A Virtual Router Schedule in the Practice of Creating Default Gateway

K. Jayachandra [#1], S. Prathap [*2]

[#1] *M.Tech 2nd year, Dept of CSE, AITS, Tirupati, AP, India*

[2*] *Assistant Professor, Dept of CSE, AITS, Tirupati, AP, India*

***Abstract*— we tend to discuss on Dynamic Time adjust Reference Load equalization technique to reinforce the Virtual Router Redundancy Protocol with Dynamic load equalization feature to utilize the redundant VRRP Backup device, in order to share the traffic load. Virtual Router Redundancy Protocol acts as default entry for the hosts on the shared Ethernet segment. VRRP protocol doesn't support the feature of load equalization for each the incoming and outgoing traffic. during this case, the Master VRRP device monitors the length of the incoming traffic from a selected Virtual native space Network (VLAN) section and redirects the traffic to the Backup VRRP device incase if the Master VRRP device still has the existing session supported the length of the flow of traffic and the variety of session through the Netflow cache information. whereas implementing Dynamic time correct reference Load equalization mechanism, the Master VRRP device redirects the traffic to Backup VRRP device through the ICMP airt message, encase there's an current session browsing the Master VRRP device by dynamically monitoring the Active Flow per Second parameter info through the Net flow cache data through the Layer three switch thereby achieving the Dynamic Load equalization feature with the utilization of existing Active Flow per Second timers to dynamically share the traffic load between the Master VRRP device and also the Backup VRRP device.**

***Keywords*— schedule, Gateway, Protocol, Router.**

I. INTRODUCTION

The section starts with distinguishing business goal, technical needs and optimizing the utilization of redundant devices. The effective and efficient use of infrastructure's redundant device in the network environment in order that failure of the only unit doesn't impact the network service offer by the LAN/WAN requests. Existing VRRP protocol is used by varied vendors however the feature that's not supported is that the load balancing feature, because of that the traffic from the User phase are processed only by the Master VRRP device and therefore the Backup

VRRP device method the traffic arp the first Master VRRP device fails in order that the gratuitous arp message is distributed to the end machine to update the Virtual Mac Address of the Backup VRRP device that has appropriated the role because the Master VRRP Device. The improvement of the present operating of VRRP protocol to include the load equalization feature to utilize the redundant Backup device to process the traffic till the Master VRRP device process the present client connection request that will significantly improve the performance of the Master VRRP device and reduce the CPU utilization. Throughout the logical network style design, the size of the network and traffic characteristics has to be thought of because the topology of the network design will vary from straightforward to complicated base on the number of VLAN Segments inside the infrastructure and variety of users connected within the VLAN Segment.

II.VRRP TRAFFIC FLOW TECHNIQUE

The Virtual Router Redundancy Protocol is implemented within the setting that has the redundant device within the distribution layer. The distribution layer switches that support the VRRP Protocol is Cisco 6500 series, 4500 series. VRRP configured with the scientific discipline Address is employed because the gateway for the end user machine amongst the redundant device. The active device is termed the Master VRRP device, whereas all others devices in the cluster are within the Backup state. The master device is selected on the idea of the device with the best device scientific discipline address within the VRRP group, in close if a particular device should be elective because the Master VRRP device priority within the VRRP cluster, then the priority is altered with the very best priority to influence the election of the Master VRRP device. The end user information processing system or the server uses the VRRP IP address because the default gateway to achieve the external network. VRRP protocol also are getting used at the Core layer of the Three-tier hierarchic network style model for the first path choice to the internet Service supplier (ISP), incase the primary path of the ISP has failing as a result of link problems or as a result of internal network outage within the ISP network then the VRRP dynamically identifies the presence of the interesting traffic to fall back to the redundant or secondary ISP to possess the connection to the external network or the VRRP is additionally used at the distribution layer of the Three-tier hierarchic network design thus that the Server/User Vlan section uses the VRRP information science address because the gateway to route the traffic to the intended destination. The VRRP protocol advertisements area unit sent each one seconds to poll the VRRP Devices to see the traffic is taken via the Master VRRP device and also the backup device area unit online or if they need gone down. The LAN segment implementation of the VRRP is taken into the consideration in order to demonstrate the recently incorporation of load equalization feature among the VRRP protocol. Current state of load equalization includes configuring the VLAN with two

totally different VRRP group so 1st VRRP group contains a higher priority in Switch A when put next to the priority within the Switch B whereas the second VRRP cluster has the higher priority in Switch B compared to the priority in the Switch A, in order that the end user nodes gets registered with the primary received arp message from the VRRP group one or cluster a pair of based on the Layer three device that receives the request. In order that the end user/server node gets the corresponding Virtual Mac Address related to the VRRP ip address. In VRRP there's no chase mechanism incorporated into the system in-order to notice the failure of the link or the interesting traffic.

This Virtual Router Redundancy Protocol (VRRP) [3] [4] [5] is designed to eliminate the single point of failure in the static default routing environment. VRRP became an IETF (RFC2338) standard in 1998. Since then, it has been widely used in a LAN environment to tolerate router/gateway failures. However, most implementations of VRRP today have been limited to a primary-backup configuration where no load balancing of traffic between the primary router and backup routers is supported. The master router in VRRP provides the routing function and sends heartbeat packets to the backup router. The backup router will start to route packets only when the master router fails. Since the backup router will be idle when there is no failure, the resource in the backup router is wasted most of the time.

The EVRRP (Enhanced VRRP) work is inspired from shortcomings of the previous RFC2338 VRRP. The major difference between EVRRP and VRRP is that EVRRP provides an efficient mechanism to do load balancing among routers without the need of running multiple VRRP daemons on each router. Furthermore, by modifying the VRRP state diagram and adding the election protocol to support multiple router cluster architecture, EVRRP further improves the scalability of the original VRRP protocol. EVRRP is backward compatible and supports all the original VRRP features such as pre-emption, virtual MAC, etc.

Election is invoked only when one of the backup routers discovers a failure of the master. In election, all backup routers will exchange election messages to determine which backup router should become the new master. While receiving an ELECTION message, any router in the backup state will compare its priority setting with the election message to see if it should become the master router. If a backup router receives an ELECTION message which has a higher priority than its own priority, the backup router will remain in the backup state. If the received packet priority is lower than its own priority, the backup router will keep on broadcasting ELECTION messages to check if any other router has a higher priority. After three rounds of sending election messages, the router who is surviving the election will become the master router. In the current VRRP protocol, there is no checking of the TYPE field in the VRRP control packet. The ELECTION packet will be received and treated as an advertisement packet. Therefore, the EVRRP election messages will be ignored in current VRRP to support the backward compatibility.

III. EVRRP LOAD BALANCING

There are at least two routers (primary and backup) in use at the same time in VRRP. It's a waste of resource if the backup router just listens to VRRP heartbeat messages without doing anything. In general, ICMP redirection [7] is used by a router to inform a client that there is a better path than sending packets to itself. The router sends an ICMP redirection packet to the client to point to another router. The EVRRP uses the ICMP redirection messages to redirect traffic to backup routers for load balancing.

The load balancing protocol in EVRRP is very straightforward: each backup router periodically sends EVRRP advertisement packets to the master router and the master router keeps a list of living backup routers. If the master router does not receive an EVRRP advertisement packet from a backup router for some time, the backup router is considered failed and is removed from the load-balancing router list. The master router checks all outgoing packets from hosts in LAN and determines what traffic should be redirected to backup routers. Besides using source and destination IPs as the redirection rule in prototype implementation, the redirection rule of EVRRP can be easily enhanced using destination IP, router load, traffic load, etc.

3.1. ADVERTISEMENT

Master router uses the advertisement message to send heartbeat packets to all backup routers. In EVRRP, a backup router also uses the advertisement control messages to inform the master router of its existence so that the master router can identify where the backup router is and redirect some of the traffic to the backup router

IV. ROUTER REDUNDANCY

The redirection algorithm, although simple, creates a new problem: what happens if a backup router fails while a host is sending packets through this failed backup router? As described earlier, if the master router does not receive a VRRP advertisement message from a backup router for some time, the backup router is considered failed and the master router will send a gratuitous ARP [8], which links the IP address of the backup router to the MAC address of the master router. Therefore, the master router could take over the job of forwarding packets for the failed backup router. As a result, without any change of configuration, a host can still send packets to WAN through the IP address of the failed backup router although the MAC address of this failed backup router IP address is now the MAC address of the master router. The usage of the gratuitous ARP in our protocol is to eliminate the router failure situation. We use ARP Poison to seamlessly move the traffic from a failed router to other working routers. There are 3 scenarios which will invoke the

ARP poison:

1. Backup Router Failure: Since there may be traffic dispatched to backup routers, if a backup router fails, the master router sends a gratuitous ARP to notify all hosts in LAN that the IP address of the failed backup router is now mapped to the MAC address of the master router.

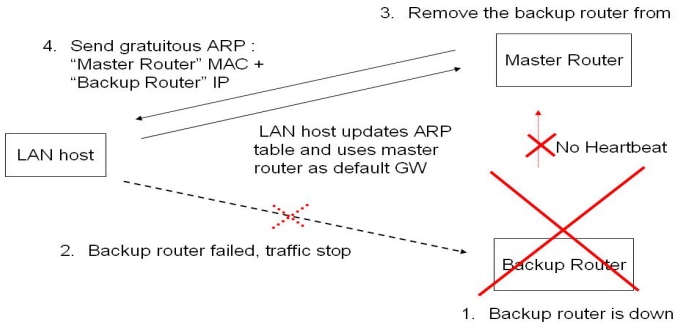

Figure 2. Backup Router Failed in EVRRP

2. Join of New Backup Router: If there is a new backup router joining the router farm, the master router needs to enlist the new router and distribute part of the traffic to the new router. The new joined router needs to broadcast its heartbeats to inform t he master router of its existence. Besides, backup routers must send gratuitous ARPs Periodically because the IP address of the backup router could have been mapped to the master router earlier.

3. Join of New Master Router: If a router becomes the master, it sends gratuitous ARP packets, using the Virtual IP address of the gateway and the virtual VRRP MAC address. The original master will be demoted to a backup. The demoted router needs to send a gratuitous ARP using its real IP address and MAC address to make sure that other hosts in LAN do not lose their WAN connections while the master router changes.

V.COMPATIBILITY WITH ORIGINAL VRRP

By inserting an original VRRP router into the EVRRP router farm to check the EVRRP backward compatible with VRRP, we can generalize them into three conditions, a VRRP router acts as a Master, Slave Router, or how does a VRRP work while receiving Election packets.

1. VRRP Router Acts as Backup Router:
When VRRP router acts as a backup router in EVRRP router farm, it can be functional okay but lack of load-balancing capability due to it does not send any heartbeats and master router cannot be aware of its existence. The VRRP router will ignore any other lower priority heartbeats which send by other EVRRP backup routers by default. And as long as there is a higher priority router sending heartbeat, the VRRP backup router will stay in Backup State.

2. VRRP Router Acts as Master Router:
After a VRRP router becomes the master router, the whole router farm will make no different between ordinary ones. The VRRP master router will route all traffic through itself since it has no load balancing capability. It will ignore all other Advertisement/Election packets because all the packets have lower priority bit.

3. VRRP Router Receives Election Packets:
The implementation of VRRP protocol supports only one type of packet, the ADVERTISEMENT packet. The EVRRP creates a new type of packet, ELECTION packet, which is almost identical with ADVERTISEMENT packet, is used when there is a new master router need to be elected. The current implementation of VRRP on Linux ignores the check of the type of VRRP packet since it assume there is only one type of packet and needless to check it. And also, the ELECTION packets received by original VRRP daemon can be viewed as useless packets and dropped without any error. Because the original VRRP state diagram does not support Election State, it must use the default ms_down_timer to make sure the Master router is down and then transit itself to the Master router.

VI. CONCLUSION

The VRRP protocol is an efficient fault tolerant networking solution and is widely used in LAN. Its simplicity and short fail-over time outperform other dynamic routing protocols such as RIP and deploying the protocol does not require any modification of network settings for hosts in LAN. However, VRRP does not support load-balancing and its scalability is limited. In our EVRRP effort, we show that the VRRP protocol can be extended easily and efficiently to support load balancing and high scalability. We believe that EVRRP protocol will be important for small to medium enterprise or campus networks as an economical solution to achieve high dependability in LAN. The EVRRP protocol as been extensively tested and used in our lab for almost one year. We are very confident in its correctness and robustness due to its simplicity, backward compatibility and the extensive testing of the protocol. In the near future, we intend to work with router manufacturers in Taiwan and submit the EVRRP work to IETF as an enhancement for RFC 2338 and RFC 3768.

REFERENCES

[1] J. Etienne, "VRRPd: overview, implementation and usage," Ottawa Linux Symposium 2001, July 2001.
[2] J. Ranta, "Router Redundancy and Scalability Using Clustering," Seminar on Internetworking, Spring 2004, eds.

A. Ylä-Jääski, N. Kasinskaja, [Online] Available: http://www.tml.hut.fi/Studies/T-110.551/2004/papers/Ranta.pdf, June 2004.
[3] R. Hinden, D. Mitzel, P. Hunt, P. Higginson, M. Shand, A. Lindem, S. Knight, D. Weaver and D. Whipple, "Virtual Router Redundancy Protocol," Internet Draft, draft-ietfvrrpspec- v2-06.txt, Feburary 2002.
[4] [VRRP] R. Hinden, Ed., "Virtual Router Redundancy Protocol," RFC 3768, April 2004.
[5] [VRRP] S. Knight, D. Weaver, D.Whipple, R.Hinden, D. Mitzel, P. Hunt, P. Higginson, M. Shand, and A. Lindem, "Virtual Router Redundancy Protocol," RFC 2338, April 1998.
[6] [HSRP] T. Li, B. Cole, P. Morton and D. Li, "Cisco Hot Standby Router Protocol (HSRP)," RFC 2281, March 1998.
[7] [ICMP] J. Postel, "Internet Control Message Protocol," RFC 792, September 1981.
[8] [ARP] D. Plummer, "An Ethernet Address Resolution Protocol," RFC 826, November 1982.
[9] VRRPd Linux Implementation, ImageStream Internet Solution, Inc., http://www.imagestream.com/VRRP.html
[10] Chariot, NetIQ Corporation, http://www.netiq.com/products/chr/default.asp
[11] Gentoo Linux, Gentoo Foundation, Inc., http://www.gentoo.org
[12] Avalanche 220™ and Reflector 220™, Spirent Communications, http://www.spirentcom.com