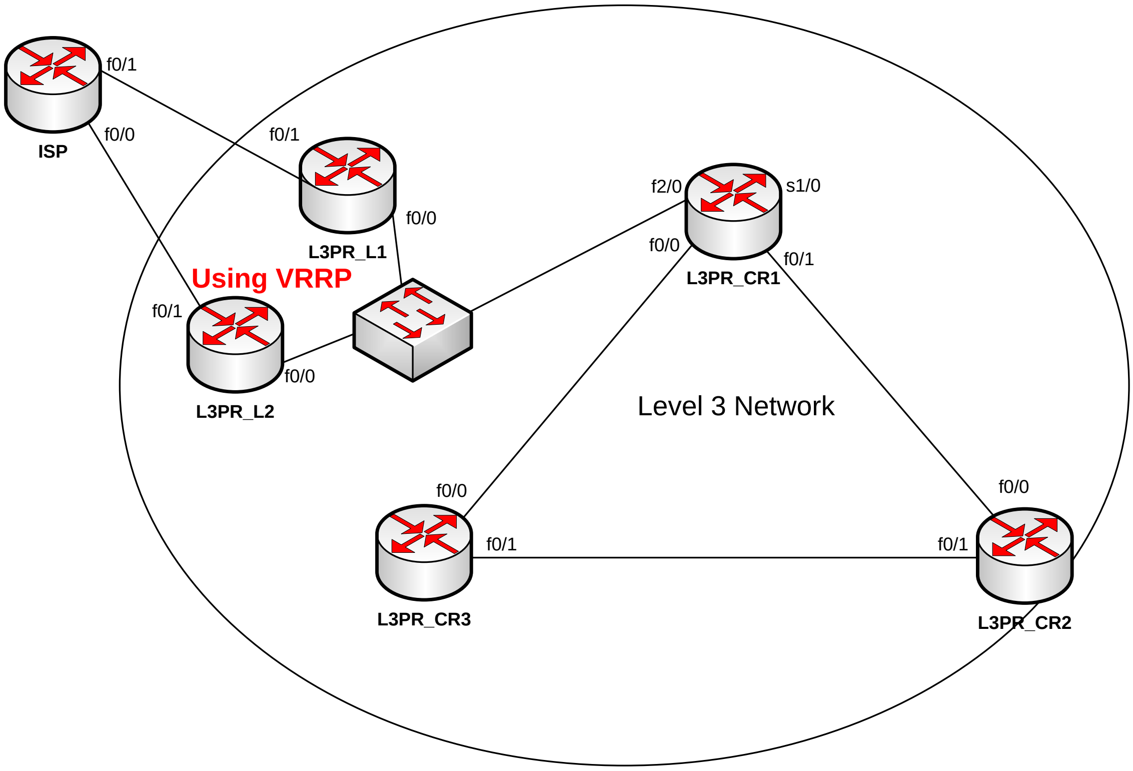


Figure 155. VRRP using network

6 RESULTS

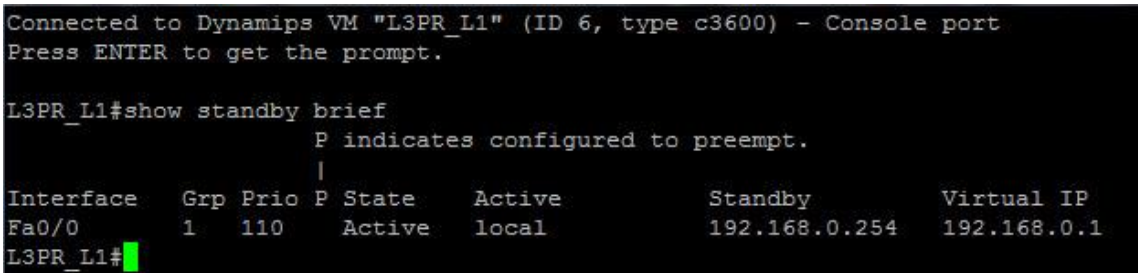
After describing all the protocols of First Hop Redundancy Protocols, I come to issues present. This Issue discussion is presented as conclusion to the review conducted in this thesis.

HSRP protocol does not provide security. The authentication field found within the message is useful for preventing misconfiguration. The protocol is easily subverted by an active intruder on the LAN. This can result in a packet black hole and a denial-of-service attack. It is difficult to subvert the protocol from outside the LAN as most routers will not forward packets addressed to the all-routers multicast address (224.0.0.2). [3]

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

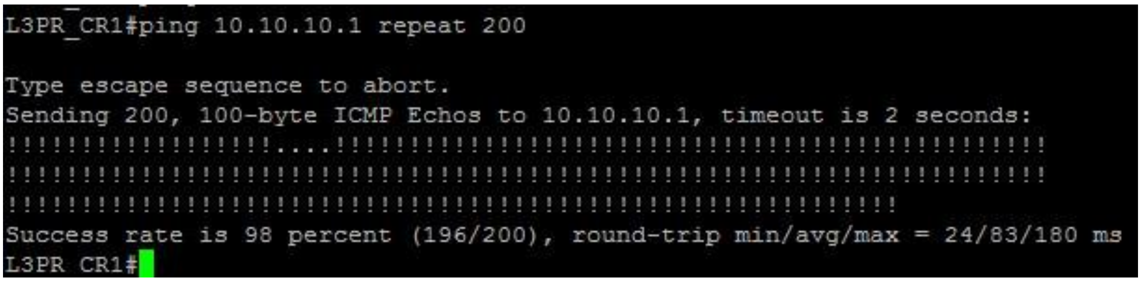
6.1 Testing results of HSRP

Pinging from L3PR_CR1 to ISP loopback ip address 10.10.10.1 with router L3PR_L1 elected as Active HSRP router.



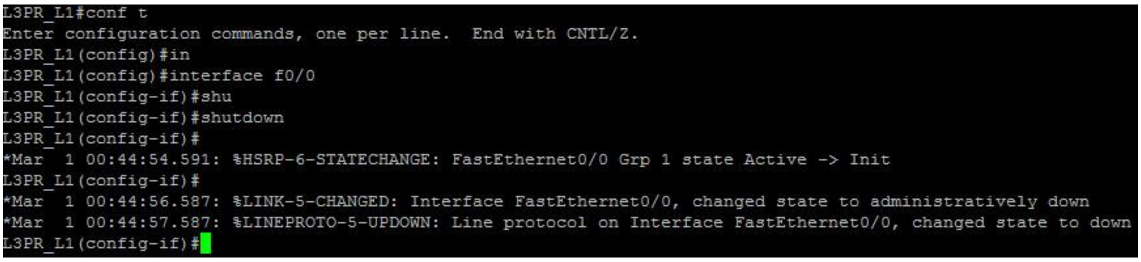
```
Connected to Dynamips VM "L3PR_L1" (ID 6, type c3600) - Console port
Press ENTER to get the prompt.

L3PR_L1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Prio P State    Active          Standby         Virtual IP
Fa0/0       1    110    Active   local           192.168.0.254   192.168.0.1
L3PR_L1#
```

Figure 166. HSRP Active elected router



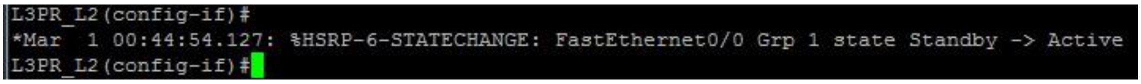
```
L3PR_CR1#ping 10.10.10.1 repeat 200

Type escape sequence to abort.
Sending 200, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 98 percent (196/200), round-trip min/avg/max = 24/83/180 ms
L3PR CR1#
```

Figure 177. Pinging from L3PR_CR1 to ISP Loopback



```
L3PR_L1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
L3PR_L1(config)#in
L3PR_L1(config)#interface f0/0
L3PR_L1(config-if)#shu
L3PR_L1(config-if)#shutdown
L3PR_L1(config-if)#
*Mar  1 00:44:54.591: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Init
L3PR_L1(config-if)#
*Mar  1 00:44:56.587: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar  1 00:44:57.587: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
L3PR_L1(config-if)#
```

Figure 188. Interface shutdown on L3PR_L1 (HSRP Active router)

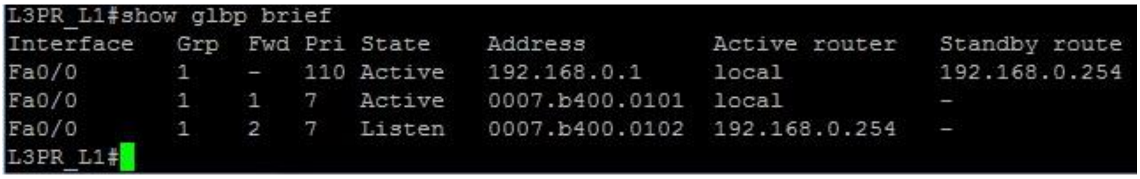


```
L3PR_L2(config-if)#
*Mar  1 00:44:54.127: %HSRP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
L3PR_L2(config-if)#
```

Figure 199. L3PR_L2 (standby router) changing from standby to Active

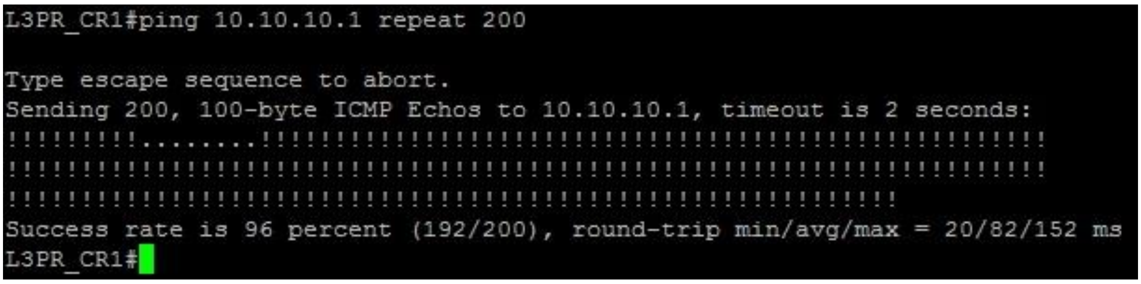
6.2 Testing results of GLBP

Pinging from L3PR_CR1 to ISP loopback ip address 10.10.10.1 with router L3PR_L1 elected as Active GLBP router.



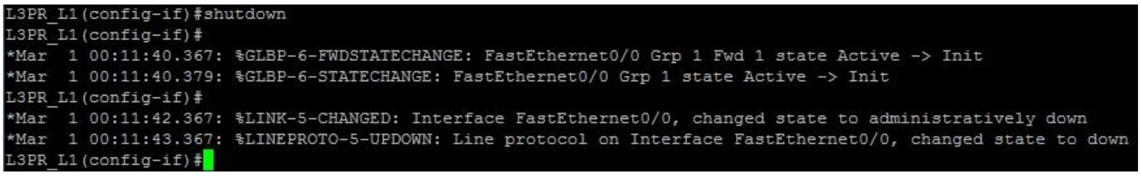
```
L3PR_L1#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby route
Fa0/0       1    -   110 Active   192.168.0.1     local           192.168.0.254
Fa0/0       1    1   7   Active   0007.b400.0101  local           -
Fa0/0       1    2   7   Listen   0007.b400.0102  192.168.0.254   -
L3PR_L1#
```

Figure 200. GLBP Active elected router



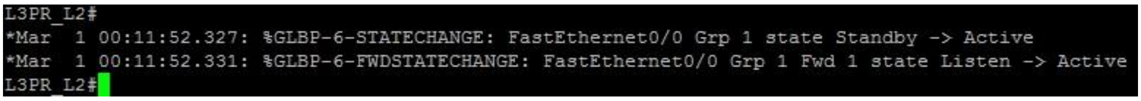
```
L3PR_CR1#ping 10.10.10.1 repeat 200

Type escape sequence to abort.
Sending 200, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!!!!!........!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 96 percent (192/200), round-trip min/avg/max = 20/82/152 ms
L3PR_CR1#
```

Figure 211. Pinging from L3PR_CR1 to ISP Loopback (GLBP)



```
L3PR_L1(config-if)#shutdown
L3PR_L1(config-if)#
*Mar  1 00:11:40.367: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 1 state Active -> Init
*Mar  1 00:11:40.379: %GLBP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Init
L3PR_L1(config-if)#
*Mar  1 00:11:42.367: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar  1 00:11:43.367: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
L3PR_L1(config-if)#
```

Figure 222. Interface shutdown on L3PR_L1 (GLBP Active router)

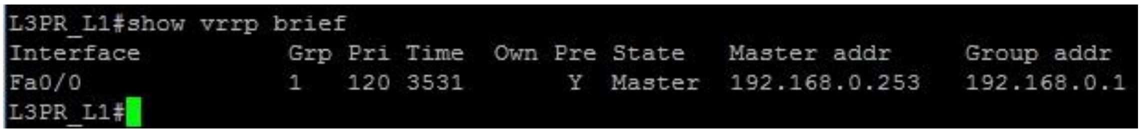


```
L3PR_L2#
*Mar  1 00:11:52.327: %GLBP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
*Mar  1 00:11:52.331: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 1 state Listen -> Active
L3PR_L2#
```

Figure 233. (standby router) changing from standby to Active (GLBP)

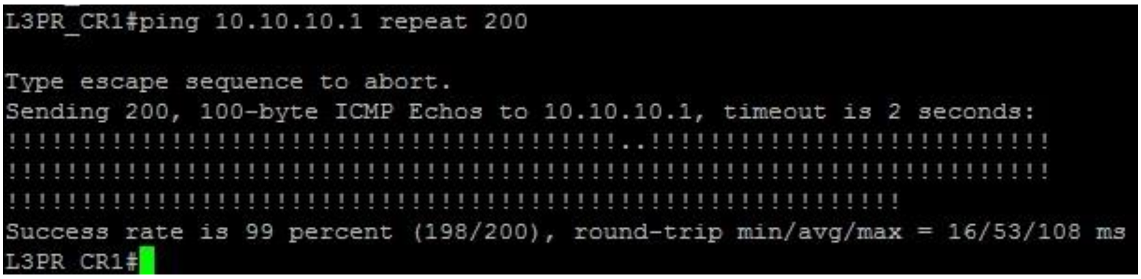
6.3 Testing results of VRRP

Pinging from L3PR_CR1 to ISP loopback ip address 10.10.10.1 with router L3PR_L1 elected as Master router.



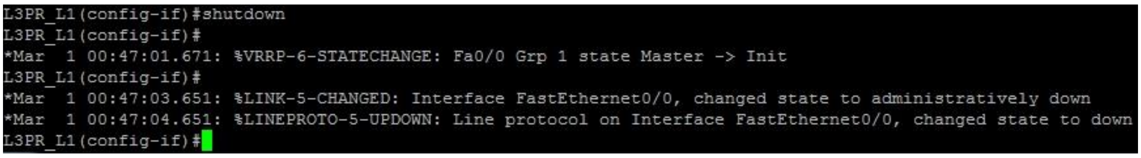
```
L3PR_L1#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Fa0/0              1   120 3531       Y  Master  192.168.0.253   192.168.0.1
L3PR_L1#
```

Figure 244. VRRP Master elected router



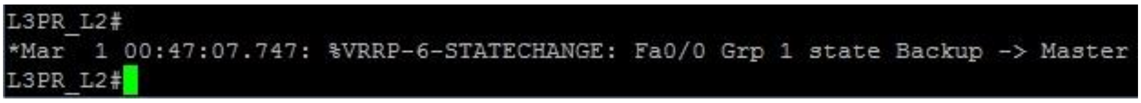
```
L3PR_CR1#ping 10.10.10.1 repeat 200

Type escape sequence to abort.
Sending 200, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!..!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (198/200), round-trip min/avg/max = 16/53/108 ms
L3PR_CR1#
```

Figure 255. Pinging from L3PR_CR1 to ISP Loopback (VRRP)



```
L3PR_L1(config-if)#shutdown
L3PR_L1(config-if)#
*Mar  1 00:47:01.671: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Master -> Init
L3PR_L1(config-if)#
*Mar  1 00:47:03.651: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Mar  1 00:47:04.651: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
L3PR_L1(config-if)#
```

Figure 266. Interface shutdown on L3PR_L1 (VRRP Master router)



```
L3PR_L2#
*Mar  1 00:47:07.747: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Backup -> Master
L3PR_L2#
```

Figure 277. (backup router) changing from Backup to Master (VRRP)

7 CONCLUSIONS

Obviously, like most things in networking, there are a number of options available which can each be used to solve a specific problem. Two of the three solutions discussed above are specific to Cisco equipment, and thus can only be used in implementations where only Cisco equipment is used (at least across the gateways). VRRP is an option implementation which is supported on multiple vendors' equipment and thus provides an option that opens the door to non-Cisco equipment. GLBP offers the ability to dynamically load balance traffic, which is a big advantage as it takes advantage of all available bandwidth and does not waste these resources. Which one to select depends a great deal on the specific situation and should each be considered depending on the details of the implementation. Every protocol works in its own specific way and contains different type specialty within it.

Below is a table which compares features of all three protocols.

Protocol Features	HSRP	VRRP	GLBP
Router role	1 active router. 1 standby router. 1 or more listening routers	1 master router. 1 or more backup routers	1 AVG routers (active virtual gateway). Up to 4 AVF routers on the group (active virtual forwarder) passing traffic. Up to 1024 virtual routers

				(GLBP groups) per physical interface
		Use virtual IP address	Can use real IP address, if not, the one with highest becomes master	Use virtual IP address
Scope		Cisco proprietary	IEEE standard	Cisco proprietary
Election		Active router Highest priority Highest IP (tiebreaker)	Master router Highest priority Highest IP (tiebreaker)	Active virtual gateway Highest priority Highest IP (tiebreaker)
Optimization feature	**Tracking**	Yes	Yes	Yes
	Pre-empt	Yes	Yes	Yes
	Timer adjustments	Yes	Yes	Yes
Traffic type		224.0.0.2-UDP 1985(version 1) 224.0.0.102-UDP 1985(version 2)	224.0.0.18-UDP 112	224.0.0.102-UDP 3222
Timers		Hello – 3 seconds	Advertisement- 1 second	Hello– 3 seconds
		(hold) 10 seconds	(master down interval) 3	(hold) 10 seconds
			Advertisement + skew time	
			(Skew time)(256 - priority)/256	
Load balancing functionality		Multiple HSRP group per interface/SVI/routed int.	Multiple VRRP group per interface/ SVI/routed int.	
		Requires appropriate distribution of GW IP per clients for optimal load balancing (generally through DHCP).	Requires appropriate distribution of GW IP per clients for optimal load balancing (generally through DHCP).	Clients are transparently updated with MAC according to load balancing algorithm through ARP requesting a unique virtual gateway.

Table 3. Difference between features of HSRP, VRRP, GLBP **[8]**

8 REFERENCES

[1] W. Odome, Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide, Indianapolis, IN 46240 USA: Cisco Press, 2013.

[2] I. Cisco Systems, "Campus Network for High Availability," *Campus Network for High Availability,* 2008.

[3] T. Lammle, CCNA - Routing and Switching Review Guide, Indiana: John Wiley & Sons, Inc., Indianapolis,, 2014.

[4] IETF, "Internet Engineering Task Force," 12 Nov 2013. [Online]. Available: http://www.ietf.org.

[5] Cybex, "CCNP - Routing Study Guide," in *CCNP - Routing Study Guide*, Alameda, CA, Cybex, 2001.

[6] IETF, "Cisco Hot Standby Router Protocol (HSRP)," IETF, Mar 1998. [Online]. Available: http://tools.ietf.org/search/rfc2281. [Accessed 12 Jan 2014].

[7] Cisco, "Cisco Systems Inc," 13 Nov 2013. [Online]. Available: http://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html.

[8] Cisco-IOS, "Cisco IOS XE 3S," 2013. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-vrrp.pdf. [Accessed 13 Jan 2014].

[9] Juniper, "Juniper Networks," 14 Nov 2013. [Online]. Available: http://www.juniper.net/techpubs/en_US/junos13.3/topics/concept/vrrp-overview-ha.html.

[10] IJETT, "IJETT," *International Journal of Engineering Trends and Technology*, pp. 1085-1088, 2013.

[11] C. Systems, Cisco IOS First Hop Redundancy Protocols Command Reference, San Jose: Cisco Inc, 2013.

9 Appendix

9.1.1 Basic configuration of HSRP

Step	Command or Action	Purpose
1	**enable** Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode.
3	**interface** *type number* Example: Router(config)# interface GigabitEthernet 0/0/0	Specifies an interface type and number, and enters interface configuration mode.
4	**ip address** *ip-address mask* **[secondary]** Example: Router(config-if)# ip address 192.168.1.2 255.255.255.0	Specifies a primary or secondary IP address for an interface.
5	**standby [**group-number**] ip [**ip-address **[secondary]]** Example: Router(config-if)# standby 1 ip 192.168.1.1	Create (or enable) the HSRP group using its number and virtual IP address. •(Optional) group-number—The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. •(Optional on all but one interface) ip-address—The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. •(Optional) secondary—The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.

6	**exit** Example: Router(config-if)# exit	Exits interface configuration mode, and returns the router to global configuration mode.
7	**show standby** Example: Router# show standby	Verify the configuration.

Example

R1 and R2 will both be configured to be in standby group 1. The HSRP address will be given an IP address of 192.168.1.1/24. All hosts on the segment and in the VLAN will use this address as their default gateway.

```
R1(config)#interface ethernet0
R1(config-if)#ip address 192.168.1.2 255.255.255.0
R1(config-if)#standby 1 ip 192.168.1.1

R2(config)#interface ethernet0
R2(config-if)#ip address 192.168.1.3 255.255.255.0
R2(config-if)#standby 1 ip 192.168.1.1
```

To see the status of HSRP use the command show standby. This is the first command you should run to ensure that HSRP is running and configured properly.

```
R1#show standby
Ethernet0 - Group 1
     Local state is Standby, priority 100
     Hellotime 3 sec, holdtime 10 sec
     Next hello sent in 0.776
     Virtual IP address is 192.168.1.1 configured
     Active router is 192.168.1.3, priority 100 expires in 9.568
     Standby router is local
     1 state changes, last state change 00:00:22

R2#show standby
Ethernet0 - Group 1
     Local state is Active, priority 100
     Hellotime 3 sec, holdtime 10 sec
     Next hello sent in 2.592
     Virtual IP address is 192.168.1.1 configured
     Active router is local
```

```
    Standby router is 192.168.1.2 expires in 8.020
Virtual mac address is 0000.0c07.ac05
2 state changes, last state change 00:02:08
```

We can see that R2 has been selected as the Active router ("Local state is Active"), the virtual router's IP is 192.168.1.1, and R1 is the standby router.

9.1.2 Basic configuration of GLBP

Step	**Command or Action**	**Purpose**
1	**enable** Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode.
3	**interface** *type number* Example: Router(config)# interface GigabitEthernet 0/0/0	Specifies an interface type and number, and enters interface configuration mode.
4	**ip address** *ip-address mask* **[secondary]** Example: Router(config-if)# ip address 10.21.8.32 255.255.255.0	Specifies a primary or secondary IP address for an interface.
5	**glbp** *group* **ip** [*ip-address* [**secondary**]] Example: Router(config-if)# glbp 10 ip 10.21.8.10	Enables GLBP on an interface and identifies the primary IP address of the virtual gateway. • After you identify a primary IP address, you can use the glbp group ip command again with the secondary keyword to indicate additional IP addresses supported by this group.
6	**exit** Example: Router(config-if)# exit	Exits interface configuration mode, and returns the router to global configuration mode.
7	**show glbp** [*interface-type interface-number*] [group] [state] [**brief**] Example: Router(config)# show glbp 10	(Optional) Displays information about GLBP groups on a router. • Use the optional brief keyword to display a single line of information about each virtual gateway or virtual forwarder.

Example

In the following example, sample output is displayed about the status of the GLBP group, named 10, on the router:

Router# **show glbp 10**

```
GigabitEthernet0/0/0 - Group 10
    State is Active
       2 state changes, last state change 23:50:33
    Virtual IP address is 10.21.8.10
    Hello time 5 sec, hold time 18 sec
       Next hello sent in 4.300 secs
    Redirect time 600 sec, forwarder time-out 7200 sec
    Authentication text "stringabc"
    Preemption enabled, min delay 60 sec
    Active is local
    Standby is unknown
    Priority 254 (configured)
    Weighting 105 (configured 110), thresholds: lower 95, upper 105
       Track object 2 state Down decrement 5
    Load balancing: host-dependent
    There is 1 forwarder (1 active)
    Forwarder 1
       State is Active
           1 state change, last state change 23:50:15
    MAC address is 0007.b400.0101 (default)
    Owner ID is 0005.0050.6c08
    Redirection enabled
    Preemption enabled, min delay 60 sec
    Active is local, weighting 105
```

9.1.3 Basic configuration of VRRP

Step	Command or Action	Purpose
1	**enable** Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode.

3	**interface** *type number* Example: Router(config)# interface GigabitEthernet 0/0/0	Specifies an interface type and number, and enters interface configuration mode.
4	**ip address** *ip-address mask* **[secondary]** Example: Router(config-if)# ip address 10.21.8.32 255.255.255.0	Specifies a primary or secondary IP address for an interface.
5	**vrrp** group **ip** ip-address **[secondary]** Example: Router(config-if)# vrrp 10 ip 172.16.6.1	Enables VRRP on an interface. • After you identify a primary IP address, you can use the vrrp ip command again with the secondary keyword to indicate additional IP addresses supported by this group. **Note** All routers in the VRRP group must be configured with the same primary address and a matching list of secondary addresses for the virtual router. If different primary or secondary addresses are configured, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.
6	**End** Example: Router(config-if)# end	Returns to privileged EXEC mode.
7	**show vrrp [brief |** *group***]** Example: Router# show vrrp 10	(Optional) Displays a brief or detailed status of one or all VRRP groups on the router.
8	**show vrrp interface** *type number* **[brief]** Example: Router# show vrrp interface GigabitEthernet 0/0/0	(Optional) Displays the VRRP groups and their status on a specified interface.

9.1.4 Router configs of ISP and L3PR_CR1

ISP

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
no aaa new-model
ip subnet-zero
no ip routing
!
no ip cef
!
!
username tuka privilege 15 password 7 044E09125E731F
!
interface Loopback0
 description >> Rrjeta Loopback 0 <<
 ip address 10.10.10.1 255.255.255.0
 no ip route-cache
!
interface FastEthernet0/0
 description Link to Level 3
 ip address 178.132.216.73 255.255.255.248
 no ip route-cache
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description Link to Level 3
 ip address 213.163.122.137 255.255.255.248
 no ip route-cache
 duplex auto
 speed auto
!
ip http server
ip classless
!
!
control-plane
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
!
end
```

L3PR_CR1

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname L3PR_L1
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 5
no aaa new-model
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name lab.local
!
username tuka privilege 15 password 7 105B0B0D544541
!
interface FastEthernet0/0
 description link to Level 3 Network
 ip address 192.168.0.253 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 standby 100 ip 192.168.0.1
 standby 100 priority 200
 standby 100 authentication ubt123
 standby 100 track FastEthernet0/0
!
interface FastEthernet0/1
 description Link to ISP
 ip address 213.163.122.138 255.255.255.248
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 213.163.122.137
!
ip nat inside source list 100 interface FastEthernet0/1 overload
!
access-list 100 remark NAT Overload
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login local
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
!
end
```

9.1.5 Router configs of HSRP Routers

L3PR_L1

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname L3PR_L1
!
boot-start-marker
boot-end-marker
```

```
!
memory-size iomem 5
no aaa new-model
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name lab.local
!
username tuka privilege 15 password 7 105B0B0D544541
!
interface FastEthernet0/0
 description link to Level 3 Network
 ip address 192.168.0.253 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 standby 100 ip 192.168.0.1
 standby 100 priority 200
 standby 100 authentication ubt123
 standby 100 track FastEthernet0/0
!
interface FastEthernet0/1
 description Link to ISP
 ip address 213.163.122.138 255.255.255.248
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 213.163.122.137
!
ip nat inside source list 100 interface FastEthernet0/1 overload
!
access-list 100 remark NAT Overload
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login local
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
!
end
```

L3PR_L2

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname L3PR_L2
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
no aaa new-model
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name lab.local
!
username tuka privilege 15 password 7 105B0B0D544541
!
interface FastEthernet0/0
description link to Level 3 Network
 ip address 192.168.0.254 255.255.255.0
 duplex auto
 speed auto
 standby 100 ip 192.168.0.1
 standby 100 priority 200
 standby 100 authentication ubt123
 standby 100 track FastEthernet0/0
!
interface FastEthernet0/1
```

```
 description Link to ISP
 ip address 178.132.216.74 255.255.255.248
 duplex auto
 speed auto
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 178.132.216.73
!
ip nat inside source list 100 interface FastEthernet0/1 overload
!
access-list 100 remark NAT Overload
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login local
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

9.1.6 Router configs of GLBP Routers

L3PR_L1

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname L3PR_L1
!
boot-start-marker
boot-end-marker
!
```

```
memory-size iomem 5
no aaa new-model
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name lab.local
!
username tuka privilege 15 password 7 105B0B0D544541
!
interface FastEthernet0/0
 description link to Level 3 Network
 ip address 192.168.0.253 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 glbp 1 ip 192.168.0.1
 glbp 1 priority 110
 glbp 1 name GLBP-group-for-UBT
!
interface FastEthernet0/1
 description Link to ISP
 ip address 213.163.122.138 255.255.255.248
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 213.163.122.137
!
ip nat inside source list 100 interface FastEthernet0/1 overload
!
access-list 100 remark NAT Overload
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login local
```

```
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
!
end
```

L3PR_L2

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname L3PR_L2
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
no aaa new-model
ip subnet-zero
!
!
ip cef
no ip domain lookup
ip domain name lab.local
!
username tuka privilege 15 password 7 105B0B0D544541
!
interface FastEthernet0/0
description link to Level 3 Network
 ip address 192.168.0.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 glbp 1 ip 192.168.0.1
 glbp 1 name GLBP-group-for-UBT
!
interface FastEthernet0/1
 description Link to ISP
 ip address 178.132.216.74 255.255.255.248
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 178.132.216.73
!
ip nat inside source list 100 interface FastEthernet0/1 overload
!
access-list 100 remark NAT Overload
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login local
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
end
```

9.1.7 Router configs of VRRP Routers

L3PR_L1

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname L3PR_L1
!
boot-start-marker
boot-end-marker
```

```
!
memory-size iomem 5
no aaa new-model
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name lab.local
!
username tuka privilege 15 password 7 105B0B0D544541
!
interface FastEthernet0/0
 description link to Level 3 Network
 ip address 192.168.0.253 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 vrrp 1 ip 192.168.0.1
 vrrp 1 priority 120
 vrrp 1 authentication text cisco
!
interface FastEthernet0/1
 description Link to ISP
 ip address 213.163.122.138 255.255.255.248
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 213.163.122.137
!
ip nat inside source list 100 interface FastEthernet0/1 overload
!
access-list 100 remark NAT Overload
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login local
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
!
end
```

L3PR_L2

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname L3PR_L2
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
no aaa new-model
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name lab.local
!
username tuka privilege 15 password 7 105B0B0D544541
!
interface FastEthernet0/0
 ip address 192.168.0.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
 vrrp 1 description VRRP-for-UBT
 vrrp 1 ip 192.168.0.1
 vrrp 1 authentication text cisco
!
interface FastEthernet0/1
 description Link to ISP
 ip address 178.132.216.74 255.255.255.248
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 178.132.216.73
!
ip nat inside source list 100 interface FastEthernet0/1 overload
!
access-list 100 remark NAT Overload
access-list 100 permit ip 192.168.0.0 0.0.0.255 any
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 login local
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```