

Campus Network Based on VRRP Redundancy and Reliability

Xiao-qi Yin, Yi-zhuo Guo

Department of Computer Science and Technology,
Cheng-Dong College of Northeast Agricultural University
Harbin, 150025, China
Yinxiaoqi1981@163.com

Abstract—With the dramatic increase in amount of information in campus network, the security and high reliability of access data have become urgent requirements on redundancy reliability design of campus network. This paper adopts the technology of VRRP and takes advantages of double backup sets and router to process the design and configuration. As is shown in the experiment, when one device fails, the other ones can still complete relevant operations under the conditions of double backup sets. Therefore, the redundancy reliability design of campus network can be realized through the technology of VRRP double backup sets.

Keywords- Campus network, VRRP, Reliability

I. INTRODUCTION

At present, the technologies adopted by each university in the redundancy reliability design are mainly HSRP and VRRP. Through a detailed analysis, great differences can be found between them. VRRP and HSRP are quite familiar in function, but VRRP enjoys one principle advantage: it allows devices in VRRP set to establish authentication mechanism. In addition, HSRP requires that the virtual router cannot be the IP address of the one of the routers, but VRRP allows such condition. Moreover, VRRP does not adopt coup or equivalent message of HSRP. The state machine of VRRP is simpler than the one of HSRP. HSRP has 6 states of Initial, Learn, Listen, Speak, Standby, Active and eight events. VRRP has only 3 states of Initialize, Master, Backup and five events. HSRP loads messages on UDP, while VRRP loads them on TCP (HSRP uses UDP 1985 port, and sends hello to multicast address 224.0.0.2). Therefore, the design adopts the technology of VRRP double backup sets owing to the fact that it is impossible for a campus network of common size to be equipped with high-end devices. The reliability of a network shall be ensured by the reliability of the device itself. In the process of campus network construction, most of the designers concentrate on the speed and performance of the network, and neglect the issue of router's single point failure. Once any failure occurs, the speed and function of network make no sense. Otherwise, the double backup sets of VRRP pose no requirements on any change of the network state or configuration of the host machine. The backup of next hop gateway can be realized simply by the configuration of several orders on relevancy routers, which will not bring any burden to the host machine. Compared with other methods, VRRP can better satisfy the demand of users. In order to avoid the problem of network interruption, the technology of VRRP shall be applied reasonably on the

basis of ensuring speed and function.

II. RELEVANT OPERATION

VRRP put several routers into one backup set so as to form one virtual router. Among all the backup methods of Master and Backup in VRRP, the gateway function shall be born by the Master router alone. When failures occur to the Master router, the other Backup routers will select one router through VRRP to take the work of the Master over. If there is still one router works properly, the virtual router can function normally. VRRP is one kind of fault-tolerant protocol, which can simplify the configuration of the host machine while increasing reliability. The messages of VRRP protocol are sent through the fixed multicast address 224.0.0.18. Among LANs with multicast or broadcast capacity, VRRP can still provide a reliable default link, thus network interruption due to a single point of failure of the gateway can be avoided. Moreover, there is no need to change the dynamic routing protocol, router discovery protocol and other configuration information. If one wants to gain a profound understanding about VRRP, he or she must fully understand its functions and state machine of VRRP protocol.

A. Functions of VRRP

1) Backup of Master and Backup: this is the basic method for VRRP to provide the function of IP address backup. It requires the establishment of a virtual router which consists of one Master and several Backup devices. Normally, all the services shall be borne by the Master. When the Master fails, the Backup devices will take it over.

2) Load sharing: a router allows to backup for several sets. Virtual router enables several routers to share the services at the same time.

3) Monitoring Port State: VRRP can monitor the state of all ports. When the state of the port being monitored is Down or Up, the priority level of the router will decrease or increase to certain value automatically, thus the priority level of each device within the backup set will be changed and VRRP router can conduct elections for Master again.

4) VRRP Quick Switch: BFD (Bidirectional Forwarding Detection) can quickly detect and monitor the connection state of links or IP router within the network. By monitoring the session state of BFD, VRRP can keep the switch time between Master and Backup within 1 second.

5) Ping Switch of Virtual IP Address: it is not regulated by RFC3768 that virtual IP address should be Ping or not. If the virtual IP address cannot be connected by Ping, it will

bring trouble to the working condition of virtual router. If the virtual IP address can be connected by ping, the working condition of the virtual router can be monitored conveniently but it may bring hidden danger of attack by ICMP.

6) Security Function of VRRP: for network environment of different grades of security, different authentication methods and authentication words can be set of header. In a safe network, default setting can be adopted. In a network with a security threat, VRRP provides simple word authentication and can set up authentication words whose lengths are between 1 and 8.

7) VRRP Management Set: While configuring large amount of VRRP backup sets, too many messages of VRRP protocol will take up relatively large link bandwidth, and the treatment of the large amount of VRRP messages will bring burden to the system. Each VRRP backup set requires the maintenance of protocol timer, which is a great burden for the system. VGMP refers to The VRRP Group Management Protocol. The VRRP management suites, which are established on the basis of VGMP, will be in charge of managing the states of all VRRP backup set, so as to ensure that the ports of one router are in the states of Master and Backup at the same time and realize the consistency of VRRP state.

B. VRRP Protocol State Machine

Three state machines are defined by VRRP protocol: Initialize, Master and Backup. Among them, the messages sent to the virtual IP address can only be transmitted by devices in active state. The VRRP state switch is shown in Fig. 2-1.

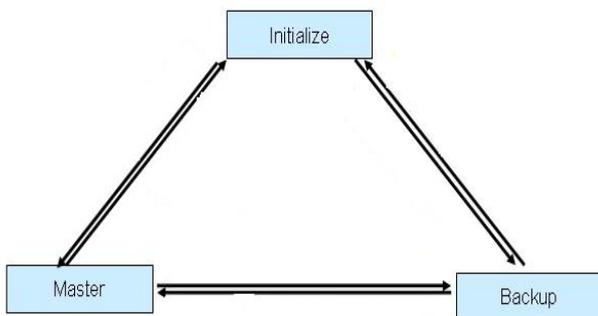


Fig. 2-1 VRRP state switch

1) Master: when the router is in Master state, it will send VRRP message regularly, respond to the call of ARP on the virtual IP address from the virtual MAC address, and transmit target MAC address as an IP message of virtual MAC address. If it is the owner of the virtual IP address, the received target IP address shall be the IP message of such virtual IP address. Otherwise, this IP message shall be discarded. If a message about larger priority level is received, it will switch to Backup state. Moreover, if a message of the same priority level is received and the main IP address of the transmitting end is greater than that of itself, it will switch to Backup state. When the Shutdown event of the port is received, it will change into the state of

Initialize.

2) Backup: When the router is in Backup state, the VRRP message sent by Master shall be received to judge whether the state of the Master is normal or not. The ARP request on the virtual IP address will not be replied. Discard target MAC address as the IP message of virtual MAC address. Discard target IP address as an IP message of virtual IP address. In the state of Backup, if messages of lower priority level are received, discard such messages and do not reset the timer; if messages of the same priority level are received, reset the timer and compare IP addresses further. Only when the Backup receives any overtime event of the MASTER_DOWN_TIMER, can it change into Master state. If it receives a shutdown event of the port, it can change into Initialize.

3) Initialize: When the device is started, it will enter such state. When the Startup message of the port is received, it will switch to Backup or Master state (if the priority level of the IP address owner's port is 255, it will switch to Master directly). Under such condition, all treatment to VRRP is available.

C. VRRP Reliability Design of Campus Network

Generally, all host machines within the same segment of campus network are equipped with one same default router with gateway as next hop. The messages sent to other segments by host machine will be sent to a gateway through default router, and then transmitted by the gateway again, thus the communication between the host machine and exterior network is realized. When the gateway fails, all the host machines with gateway as default router cannot communicate with exterior network. Due to the particularity of the campus network, the method of double backup sets of VRRP shall be adopted. Both Master and Backup devices use a MSR30-20 router of H3C. SWA and SWB connect with each other by the Ethernet network with them. However, The Internet connects to exterior network through V3.5 cable. SWA and SWB belong to Backup Set 1 with IP address of 192.168.0.254 and Backup Set 2 with IP address of 192.168.1.254 respectively. When SWA and SWB work normally, the flow of Vlan 10 of LAN will be transmitted through SWA and the one of Vlan 20 of LAN will be transmitted through SWB. The detailed topology is shown in Fig. 2-2.

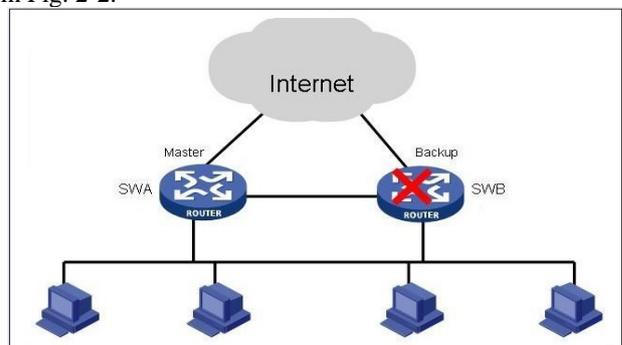


Fig.2-2 The detailed topology of VRRP Switch SWA is configured as follows:

```
[SWA]VLAN 10
[SWA]interface vlan-interface 10
[SWA-vlan-interface10]ip add 192.168.0.252 255.255.255.0
[SWA-vlan-interface10]vrrp vrid 1 virtual-ip 192.168.0.254
[SWA-vlan-interface10]vrrp vrid 1 priority 120
[SWA-vlan-interface10]vrrp vrid 1 preempt-mode
[SWA]VLAN 20
[SWA]interface vlan-interface 20
[SWA-vlan-interface10]ip add 192.168.1.252 255.255.255.0
[SWA-vlan-interface10]vrrp vrid 2 virtual-ip 192.168.1.254
[SWA-vlan-interface10]vrrp vrid 2 priority 100
[SWA-vlan-interface10]vrrp vrid 2 preempt-mode
Switch SWB is configured as follows:
[SWB]VLAN 10
[SWB]interface vlan-interface 10
[SWB-vlan-interface10]ip add 192.168.0.253 255.255.255.0
[SWB-vlan-interface10]vrrp vrid 1 virtual-ip 192.168.0.254
[SWB-vlan-interface10]vrrp vrid 1 priority 100
[SWB-vlan-interface10]vrrp vrid 1 preempt-mode
[SWB]VLAN 20
[SWB]interface vlan-interface 20
[SWB-vlan-interface10]ip add 192.168.1.253 255.255.255.0
[SWB-vlan-interface10]vrrp vrid 2 virtual-ip 192.168.1.254
[SWB-vlan-interface10]vrrp vrid 2 priority 120
[SWB-vlan-interface10]vrrp vrid 2 preempt-mode
```

III. EXPERIMENT ANALYSIS AND RESULTS

After completing the design and configuration of VRRP, the VRRP state check on SWA and SWB can be conducted with the use of display vrrp verbose.

```
<SWA>dis vrrp verbose
IPv4 Standby Information:
Run Method      :VIRTUAL-MAC
Total number of virtual routers: 2
Interface       : Vlan-interface10
VRID            : 1
Admin status    : UP
Config pri      : 120
Preempt Mode    : YES
Auth Type       : NONE
Track IF        :Vlan100
Virtual IP      : 192.168.0.254
Virtual MAC     : 0000-5e00-0101
Master IP       : 192.168.0.252
Adver. timer    : 1
State           : Master
Run pri         : 120
Delay Time      : 0
Pri Reduced     : 30

Interface       : Vlan-interface20
VRID            : 2
Admin status    : UP
Config pri      : 100
Preempt Mode    : YES
Auth Type       : NONE
Virtual IP      : 192.168.1.254
Master IP       : 192.168.1.253
Run Method      : VIRTUAL-MAC
IPv4 Standby Information:
```

Fig.3-1 SWA validation results

```
<SWB>dis vrrp verbose
IPv4 Standby Information:
Run Method      :VIRTUAL-MAC
Total number of virtual routers: 2
Interface       : Vlan-interface10
VRID            : 1
Admin status    : UP
Config pri      : 100
Preempt Mode    : YES
Auth Type       : NONE
Virtual IP      : 192.168.0.254
Master IP       : 192.168.0.252
Adver. timer    : 1
State           : Backup
Run pri         : 100
Delay Time      : 0

Interface       : Vlan-interface20
VRID            : 2
Admin status    : UP
Config pri      : 120
Preempt Mode    : YES
Auth Type       : NONE
Virtual IP      : 192.168.1.254
Virtual MAC     : 0000-5e00-0102
Master IP       : 192.168.1.253
Run Method      : VIRTUAL-MAC
IPv4 Standby Information:
```

Fig.3-2 SWB validation results

By comparing Fig. 3-1 and Fig. 3-2, it can be found that SWA is the Master device of VRRP Backup Set 1. The virtual IP address of Backup Set 1 is 192.168.0.254. SWA is the Backup device of VRRP Backup Set 2. The virtual IP address of Backup Set 2 is 192.168.1.254. Thus, we can know that SWB is the Backup device of VRRP Backup Set 1, and the virtual IP address of Backup Set 1 is 192.168.0.254. SWA is the Master device of VRRP Backup Set 2 and the virtual IP address of Backup Set 2 is 192.168.1.254. For the convenience of understanding, we can use one chart to illustrate the relations between the two routers, as is shown in TABLE I.

TABLE I. The Master and Backup Relations between Devices of Double Backup Sets

Device	Virtual group	
	VRRP 1	VRRP 2
SWA	Master	Backup
SWB	Backup	Master

Since the Internet part of this design has already been completed, we can still communicate with the Internet when any failure occurs to SWB. For example, ping via www.163.com. It can pass the test no matter it is conducted on which machine within the campus network. Thus, it is proved that the flows of Vlan10 and Vlan20 have been transmitted by the SWA. Through the experiment and proof procedures above, we can believe that the reliable design of VRRP plays a role of protection and has reached the requirements of redundancy reliability design for campus networks.

IV. CONCLUSION

Through the application of VRRP protocol in campus networks, default router with higher reliability can be achieved without any change of network conditions or allocation of any dynamic router and router discovery protocol on the host machine. The consistency and reliability of communication are realized by switching services to other devices, which can effectively avoid

single point failure in the network and provides a stable, fast and reliable campus network system. However, special attention must be paid to setup for the notice period. If it is set improperly, it may lead to frequent election of VRRP and result in network interruption instead of increase in reliability. In practical application, we should try to allocate devices with high reliability to increase reliability of the devices themselves. At the same time, the reliability of the network can be further increased through the use of VRRP protocol.

REFERENCES

- [1] Baoqing Pu. A Solution to Improve Reliability of Campus Network by VRRP. *Journal of Gansu Normal College*, pp.2011
- [2] Dong Wang. Router Redundancy and Load Balance of Campus Network Governed by the VRRP. *Journal of Chongqing University of Science and Technology(Natural Science Edition)*, 2010
- [3] Yingguo Zhu, Senlin Jiang. The Construction of High Reliability Data Center of Colleges and Universities Based on VRRP. *Journal of Wuxi Institute of Technology*, 2008,pp. 45-46
- [4] Lan Zhang, Junliang Wang. On the Application of VRRP in Enterprise Network. *Science and Technology Innovation Herald*, 2010,pp.249-251.
- [5] Fenge-Wang and Chang-xing-Zhu, HSRP Protocol Based on High Reliable Redundant Campus Network Design , *Communications and Information Processing , Communications in Computer and Information Science*, 2012, pp.107-114
- [6] C. Nuangjamong, S. P. Maj and D. Veal.Resource Redundancy – A Staffing Factor using SFIA , *Innovations and Advances in Computer Sciences and Engineering*, 2010, pp.31-35