5-2019

First Hop Redundancy Protocols (FHRP)

Raghad Faisal Alshehri
Florida Institute of Technology

First Hop Redundancy Protocols (FHRP)

by

Raghad Faisal Alshehri

A thesis submitted to the Computer Engineering and Science of
Florida Institute of Technology
in partial fulfillment of the requirements
for the degree of

Master of Computer Information Systems
in
Computer Sciences Department

Melbourne, Florida
May, 2019

We the undersigned committee hereby approve the attached thesis

First Hop Redundancy Protocols (FHRP)

by

Raghad Faisal Alshehri

David LeVan, Ph.D.
Assistant Professor
Computer Sciences

Marius Silaghi, Ph.D.
Associate Professor
Computer Sciences

Tiauw Hiong Go, Ph.D.
Associate Professor
Aerospace Engineering

Philip Bernhard, Ph.D.
Associate Professor and Department Head
Computer Engineering and Sciences

Abstract

Title: First Hop Redundancy Protocols

Author: Raghad Alshehri

Advisor: David LeVan, Ph. D.

When a network is designed, the most important thing that is always kept in mind is the factor of availability. However, a lot of researchers are still working on managing and implementing more dependable networks are resilient to severe failovers and can cope up under immense traffic loads. With that being said, a lot of questions still need to be answered according to the financial and implementation point of view. Correspondingly, the current study aims at answering all these questions and providing with the best optimal solutions to deploy dependable networks primary aimed towards hardening and enforcing various techniques and protocols in the gateway router.[1]

Gateway routers are of main concern because all the connectivity depends on them, if the gateway router goes down, the entire network goes down and becomes un-available. So, to address the specific issue, adding redundancy in the network was proposed and several vendors such as CISCO started working on them and came up with a couple of protocols that enable network redundancy and prevents failovers. Similarly, the current study is all about studying various aspects of these protocols and presenting with various optimal solutions around these protocols that are easily implementable and attainable. The current study would try to answer several questions regarding these protocols and their implementation. However, the main focus would be on these three primary protocols such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP).

Table of Contents

List of Figures

List of Tables

Acknowledgement

First of all, I would like to thank the lord of the worlds, Allah, the one who is most deserving of thanks and praise, and who directed me to the path of knowledge and wisdom in my educational journey and life in general.

Foremost, I would like to express my sincere gratitude to my advisor David LeVan for the continuous support of my 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. I could not have imagined having a better advisor and mentor for my FHRP study.

Besides my advisor, I would like to thank the rest of my thesis committee: Professor. Go, and Professor. Silaghi for their encouragement, insightful comments.

My sincere thanks also to my parents Mr. Faisal Alshehri and Mrs. Thuraya AL Qubaisi, for raising me, standing behind me, helping me and supporting me in the pursuit of my graduate studies from one of the top programs for computer science majors at the First place and supporting me spiritually throughout my life.

Last but not the least, I would like to thank my Sisters, my Brothers, and my Friends, for their motivation and patience during my academic journey.

Chapter 1

Introduction

There are three major first hop redundancy protocols provided by CISCO, however, they lie in two different categories and the protocols are named HSRP, VRRP, and GLBP. Correspondingly, HSRP and VRRP lie under the same category as they provide backup redundancy on Layer 3 Gateway routers, furthermore, the main functionality involves the placement of a backup gateway router which enables by itself under un-availability of the main gateway router. However, GLBP works in a different fashion as it involves the active usage of backup or redundant gateway routers parallel to the main gateway router as the load is shared and balanced among multiple instances instead of relying on a single unit and coming up with a backup. The current study would evaluate and present the multiple aspects of these protocols under the parameters of cost, applicability and efficiency.[1]

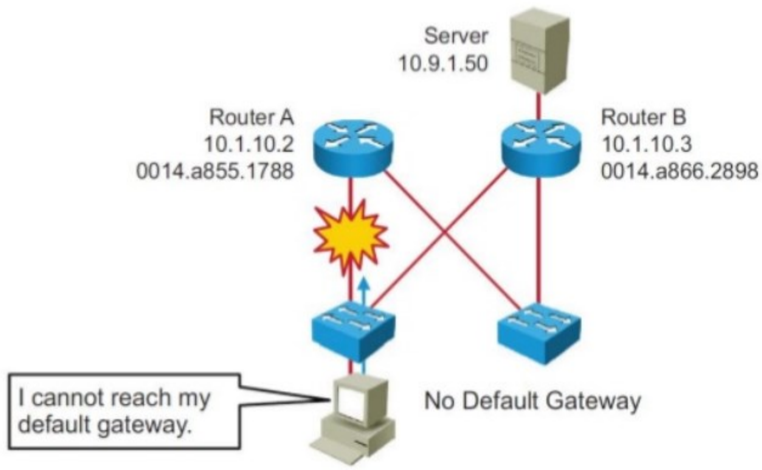


Figure 1

Problem Statement

First Hop Redundancy Protocol (FHRP) can be defined as a set of protocols that incorporate backup and provide redundancy to the network gateway in-case it goes down or is temporarily unavailable at the moment. The primary purpose of this protocol was to facilitate Ethernet as well as Token Ring networks. Moreover, it has also been analyzed that all the devices on a network are preconfigured to identify the gateway router which connects them with the outside network or the internet, the machines contain a default gateway address which directly points towards the gateway router. However, the problem escalates when the primary gateway router fails to cope up or fails due to certain reasons and the devices don't know about the backup or redundant router to contact. This problem occurs when there is no proper configuration of the protocol that specifically handles this job.

Correspondingly, the solution to this problem is the employment of First Hop Redundancy Protocols which would enable the use of backup of load balancing routers on the go. In due context, the current study is aimed towards exploring the characteristics and deployment point of views of the main three redundancy protocols which are HSRP, VRRP, and GLBP.

The current study specifically aims to answer following research questions:

- Which protocol is suitable according to a particular environment?
- How to effectively configure the protocols
- How long would it take to changeover to the backup router
- What are the specific requirements to implement the protocol?
- How exactly the communication happens between the master and backup router.
- What exactly would happen if the primary router goes down
- What are the benefits of adding redundancy in the network?

Chapter 2
First Hop Redundancy Protocols (FHRP)

2.1 Hot Standby Router Protocols (HSRP)

HSRP is developed by CISCO and it is one of their proprietary protocols which is specifically designed to incorporate non-disruptive failover and support redundancy in the network. However, if the network is deprived of this particular protocol, each and every station on the network would be separately configured to communicate with a specific router in case of a failure, although this technique would not provide us with redundancy but would limit the number of stations that would be affected under failure of the gateway. [1]

Furthermore, if HSRP is configured properly and backup gateways are installed, there would be a single virtual IP that would be assigned to the stations or the systems and they would automatically communicate with the backup router if the primary one goes down [2].

2.1.1 How it is work

Working mechanism of this protocol is quite efficient as different routers in the HSRP domain would communicate with the primary live router which would be responsible of controlling all the live incoming and outgoing traffic. Similarly, the backup routers would constantly communicate with the primary router on the multicast address of 224.0.0.2 so that they would be able to detect on time if the primary router fails or goes down. In due context, the backup routers would automatically take charge if the primary one goes down, however, the end users won't face any sort of delay as the same process of selecting a standby router would be repeated and a new backup would be selected.[1]

2.1.2 Configuration

Table 1

Steps	Command	Purpose
1	**configure terminal**	Enter global configuration mode.
2	**Interface** *interface-id*	Enter interface configuration mode and enter the Layer 3 interface on which you want to enable HSRP.
3	**standby version** {**1** | **2** }	(Optional) Configure the HSRP version on the interface. 1— Select HSRPv1. 2— Select HSRPv2. If you do not enter this command or do not specify a keyword, the interface runs the default HSRP version, HSRP v1.
4	**standby** [*group-number*] ip [*ip-address* [**secondary**]]	Create (or enable) the HSRP group using its number and virtual IP address. 1. (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. 2. (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. 3. (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.
5	**end**	Return to privileged EXEC mode.
6	**show standby** [*interface-id* [*group*]]	Verify the configuration.
7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

2.1.3 Enabling HSRP Support for ICMP Redirect Messages

When the interfaces are configured to work with HSRP, it by default enables the ICMP redirection. ICMP is a major Layer 3 protocol which is used to check the end to end connection and detect any sort of errors in the path. Moreover, it also presents us with various IP processing information and diagnostic information, likewise, the filtering of outgoing ICMP redirection messages is done by HSRP which further includes the changing to and HSRP virtual IP address rather than the next hop IP.[3]

2.2 Virtual Router Redundancy Protocol (VRRP)

VRRP is an open standard that can be used in environments where equipment from multiple vendors exists. Its operation is similar to HSRP but differs in a couple of ways.[1]

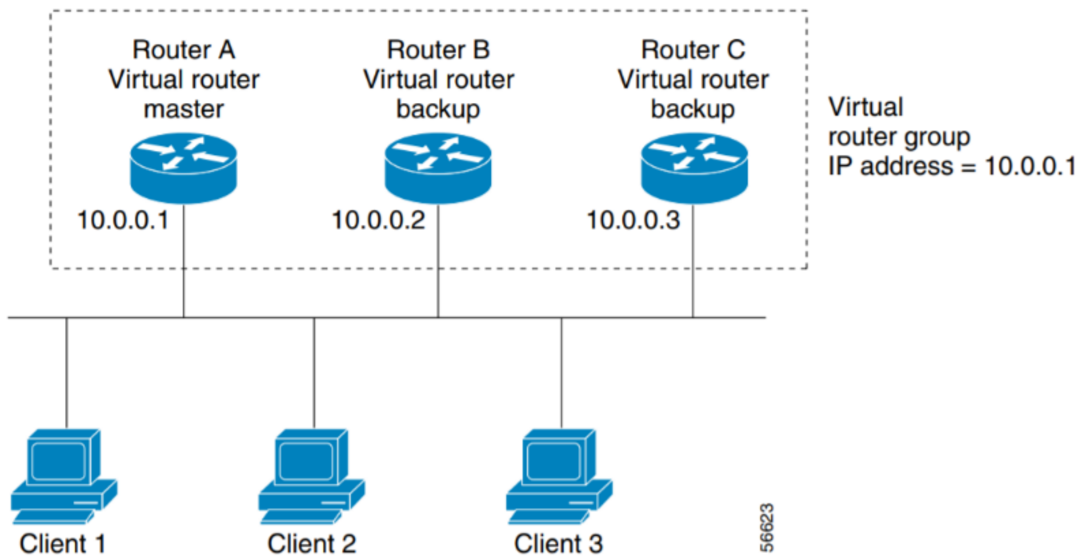


Figure 2_VRRP

2.2.1 How it is work

In VRRP, the working mechanism is almost same, however, in HSRP, the backup router was selected automatically by the protocol whereas, in VRRP, a specific group of routers is selected and configured by the network admin along with the selection of backup router. In this protocol, there is a specific physical interface of the master router which would be used by the entire subnet to communicate, alongside the backup routers would also communicate via different interface and would take the responsibilities of the gateway if it fails. However, the IP would remain static and the master would automatically take back the control once it recovers from the failover.[2]

2.2.2 Configuration

Table 2

Sr No	Command	Method	Example
1	enable	This step enables privileged of EXEC mode. It enters the passwords if correct.	router> enable
2	configure terminal	This step enters the global configuration mode.	router# configure terminal
3	interface type number	This step enters an interface configuration.	Router (config) # interface GigabitEthernet 0/0/0

4	ip address ip-address mask	This step configure the IP address for the interface.	Router (config-if) # ip address 172.16.6.5 255.255.255.0
5	**vrrp** group **description** text	It assigns the text description to a VRRP group.	Router (config-if) # vrrp 10 description working-group
6	**vrrp** group **priority** level	It sets a router priority level within the VRRP group. Here a default priority is 100	Router (config-if) # vrrp 10 priority 110
7	**vrrp** group **preempt [delay minimum seconds]**	This step configures a router to take over as the virtual router master for the VRRP group if it has higher priority than a current virtual router master.	Router (config-if) # vrrp 10 preempt delay minimum 380
8	**vrrp** group **timers advertise [msec]** interval	This step configures an interval between the successive advertisements by a virtual router master in the VRRP master.	Router (config-if) # vrrp 10 timers advertise 110
9	**vrrp** group **timers learn**	It configures a router, when it acted as the virtual router backup for the VRRP group, that to learn an advertisement intervals used by a virtual router master.	Router (config-if) # vrrp 10 timers learn

10	exit	This exit interface configuration.	Router (config-if) # exit
11	copy **running-config startup-config**	This saves the configuration.	Router # copy **running-config startup-config**

2.2.2.1 Enable VRRP

Steps	**Command**
1	enable
2	configure terminal
3	interface type number
4	ip address ip-address mask
5	**Vrrp** group ip ip-address [secondary]
6	End
7	Show vrrp [brief | group]
8	Show vrrp interface type number [brief]

2.2.2.2 Configure VRRP in Object Tracking

Steps	**Command**
1	enable

2	configure terminal
3	Tract object-number interface type number {line-protocol | ip routing}
4	Interface type number
5	**Vrrp** group ip ip-address [secondary]
6	Vrrp group priority level
7	Vrrp group track object-number [decrement priority]
8	end
9	Show track [object-number]

2.2.2.3 VRRP message

As the due research observed, all of the communication done on VRRP is done through multicast addresses which implies that VRRP can be used on any sort of LAN which is capable of supporting multicasting. However, there is a specific multicast address assigned by IANA specifically for this purpose which is 244.0.0.18, it is used by all the routers communicating over VRRP and the actual packets incoming or outgoing between them are actually encapsulated or catered by IP packets. Furthermore, VRRP messages include VRRP state messages, VRRP priority messages and VRID information is also shared [3].

Also, there is a major difference between VRPR and HSRP is that all of these messages are distributed form the primary router towards the backup routers which are always in passive listening mode and as soon as they stop listening form the primary router, they assume it as a failover and take the charge.[4]

There are four fields in IP header that are important for VRRP. These fields are:

- Time To Live (TTL)
- Protocol type
- Source IP Address
- Destination IP Address

2.3 Gateway Load Balancing Protocols (GLBP)

GLBP is observed as another efficient redundancy protocol which is designed by CISCO and is their proprietary item which means that it is limited to work with CISCO devices and not interoperable. However, there are a couple of functionalities provided by GLBP which is not offered by the other two protocols is the active load balancing as the backup routers are actively communicating and sharing the load of the gateway router to maintain the availability.[3]

2.3.1 How it is work

In GLBP, all the routers are actively taking part and are in group which is capable of active traffic forwarding. However, the configuration mechanism is a little bit different because it includes the selection of an AVG (Active Virtual Gateway) while the other routers are considered and selected as backup routers. Also, in this defined group, the AVG is responsible of assigning physical MAC addresses to the backup routers and all of the backup routers are called as AVF (Active Virtual Forwarder). Furthermore, the AVG is also responsible of responding and replying to all of the ARP requests sent by the stations in the subnet and on the basis of these requests, assigning a specific AVF to that particular part of the subnet to handle the traffic.[4]

However, the default gateway router IP would be same across all the stations in the subnet and when the station sends an ARP, the AVG would reply back with a virtual MAC of the backup router to balance the load so that the particular station would contact the AVF in the future and the load on the AVG is automatically balanced.[1]

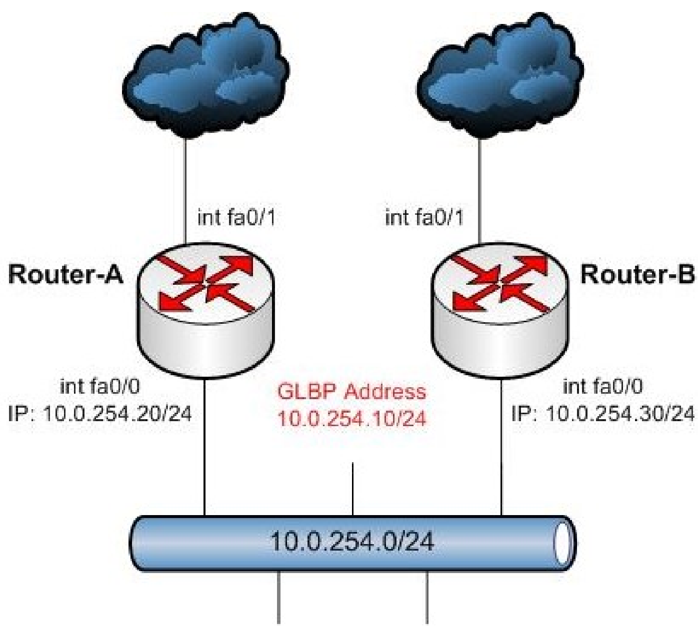


Figure 3_GLBP Topology

2.3.2 Configuration

Table 3

	Command or Action	Purpose
Step 1	**enable** Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* Example: Router(config)# interface fastethernet 0/0	Specifies an interface type and number and enters interface configuration mode.
Step 4	**ip address** *ip-addressmask* [**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. • Refer to the "Configuring IP Addressing" chapter of the Release 12.2 *Cisco IOS IP Configuration Guide* for information on configuring IP addresses.

Step 5	**glbp** *group* **authentication text** *string* Example: Router(config-if)# glbp 10 authentication text stringxyz	Authenticates GLBP packets received from other routers in the group. • If you configure authentication, all routers within the GLBP group must use the same authentication string.
Step 6	**glbp** *group* **forwarder preempt** [**delay minimum** *seconds*] Example: Router(config-if)# glbp 10 forwarder preempt delay minimum 60	Configures the router to take over as AVF for a GLBP group if it has a higher priority than the current AVF. • This command is enabled by default with a delay of 30 seconds. • Use the optional **delay** and **minimum** keywords and the *seconds* argument to specify a minimum delay interval in seconds before preemption of the AVF takes place.
Step 7	**glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**] Example: Router(config-if)# glbp 10 load-balancing host-dependent	Specifies the method of load balancing used by the GLBP AVG.
Step 8	**glbp** *group* **preempt** [**delay minimum** *seconds*] Example:	Configures the router to take over as AVG for a GLBP group if it has a

	Router(config-if)# glbp 10 preempt delay minimum 60	higher priority than the current AVG. • This command is disabled by default. • Use the optional **delay** and **minimum** keywords and the *seconds* argument to specify a minimum delay interval in seconds before preemption of the AVG takes place.
Step 9	**glbp** *group* **priority** *level* Example: Router(config-if)# glbp 10 priority 254	Sets the priority level of the gateway within a GLBP group. • The default value is 100.
Step 10	**glbp** *group* **timers** [**msec**] *hellotime* [**msec**]*holdtime* Example: Router(config-if)# glbp 10 timers 5 18	Configures the interval between successive hello packets sent by the AVG in a GLBP group. • The *holdtime* argument specifies the interval in seconds before the virtual gateway and virtual forwarder information in the hello packet is considered invalid. • The optional **msec** keyword specifies that the following argument will

		be expressed in milliseconds, instead of the default seconds.
Step 11	**glbp** *group* **timers redirect** *redirect timeout* Example: Router(config-if)# glbp 10 timers redirect 1800 28800	Configures the time interval during which the AVG continues to redirect clients to an AVF. • The *timeout* argument specifies the interval in seconds before a secondary virtual forwarder becomes invalid. **Note** The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a router fails, new hosts continue to be assigned to the failed router instead of being redirected to the backup.

Step 12	**exit** Example: Router(config-if)# exit	Exits interface configuration mode, and returns the router to global configuration mode.

Chapter 3
Implementation

3.1 Basic Concept of FHRP

First Hop means that any packet traveling out the network has its gateway as its first hop. The Gateway redundancy protocol is used. IP routing redundancy is designed to allow for transparent fail-over at the first-hop IP router. Each HSRP and VRRP allows or allows multiple devices to work in a group, sharing a single IP address, a virtual IP address. First Hop means that any packet that travels the network has as its first hop its gateway.[8]

The virtual IP address is configured in each end user's workstation as a default gateway address and is cached in the host's Address Resolution Protocol (ARP) cache. In an HSRP or VRRP group, one router is elected to handle all requests sent to the virtual IP address. With HSRP, this is the active router. An HSRP group has one active router, at least one standby router, and perhaps many listening routers. A VRRP group has one master router and one or more backup routers.[6]

“First Hop Redundancy Protocol, which means they allow you to configure more than one physical router, but it can still be seen as a single router. First Hop means that any packet traveling out the network has its gateway as its first hop. It is protocol used for Gateway redundancy”.[10]

Protocol	**HSRP** CISCO-PROPRIETARY Hot Standby Router protocol	**VRRP** Multi-Vendor Virtual Router Redundancy Protocol	**GLBP** CISCO-PROPRIETARY Gateway Load Balancing Protocol
Terminology	One Active Router, one Standby Router, other Routers in Standby group (able to assume roles)	One Master, one or more Backup Virtual Routers	Active Virtual Gateway (AVG), Standby Virtual GW (SVG), Active Virtual Forwarders (AVFs)

Virtual object	GW IP, bound to the group-specific HSRP MAC address:
	`0000.0C07.ACXX (v1, XX is Group ID)`
	`0000.0C9F.FXXX (v2, XXX is Group ID)`
	`0005.73A0.0000 - 0005.73A0.0FFF (IPv6)`
		GW IP, bound to the group-specific VRRP-managed MAC address:
		`0000.5E00.01XX (XX is VRID)`
			GW IP bound to an AVG-managed set of virtual MAC addresses, one for each of the physical routers in the group.

Communication Method and Destination	IP Multicast
	`224.0.0.2 (v1)`
	`224.0.0.102 (v2)`
		IP Multicast
		`224.0.0.18 (IPv4)`
		`FF02:0:0:0:0:0:0:12 (IPv6)`
			IP Multicast
			`224.0.0.102`

Communication Protocol	IPv4, UDP port 1985 IPv6, UDP port 2029	IPv4 and IPV6, protocol 112 (IANA)	IPv4, UDP port 3222
Authentication	**Default:** No authentication Plain text authentication MD5 authentication (newly added)	**Default:** No authentication Plain text authentication MD5 authentication	**Default:** No authentication Plain text authentication
Active Selector	**Priority** – Hard-coded. One router is elected as Active, another as Standby router. The remaining routers are in a listen state. Highest value wins. **Default: 100**	**Priority** – Highest value wins. **Default: 100 Backup, 254 Active**	**Priority** - One gateway is elected as AVG; another is elected as standby virtual GW (SVG). The remaining routers are in a listen state. Highest value wins. **Default: 100**
Hello and Hold Timer	**HELLO** - Interval between successive HSRP Hello messages from a given router. **Default: 3 sec** **HOLD** - Interval between the receipt of a Hello, and the presumption that the sending router failed. **Default: 10 sec**	Unlike HSRP and GLBP, VRRP does not learn timers from the master router. VRRP requires that the hello timer of all routers in the group match. **HELLO – Default: 1 sec, HOLD - Default: 3 sec**	**HELLO** - Interval between successive GLBP Hello messages from a given router. **Default: 3 sec** **HOLD** - Interval between the receipt of a Hello, and the presumption that the sending router failed. **Default: 10 sec**
Active Timer	10 sec		
Standby Timer	10 sec		
Preemption	Use of preemption allows a HSRP device whose priority has become higher to take over the role as the active router in HSRP. **Default: preempt off**	With preemption enabled, VRRP switches to a backup if that backup comes online with a priority higher than the new master. **Default: preempt on.** **Exception:** The router that owns the IP address(es) associated with the virtual router always preempts.	**AVG Preemption** allows a backup virtual gateway to become AVG, if it has a higher priority than the current AVG. **Default: preempt off** **AVF (Forwarder) Preemption** is similar, except that the forwarder preemption uses weighting instead of priority, and it is **enabled by default.**

Figure 4_FHRP Overview

Protocol	**HSRP** CISCO-PROPRIETARY Hot Standby Router protocol		**VRRP** Multi-Vendor Virtual Router Redundancy Protocol		**GLBP** CISCO-PROPRIETARY Gateway Load Balancing Protocol	
Role States	HSRP	6 Roles:	VRRP	3 Roles:	AVG	6 Roles:
	Initial	Start state, HSRP does not run. This state is entered through a configuration change or when an interface first becomes available.	Initialize	Wait for a Startup event.	Disabled	No Virtual IP address configured.
	Learn	The router has not determined the virtual IP address and has not yet seen an authenticated hello message from the active router. The router still waits to hear from the active router.	Backup	Monitors the state of the Master router	Initial	The virtual IP address configured, but virtual gateway configuration is incomplete.
	Listen	The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for 'hello' messages from those routers.	Master	Forward packets for its virtual router MAC address. Respond to ARP requests for its virtual router IP addresses.	Listen	The Virtual GW receives hello messages and is ready to enter "speak" state if AVG unavailable.
	Speak	The router sends periodic hello messages and actively participates in the election of the active and/or standby router. A router cannot enter speak state unless the router has the virtual IP address.			Speak	The Virtual GW is attempting to become the Active Virtual Gateway (AVG).
	Stand by	The router is candidate to become the next active router and sends periodic hello messages. Excluding transient conditions, there is, at most, one router in the group in standby state.			Standby	The Virtual GW is ready to become the next AVG.
	Active	The router currently forwards packets that are sent to the group virtual MAC address. The router sends periodic hello messages. Excluding transient conditions, there must be, at most, one router in active state in the group.			Active	The Virtual GW is AVG, responding to client ARP requests for the virtual IP address, providing one of the AVF MACs based on its load balancing scheme.
					AVF	4 Roles:
					Disabled	No Virtual MAC address assigned.
					Initial	The virtual MAC address is set, but the virtual forwarder (AVF) configuration is incomplete.
					Listen	Virtual forwarder listens for 'hello' messages and is ready to go into "active" state, if another AVF is unavailable.
					Active	Be an AVF, and responsible for forwarding packets sent to its virtual forwarder MAC address.

Figure 5_FHRP Overview

3.2 General FHRP Operation

First, we describe First-hop redundancy protocol as a general operation. The basic principle is that clustered redundant routers form an FHRP group that acts as a single virtual router with an IP address of its own. within the group, a single router is elected as the coordinator based on announced priority. higher priority means superior willingness to turn out to be a coordinator.[9]

In the case of equal priorities between two candidates, a router with the higher IP address is preferred. The election process may be preemptive or non-preemptive. Preemption means that the router with the highest priority always acquires the role of coordinator even if the coordinator already exists.[9]

3.3 Plan of Operation

3.3.1 Virtual Router Redundancy Protocol (VRRP)

3.3.1.1 Basic Concept of VRRP

It is optional to customize VRRP behavior. Be aware that this group operates as soon as you enable a VRRP group. It is possible that if you first enable a VRRP group before customizing VRRP, before you finish customizing the feature, the router could take over group control and become the virtual router master. So if you're planning to customize VRRP, it's a good idea.[2]

The VRRP stands for the redundancy protocol for virtual router. it is the computer networking protocol that permits the participating host to automatically assign the available IP router. it is the election protocol that dynamically assigns duty for one or more virtual routers to a virtual router on the LAN, permitting the usage of the equal virtual IP address by using numerous routers on multi-access links. at the side of 1 or more routers connected to the LAN, the VRRP routers are configured to run a VRRP protocol. 1 router is chosen as a virtual router master in the VRRP configuration, with another router performing as backup if a master fails within the virtual router.[11]

3.3.1.2 The VRRP working process is as follow

Based on device priorities, devices in the VRRP group select the master. The master sends free ARP packets to inform its virtual MAC address to the linked device or host. VRRP advertisement packets are periodically sent by the master to all backups in the VRRP group to advertise their configuration and running status.[11]

If the master becomes faulty, the backups in the group select a new master based on priorities.

“When the VRRP group status changes, a new master is used. The new master sends gratuitous ARP packets carrying the virtual MAC address and virtual IP address of the virtual router to update the MAC address entry on the connected host or device. Then user traffic is switched to the new master. This process is transparent to users. When the original master recovers and is the IP address owner, the original master directly switches to the Master state. If the original master is not the IP address owner, it first switches to the Backup state and its original priority is restored”.[2]

To ensure that the master and backup cooperate, VRRP must be able to:

- Select the master.
- Advertise the master status.

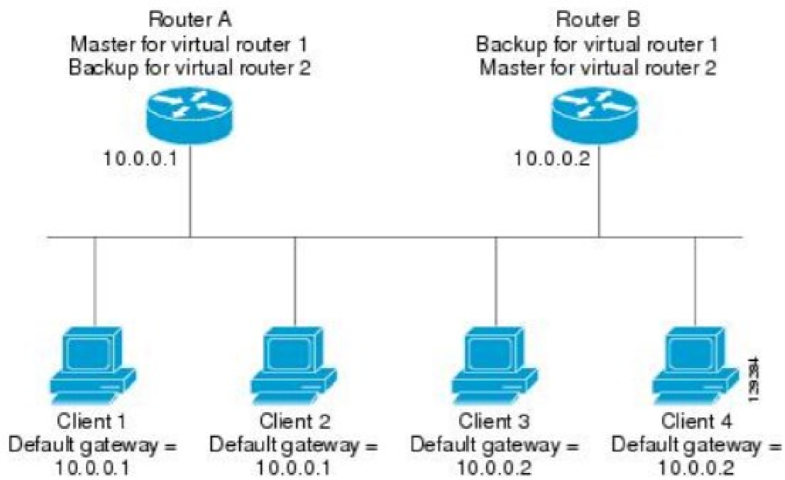


Figure 6_VRRP Network

Summery Steps

1. enable
2. configure terminal
3. interface type number
4. ip address ip-address mask
5. vrrp group description text
6. vrrp group priority level
7. vrrp group preempt [delay minimum seconds]
8. vrrp group timers learn
9. exit
10. no vrrp sso

3.3.1.3 Experiment

The experiment consists four PCs and two Routers. The first step is the IP address configuration on interfaces of Router A and Router B is given below (figure 6,7).

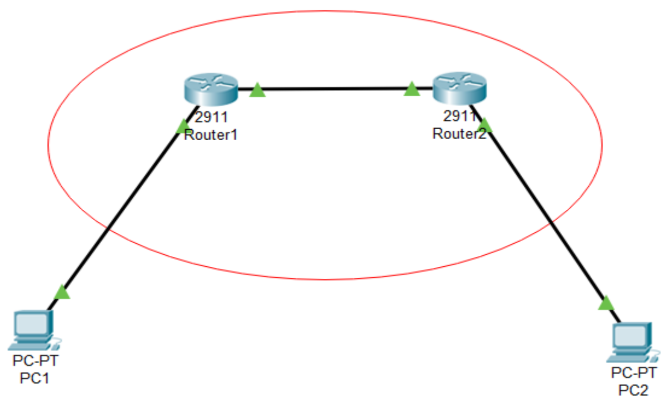


Figure 8_VRRP Diagram

Router A = Master for Group 1 & Backup for Group 5

VRRP Configuration

Router A

Interface Configuration

Router # configure terminal
Router(config)# **interface GigabitEthernet 1/0/0**
Router(config-if)# **ip address 10.1.0.2 255.0.0.0**

VRRP First Group Configuration with Clear Text Authentication:

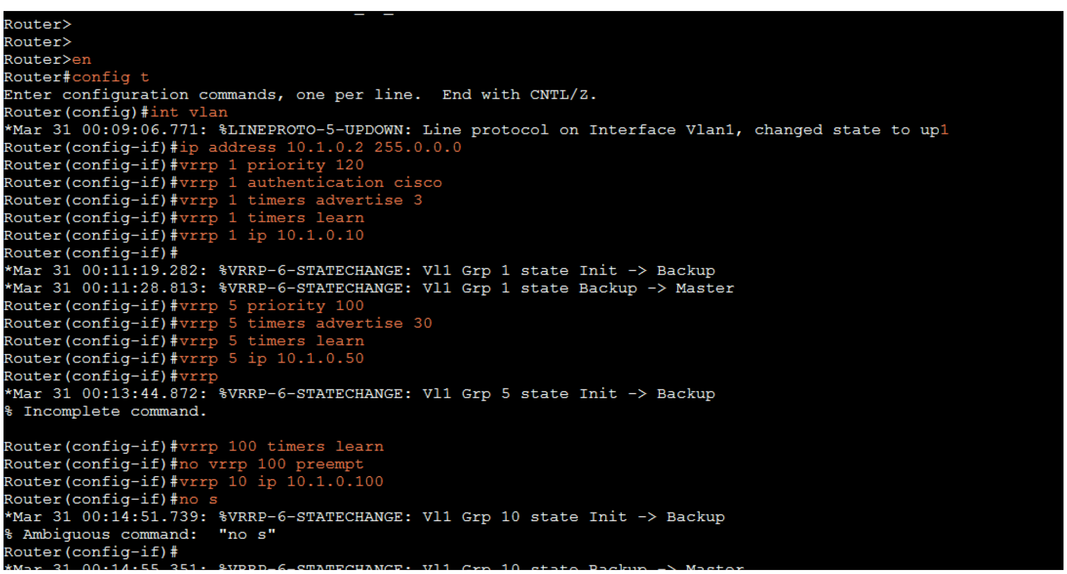
Router(config-if)# **vrrp 1 priority 200**
Router(config-if)# **vrrp 1 authentication cisco**

Router(config-if)# **vrrp 1 timers advertise 3**
Router(config-if)# **vrrp 1 timers learn**
Router(config-if)# **vrrp 1 ip 10.1.0.10**

VRRP Second Group Configuration

Router(config-if)# **vrrp 5 priority 100**
Router(config-if)# **vrrp 5 timers advertise 30**
Router(config-if)# **vrrp 5 timers learn**
Router(config-if)# **vrrp 5 ip 10.1.0.50**
Router(config-if)# **vrrp 100 timers learn**
Router(config-if)# **no vrrp 100 preempt**
Router(config-if)# **vrrp 100 ip 10.1.0.100**
Router(config-if)# **no shutdown**

Router A



```
Router>
Router>
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int vlan
*Mar 31 00:09:06.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up1
Router(config-if)#ip address 10.1.0.2 255.0.0.0
Router(config-if)#vrrp 1 priority 120
Router(config-if)#vrrp 1 authentication cisco
Router(config-if)#vrrp 1 timers advertise 3
Router(config-if)#vrrp 1 timers learn
Router(config-if)#vrrp 1 ip 10.1.0.10
Router(config-if)#
*Mar 31 00:11:19.282: %VRRP-6-STATECHANGE: Vl1 Grp 1 state Init -> Backup
*Mar 31 00:11:28.813: %VRRP-6-STATECHANGE: Vl1 Grp 1 state Backup -> Master
Router(config-if)#vrrp 5 priority 100
Router(config-if)#vrrp 5 timers advertise 30
Router(config-if)#vrrp 5 timers learn
Router(config-if)#vrrp 5 ip 10.1.0.50
Router(config-if)#vrrp
*Mar 31 00:13:44.872: %VRRP-6-STATECHANGE: Vl1 Grp 5 state Init -> Backup
% Incomplete command.

Router(config-if)#vrrp 100 timers learn
Router(config-if)#no vrrp 100 preempt
Router(config-if)#vrrp 10 ip 10.1.0.100
Router(config-if)#no s
*Mar 31 00:14:51.739: %VRRP-6-STATECHANGE: Vl1 Grp 10 state Init -> Backup
% Ambiguous command:  "no s"
Router(config-if)#
```

Figure 9_VRRP Configuration

Router B

The experiment consists four PCs and two Routers. The first step is the IP address configuration on interfaces of Router A and Router B is given below (Figure 6).

Router B = Master for Group 5 & Backup for Group 1

Router B
Interface Configuration

Router # configure terminal
Router(config)# **interface GigabitEthernet 1/0/0**
Router(config-if)# **ip address 10.1.0.1 255.0.0.0**

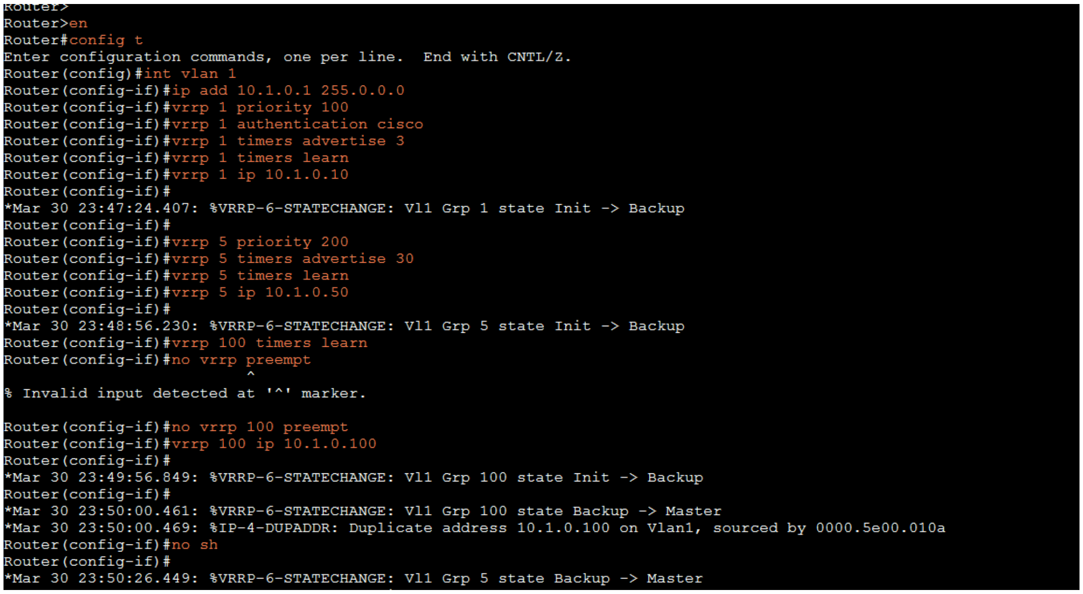
VRRP First Group Configuration with Clear Text Authentication

Router(config-if)# **vrrp 1 priority 100**
Router(config-if)# **vrrp 1 authentication cisco**
Router(config-if)# **vrrp 1 timers advertise 3**
Router(config-if)# **vrrp 1 timers learn**
Router(config-if)# **vrrp 1 ip 10.1.0.10**

VRRP Second Group Configuration

Router(config-if)# **vrrp 5 priority 200**
Router(config-if)# **vrrp 5 timers advertise 30**
Router(config-if)# **vrrp 5 timers learn**
Router(config-if)# **vrrp 5 ip 10.1.0.50**
Router(config-if)# **vrrp 100 timers learn**
Router(config-if)# **no vrrp 100 preempt**
Router(config-if)# **vrrp 100 ip 10.1.0.100**

Router(config-if)# **no shutdown**



```
Router>
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int vlan 1
Router(config-if)#ip add 10.1.0.1 255.0.0.0
Router(config-if)#vrrp 1 priority 100
Router(config-if)#vrrp 1 authentication cisco
Router(config-if)#vrrp 1 timers advertise 3
Router(config-if)#vrrp 1 timers learn
Router(config-if)#vrrp 1 ip 10.1.0.10
Router(config-if)#
*Mar 30 23:47:24.407: %VRRP-6-STATECHANGE: Vl1 Grp 1 state Init -> Backup
Router(config-if)#
Router(config-if)#vrrp 5 priority 200
Router(config-if)#vrrp 5 timers advertise 30
Router(config-if)#vrrp 5 timers learn
Router(config-if)#vrrp 5 ip 10.1.0.50
Router(config-if)#
*Mar 30 23:48:56.230: %VRRP-6-STATECHANGE: Vl1 Grp 5 state Init -> Backup
Router(config-if)#vrrp 100 timers learn
Router(config-if)#no vrrp preempt
                              ^
% Invalid input detected at '^' marker.

Router(config-if)#no vrrp 100 preempt
Router(config-if)#vrrp 100 ip 10.1.0.100
Router(config-if)#
*Mar 30 23:49:56.849: %VRRP-6-STATECHANGE: Vl1 Grp 100 state Init -> Backup
Router(config-if)#
*Mar 30 23:50:00.461: %VRRP-6-STATECHANGE: Vl1 Grp 100 state Backup -> Master
*Mar 30 23:50:00.469: %IP-4-DUPADDR: Duplicate address 10.1.0.100 on Vlan1, sourced by 0000.5e00.010a
Router(config-if)#no sh
Router(config-if)#
*Mar 30 23:50:26.449: %VRRP-6-STATECHANGE: Vl1 Grp 5 state Backup -> Master
```

Figure 10

For **Master/Backup** selection, **VRRP** priorities are configured. To manipulate VRRP selection and determine a Master manually, **VRRP Priority** values are important.

The Priority given for the Master Router is 200 while the Backup Router is 100. Router with higher priority will be elected as the virtual router master, and the one with lower priority as standby.

By default, preempt is on in VRRP which means that if a router that was master goes down, it loses mastership but if it comes up again, it becomes master without any config changes or intervention

After the configuration of the routers is done, the VRRP tested by turn of the Active router so the Backup Router (Standby Router) act as active (Figure 8).

```
*Mar 30 23:56:01.306: %IP-4-DUPADDR: Duplicate address 10.1.0.100 on Vlan1, sourced by 0000.5e00.010a
*Mar 30 23:56:31.305: %IP-4-DUPADDR: Duplicate address 10.1.0.100 on Vlan1, sourced by 0000.5e00.010a
*Mar 30 23:57:01.305: %IP-4-DUPADDR: Duplicate address 10.1.0.100 on Vlan1, sourced by 0000.5e00.010a
*Mar 30 23:57:31.305: %IP-4-DUPADDR: Duplicate address 10.1.0.100 on Vlan1, sourced by 0000.5e00.010a
*Mar 30 23:58:01.304: %IP-4-DUPADDR: Duplicate address 10.1.0.100 on Vlan1, sourced by 0000.5e00.010a
*Mar 30 23:58:30.168: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2, changed state to down
*Mar 30 23:58:31.180: %LINK-3-UPDOWN: Interface FastEthernet2, changed state to down
*Mar 30 23:58:37.656: %VRRP-6-STATECHANGE: Vl1 Grp 1 state Backup -> Master
```

Figure 11

After configuring the routers, the Wireshark application will show the working of the router which are configured with VRRP. The below screenshot shows that the data travels from PC to the Router A, the router A is chosen because the priority value of router A is 200 which greater than Router B default priority value 100. It shows that the network 10.1.0.1 is in active state and 10.1.0.2 is in standby state (Figure9).

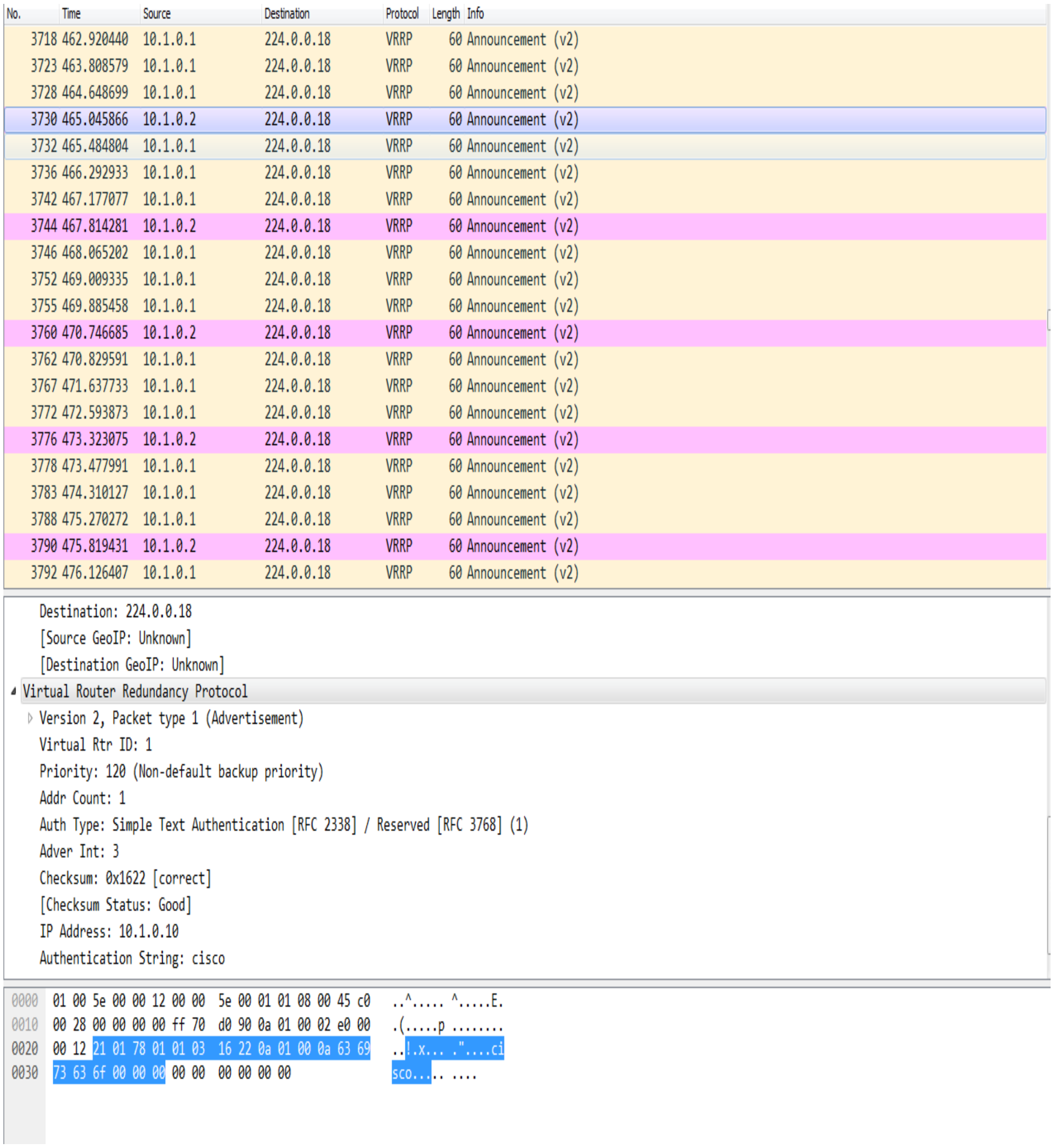


Figure 12_VRRP Status

3.3.2 Hot Standby Router Protocol (HSRP)

3.3.2.1 Basic Concept of HSRP

The HSRP stands for the protocol of hot standby router. The Cisco proprietary redundancy protocol is used to perform the default gateway tolerant to faults. This HSRP is the FHRP that allows a first-hop IP router to fail transparently. This HSRP gives redundancy for the IP host to the first-hop routing on an Ethernet network configured with the default IP address of the router. If the HSRP used to decide on the active router and the standby router in the router group. Within the router group, an active router is a router that routes packets and a standby router is a router that takes over simultaneously with an active router failure or a pre-set condition.[10]

3.3.2.2 The HRP working process is as follow

While HSRP is, it is the responsibility of a single router chosen from the group to forward the packets sent by hosts to the virtual router. This router is referred to as the Active router. As the Standby router, another router is chosen. If the Active router fails, the Standby assumes the Active router's packet forwarding duties. Although HSRP can be run by an arbitrary number of routers, only the Active router will forward the packets sent to the virtual router.[2]

A set of routers that run HSRP works in concert to present the illusion of a single default gateway router to the hosts on the LAN. This set of routers is known as an HSRP group or standby group. A single router that is elected from the group is responsible for the forwarding of 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.[8]

3.3.2.3 Experiment

The experiment consists two routers with two switches and two PCs. The figure below explains the topology. The both PCs are in different network. The router 0 set as active router and router 1 standby router (Figure 10).

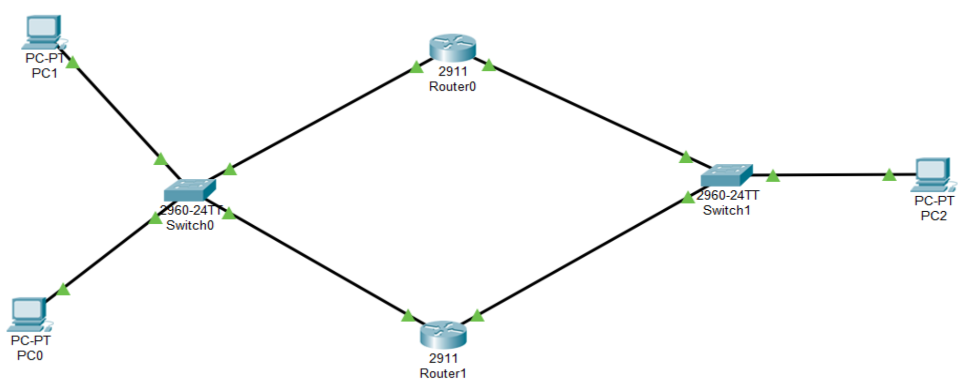


Figure 13_HSRP Diagram

Here, R1 is configured as an active HSRP default gateway & R2 is configured as the standby.

Configuration at Router 1

Interface Configuration

Router# configure t
Router (config)# interface gigabitethernet0/1
Router (config-if) # ip address 10.0.0.10 255.255.255.0

HSRP Configuration for Group 1 with preempt enable:

Router (config-if) # standby 1 ip 10.0.0.100
Router (config-if) # standby 1 priority 150
Router (config-if) # standby 1 preempt

HSRP Configuration for Group 2 with preempt enable:

Router (config-if) # standby 2 ip 10.0.0.150
Router (config-if) # standby 2 preempt
Router (config-if) # end

Configuration at Router 2:

Interface Configuration:

Router# configure t
Router (config)# interface gigabitethernet0/1
Router (config-if) # ip address 10.0.0.11 255.255.255.0

HSRP Configuration for Group 1 with preempt enable:

Router (config-if) # standby 1 ip 10.0.0.100
Router (config-if) # standby 1 priority 150
Router (config-if) # standby 1 preempt

HSRP Configuration for Group 2 with preempt enable:

Router (config-if) # standby 2 ip 10.0.0.150
Router (config-if) # standby 2 preempt
Router (config-if) # end

Here, the command preempt is configured on the both routers. Which means that if a router that was master goes down, it loses mastership but if it comes up again, it becomes master without any config changes.

In each router the configuration is set up, also the connection between the router and PCs are established by using the switches. After assign the IP address for each PC, the priority also assigned for each router.

As we can see in above HSRP Configuration Router R1 has highest PRIORITY than Router R2, so according to our configuration here Router R1 will work as Active Router and R2 will be Backup Router. If the active router fails, the standby assumes the packet forwarding duties.

Although an arbitrary number of routers may run HSRP, only the active router forwards the packets that are sent to the virtual router IP address. In order to minimize network traffic, only the active and the standby routers send periodic HSRP messages after the protocol has completed the election process.

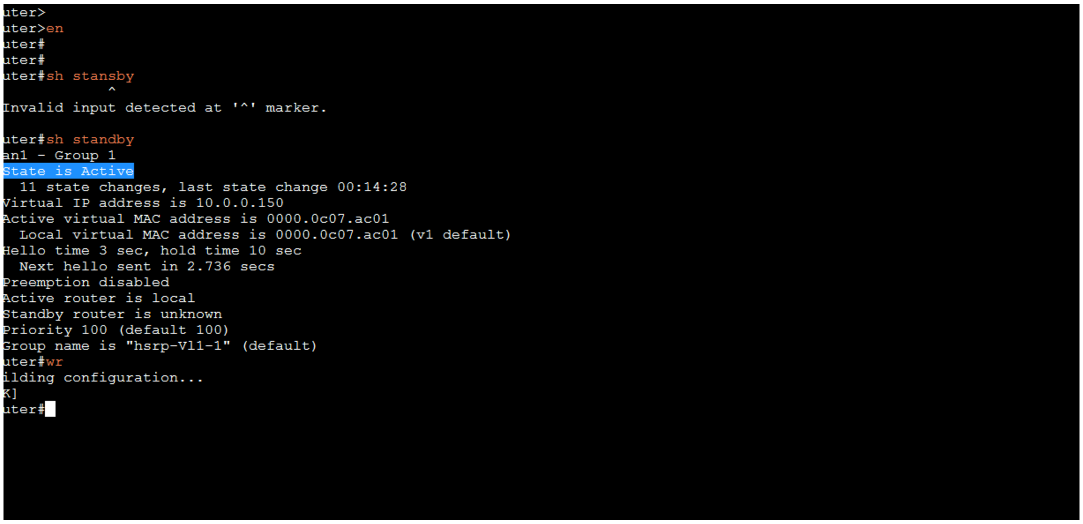


Figure 14_HSRP Status

HSRP is configured on the interface that is accepting traffic from hosts. Recall that the interface with the highest priority is elected the active router. To configure the priority of a router from its default of 100:
Router (config)# interface gi0/3
Router(config-if)# standby 1 priority 150

The standby 1 command specifies the HSRP group the interface belongs to (Figure11).

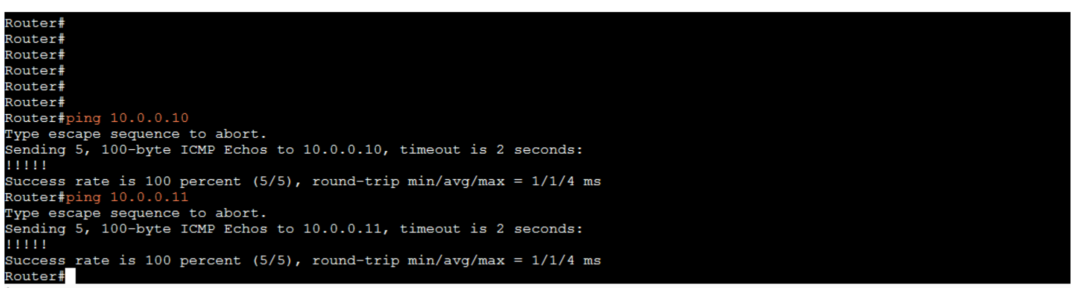


Figure 15_HSRP Status

After the configuration, provide some moment and then use the commands show standby brief and show standby on R2 and R1 to verify it. Here, R2 must be standby and R1 must be active router (Figure 13).

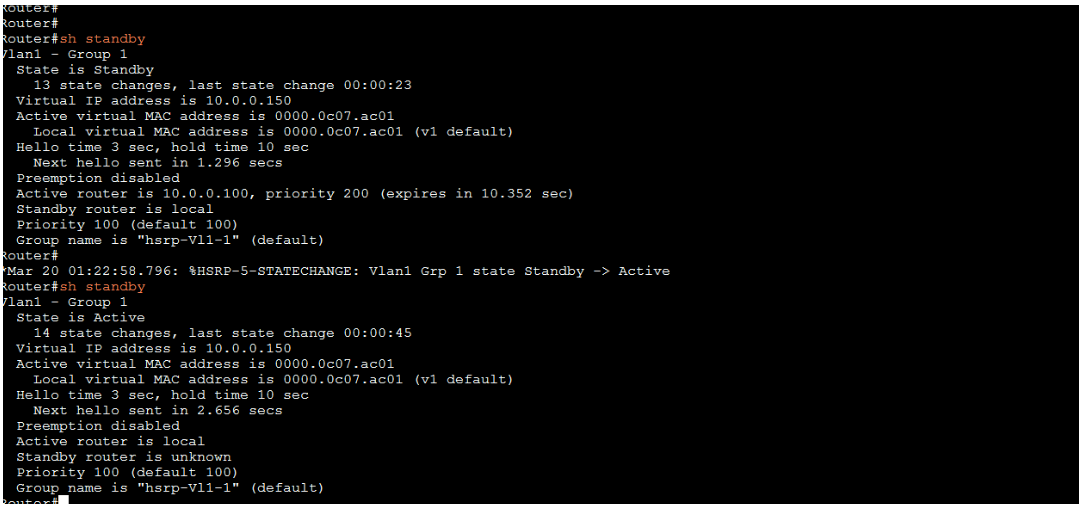


Figure 16_HSRP Standby

After configuring the routers, the Wireshark application will show the working of the router which are configured with HSRP. The below screenshot shows that the data travels from PC to the Router 1, the router 1 is chosen because the priority value of router 1 is 150 which greater than Router 2 default priority value 100 (Figure 14).

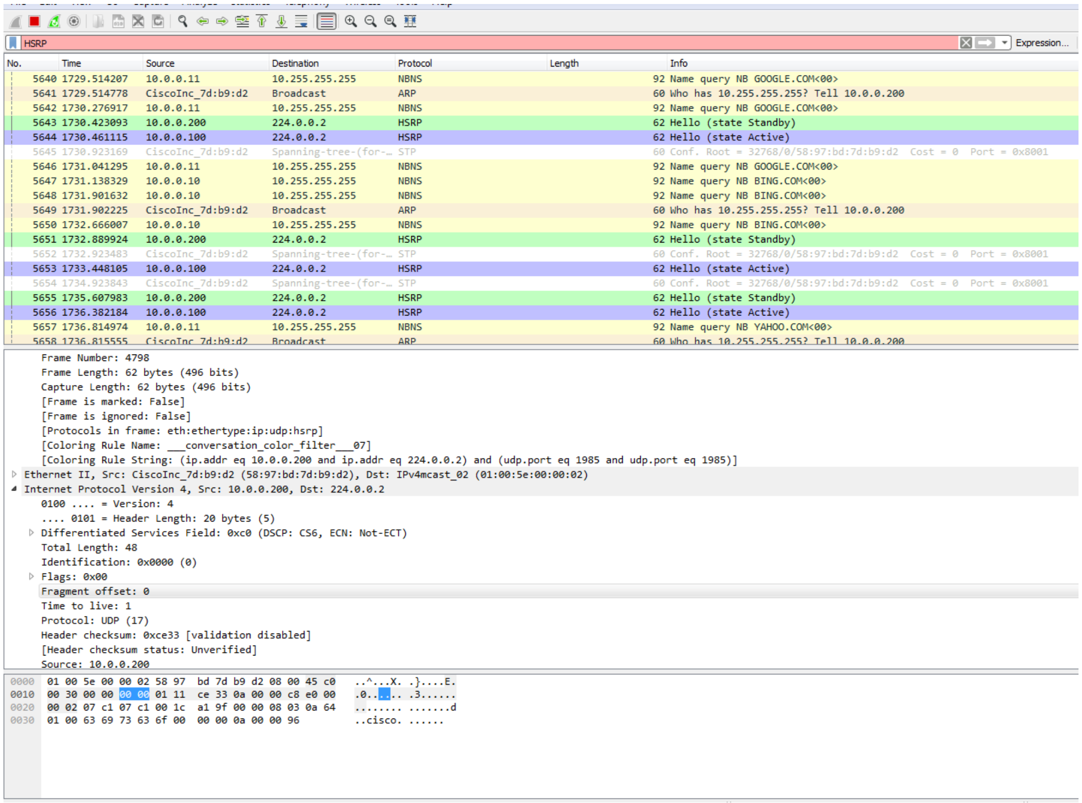


Figure 17_HSRP Wireshark

3.4 Testing

The goal of the test is to verify network recovery after a failed link in both HSRP and VRRP whose configuration has been demonstrated above.

A. VRRP Testing

Step1: Verify the configuration of VRRP on both the routers with below mention commands show ip vrrp

Router A will be as active for group 1 as priority has been set to 200 and Backup for group 5 and Router B will be as active for group 5 as priority has been set to 200 and Backup for group 1.

Step2: Shutdown the interface on Router A and check if Router B has been elected as Active router.

Router # config t
Router(config) # int gi1/0/1
Router(config-if) # shut

Check vrrp status again by using below command

show ip vrrp this time router B will be elected as an Active router.

Check connectivity by pinging gateway from host.

Step3: Bring back up the interface on Router A and status.

Router # config t
Router(config) # int gi1/0/1
Router(config-if) # no shut

Check vrrp status again by using below command

show ip vrrp the status will be the same as we have disable the preempt, Router B will be active, for router A to be active we need to disable router B interface.

B. HSRP Testing

Step1: Verify the configuration of HSRP on both the routers with below mention commands

show standby
show standby brief

Router 1 will be as active for active as priority has been set to 150 Router 2 will be as standby as priority is default.

Step2: Shutdown the interface on Router 1 and check if Router B has been elected as Active router.

Router # config t
Router(config) # int gi 0/1
Router(config-if) # shut

Check hsrp status again by using below command

show standby
show standby brief

Now u can see router 2 will be elected as active.

Check connectivity by pinging gateway from host.

Step3: Bring back up the interface on Router 1 and status.

Router # config t
Router(config) # int gi 0/1
Router(config-if) # no shut

Check hsrp status again by using below command

show standby
show standby brief

Now u can see router 1 is acting as an Active Router as preempt is enabled. Same procedure can check vice versa.

Chapter 4
Performance

4.1 High availability

High availability is a feature that keeps on operating continuously without any disaster to provide maximum uptime in network environment. It provides multiple functional gateways simultaneously, if one goes down other will take up in no time without end user interruption and without any human intervention. Everything works so quickly and automatically that end users or end user applications even don’t sense any network fluctuation or down time.

4.1.1 Why it is important

High availability is part and parcel in today’s networks because it provides redundancy into the networks and to user end applications. High availability is required equally on all tiers of networks whether it is access, distribution or core layer. Now days along with onsite redundancy, geo-graphical redundancy is also maintained so that if a site is hit by any natural disaster other site can take up and running, replica of sites is replicated to other geo-graphical locations.

4.1.2 Which Protocol are used

Number of protocols and techniques are used to achieve high availability in networks, some of which are given below.

A. HSRP

HSRP allows end users to access internet/other networks through multiple gateways available, for the purpose along with two physical layer three devices (Acting as Active and standby) a virtual layer three devices is also configured with a virtual MAC and virtual IP address. End user only knows the address of virtual layer three devices as gateway. Virtual router continuously monitors active device, if it goes down it makes the standby devices acting as active/primary gateway. HSRP is UDP based CISCO proprietary protocol.

B. VRRP

VRRP also does the same jobs as HSRP, the difference is it is an open standard protocol. It uses term Master (for Active Router) and Backup (for passive router).

4.1.3 Different between two protocols

There are some of the differences between both protocols (HSRP & VRRP) which are given below.

Table 4

HSRP	VRRP
Cisco Proprietary	Open Industry Standard
Uses Active & Standby terms	Uses Master & Backup terms
1 active, 1 standby	1 active, many backups
Authentication Supported	No longer supported.

4.2 Comparing Performance

In the above experiment for HSRP and VRRP below are the points on which performance can be monitored.

Table 5

Sr no	HSRP	VRRP
1	Cisco Proprietary	Open Standard
2	In above experiment default hello times has been used which is 3 sec	In above experiment default hello times has been used which is 1 sec, so VRRP has faster convergence.
3	1 Active router, 1 standby router & 1 or more router in listening state.	1 master and 1 or more backup routers.
4	In above experiment default hold timers has been used which is 10 sec	In above experiment default hold times has been used which is 3 sec, so VRRP has faster convergence.
5	Enabled preempt for router ownership takeover.	Disabled preempt as it was enabled by default.
6	Virtual IP has been used as gateway.	Highest IP address has been used as gateway.
7	Multicast address 224.0.0.2	Multicast address: 224.0.0.18

4.3 Working behavior and best practices of HSRP

In single point of failure environment all the network traffic is dependent to that single link, if goes down all the network traffic also gets stopped. To overcome this deficiency high availability protocols have been introduced. HSRP is the protocol used for high availability, main idea behind HSRP is to provide redundant paths to the destination so that if active path goes down standby will takeover in no time.

HSRP provides a virtual router with virtual IP and MAC addresses between two physical devices, the active device is considered in authority for controlling network and standby device keeps tracking active device, when active devices goes standby device will start controlling network traffic.

There is a criteria to select active device and standby device, the devices with highest priority (from 0-255) is considered the active and second highest is considered standby.

Conclusion

Both HSRP and VRRP are very similar and follow the same general rules. There are two big differences that affect the selection of one over the other. Whether all of the implemented devices are Cisco, and whether more than two devices are ever going to be configured onto a single LAN segment. If all of the current (or future) devices are not Cisco, then the selection of VRRP is easy, as (for the most part) HSRP is only widely supported on Cisco equipment, whereas VRRP is a standards-based solution and is supported by many different vendors. The other difference may not be that big of a deal on many networks because most don't have multiple routers that are connected to a single LAN segment. HSRP supports an active and standby device, which is typically enough to satisfy the requirements of obtaining enough redundancy.

However, VRRP does support more than two devices, and this can be helpful in those situations where multiple (more than two) are connected to the same LAN segment. Ultimately, the use of one of the FHRPs (generally) is a good common practice on LAN segments that require high uptime and where outages can be costly.

References

1. Priyanka, D. Shilpi, S. H., & Aabha, S. (2013). Review of First Hop Redundancy Protocol and Their Functionalities (01).
2. Cisco (Jan 19,2018) First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Release 3S (Cisco Site)
3. Juha, R. (2005). Router Redundancy and Scalability Using Clustering.
4. Christof Paar, Jan Pelzl & Bart Preneel (2010). Understanding Cryptography: A Textbook for Students and practitioners. Springer (Page 7) ISBN 364204100
5. Lehocine, M. B., & Batouche, M. (2018). Achieving efficiency in autonomic network management of IP networks based on SDN management logic. International Journal of Communication Networks and Distributed Systems, 20(4), (Page 484-518).
6. Huawei. (2012). VRRP Technology White Paper (01).
7. Cisco (Jan 19,2018) First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Series) (Cisco Site)
8. Cisco (2016) First Hop Redundancy Protocols (FHHP) (Cisco Site)
9. Veselý, V., Holuša, J. and Ryšavý, O.First-hop Redundancy Protocols in Omnet++.DOI: 10.5220/0006441503310339 In Proceedings of the 7th International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH 2017), pages 331-339
10. Exam Collection (2015) , Configuration Guide (Exam Collection Site)
11. S. Nadas, “Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6,” RFC 5798, March 2010.