IGNITION
DESIGN LABS

VRRP Solution

Technical White Paper V1.1

Disclaimer

© 2024 Ignition Design Labs. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ignition Design Labs ("IDL"), or as expressly provided by under license from IDL.

This documentation and all information contained herein (“material”) is provided for general information purposes only. IDL and its licensors make no warranty of any kind, express or implied, with regard to the material, including, but not limited to, the implied warranties of merchantability, non-infringement and fitness for a particular purpose, or that the material is error-free, accurate or reliable. IDL reserves the right to make changes or updates to the material at any time.

Limitation of Liability

In no event shall IDL be liable for any direct, indirect, incidental, special or consequential damages, or damages for loss of profits, revenue, data or use, incurred by you or any third party, whether in an action in contract or tort, arising from your access to, or use of, the material.

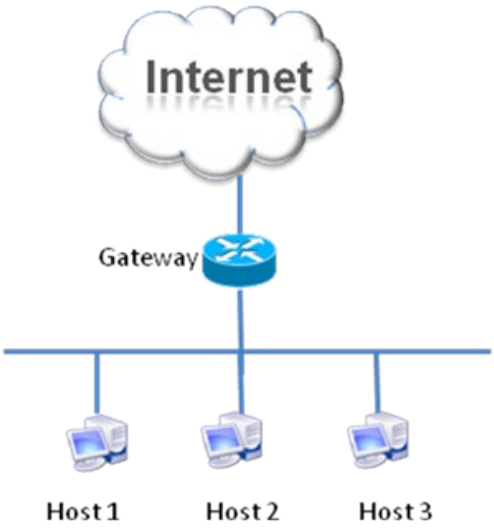
Website:

https://ignitiondl.com/

Table of Contents

Chapter 1 Background

With the development of the Internet, users require more diverse experiences as well as faster and more stable network services, which put forward higher requirements for network redundancy, reliability and recovery. Users require real-time communication with the network. Even if a failure occurs, the connection should recover immediately without user perception.



Normally, the host communicates with the external network through the gateway. When there is a failure on the gateway, the host loses contact with the external network. Adding a new gateway can solve this problem, but it needs the administrator to manually configure it, because mostly one host can only configure one default gateway. With complex configurations and low security and reliability, these dynamic routing protocols (such as RIP and OSPF) cannot meet the demand of users, neither.

Virtual router redundancy protocol (VRRP) is a better solution to this problem. No any manual configuration or change of the network structure is required. Only a few configurations on the gateway router are needed. Apparently, VRRP reduces the workload of network configuration and meets the demand of users.

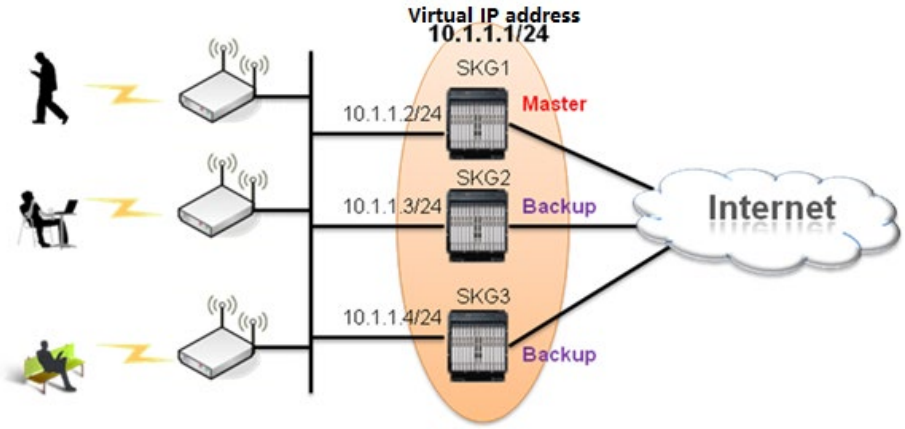
Chapter 2 VRRP Introduction

VRRP is put forward by IETF which solves the single point failure when configuring the static gateway in the local area network (LAN).

2.1 Overview

The VRRP protocol in the LAN is grouped into a set of multiple routers, called the VRRP backup group. The VRRP backup group is logically equivalent to a virtual router identified by the virtual router ID number. The virtual router has its own IP address and MAC address. The host in LAN configures the IP address of the virtual router as the next-hop default gateway to communicate with the external network.

The virtual router, composed of multiple routers, can be divided into a master router and several backup routers. The VRRP router which controls the IP address of virtual router is the master router, which is responsible for data packet forwarding. Once the master router is not available, the backup router with the highest VRRP priority replaces the master router and is responsible for data packet forwarding. The selection process provides a dynamic failover mechanism, allowing the virtual router's IP address to be the default first-hop router of the terminal host, as shown in the figure below.



2.2 Explanation

The following table lists the explanation of several key nouns.

Item	Description
Virtual router	It includes a master router and multiple backup routers, as the host default gateway of the next hop. In one router group, the virtual router can define multiple virtual routers.
Master router	It is a router in the state of Master router, which is responsible for packet forwarding.
Backup router	It is the router in Backup state, which might consist of multiple routers. Once the master router fails, one of the backup routers can serve as the master router and continue forwarding packets.
VRID	It is virtual router ID. In a VRRP backup group, each router has the same VRID. Therefore routers with the same VRID belong to the same virtual router. A router can have multiple VRIDs, which means it can belong to multiple virtual routers and therefore be able to configure multiple virtual addresses.
Virtual IP address	VRRP assigns an IP address for a virtual router as a virtual router interface address, which is a virtual IP address. Virtual IP address can be either one of the router interface addresses, or the address of a third party. If the third party address is used, the router with the highest priority is the master router. If two routers have the same priority, the router with a larger interface IP address becomes the master router.
IP owner	When the interface IP addresses of the virtual IP address and the backup group are the same, the router is referred to as the IP owner.
Virtual MAC address	VRRP assigns a MAC address for the virtual router in the format of 00-00-5E-00-01-{VRID}.
VRRP priority	The replacement of router is based on the VRRP priority, whose value range is 0~255 (larger value has a higher priority) and configurable range is 0~254. 0 is reserved for routers that give up as master router. 255 is reserved for the IP owner. Therefore, when the router is the IP owner and works properly, it will always be the master router. When the master router fails, the router with highest priority replaces the master router, undertaking the packet forwarding.
Backup router working mode	It is divided into the preemptive mode and the nonpreemptive mode. In preemptive mode, when a backup router receives the VRRP packets, it will compare its own priority with that in the packets. If its own priority is higher, this backup router will preempts as the master router and the original router will be a backup router. Otherwise, they keep the original state. In the non-preemptive mode, even if the backup router has a higher priority than the master router, as long as no fault occurs in the master router, the backup router with the highest priority still does not preempt master router but keeps the backup state.

2.3 VRRP Operational Process

The VRRP operation process is as described below:

Step 1 According to the VRRP priority (comparing the IP address given that the priorities are the same), select a master router. The master router notices the virtual MAC address to the adjacent equipment or host, and then begins the packet forwarding.

Step 2 Master router, with configured periodic announcement VRRP packets, notifies the backup router configuration information and status.

Step 3 If the master router fails, the backup router selects a new master router according to VRRP priority. By sending a free ARP packets which contains a virtual IP address and MAC address, the new master router can update adjacent equipment or host information, and the host in the LAN will not have any awareness of this router switch.

Step 4 If the VRRP priority of the backup router is higher than that of master router and the master router does not fail, the operation mode of the backup router (preemptive and non-preemptive) decides whether to switch the VRRP state.

2.4 Router Selection

According to VRRP priority, VRRP determines which router will be the master router. The router with the highest priority is the master router, and the rest are backup routers. When the master router fails, the backup router with highest priority will replace the master router.

- The initialized VRRP router in the backup state, learns other routers VRRP priority through the VRRP packets interaction.
- If the priority of the master router in the VRRP packets is higher than that of itself, the router keeps in backup state.
- If the priority of the master router in the VRRP packets is higher than itself, the router under preemptive mode will preempt master router; the router under non-preemptive mode of the router will keep its original state.
- If a router does not receive VRRP packets after a while, then this router will become the master router. The default waiting time of the backup router is called Master_Down_Interval, the value of which is: (3 x interval of VRRP packets sending) + switch time of the backup router (Skew time). The unit is second.

2.5 Router State

- The master router periodically sends VRRP packets, reporting its configuration information and working condition in the network. The backup router according to the received VRRP packets determines if the master router is working properly.
- When the master router initiatively forgoes the master position, it sends VRRP priority 0 message to other routers to switch the backup router to a master one. The time that the backup router switching to the master router is called Skew time. The calculation method is: (256-backup router priority) / 256. The unit is second.

- When the master router fails to notice, the backup router updates itself as a master router and periodically sends VRRP packets after waiting for a certain period of time (3 * notice time + Skew time = Master_Down_Interval), receiving no VRRP packets and confirming that the master router cannot work. The notice time of all equipment within the VRRP group must be consistent, otherwise the VRRP cannot work (the status will become Master).
- Among backup routers with the same priority, the one with the largest IP address becomes the master router.

2.6 VRRP Preemption and Delay Time

In the unstable network, network congestion may lead to that the backup devices fail to receive the VRRP notification message during the Master_Down_Interval and the backup takes the initiative to switch to Master. If the notification message of the original Master VRRP reaches to the original backup, and then the new Master switches to backup. The frequent switching of VRRP Master may take place, which leads to the unstable network. In order to alleviate the occurrence of this phenomenon, you can configure delay-time in the preemptive mode, which makes the Backup device continues to wait for preemptive time after the Master_Down_Interval.

2.7 VRRP Tracking

VRRP Tracking mechanism tracks the specified physical interface, layer 3 interface (VLAN), IP track status, route and VRRP backup group. According to the network conditions, different Tracking strategies can be used to trigger the master router's priorities change, and thus to realize the switch between the master and backup routers. For example, if the specified tracked interface fails, the VRRP automatically lowers or higher the priority of the master router according to the configuration information.

Chapter 3 Implementation and Advantages

In order to guarantee the reliability of the network and to avoid the single point failure of the static gateway, the AC series multiple service gateway uses VRRP protocol to realize the redundant backup function.

3.1 AC Tracking and VRRP Priority Modification

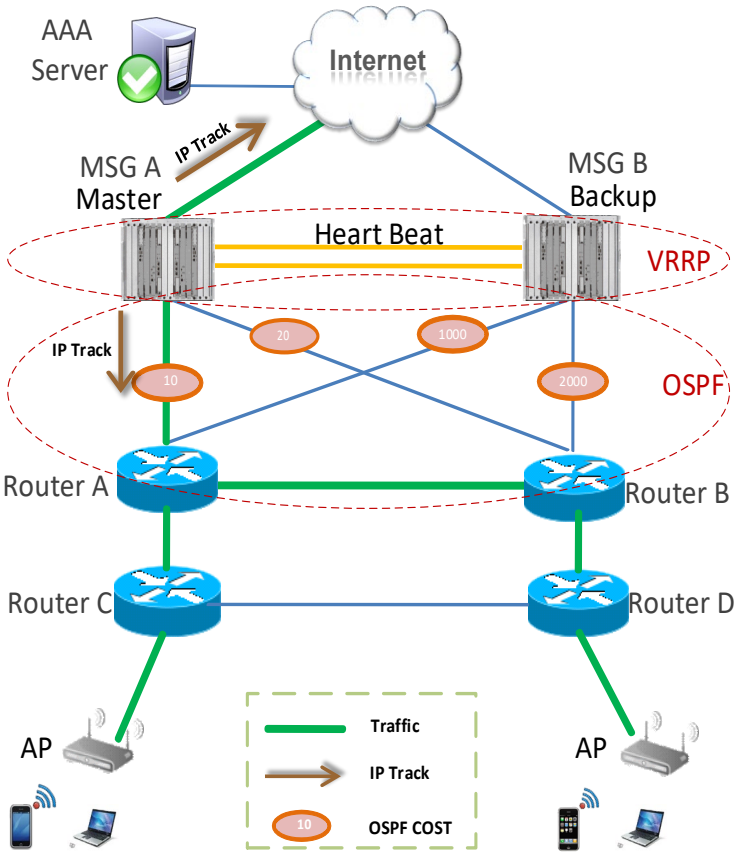
VRRP protocol can detect the upward or downward interface state of the layer 2 and layer 3 through its own Tracking mechanism. The interface state determines whether the link is clear and thus deciding whether to modify the VRRP priority to implement the switch of master and backup equipment. When the uplink interface is down, for example, the VRRP priority of the master equipment will be lowered to the specified priority level. At the same time, the VRRP priority still can be switched according to the route detection in Tracking mechanism even if the interface and link of the device have no change, but a loss of one key route.

Sometimes there are upward or downward link failures, but the interface state of the device does not change. For this, the IP Track technology is introduced to perfect the function of VRRP link detection. This technology can track the state of a specified IP address, including but not limited to a particular interface or the state of routing. When a break of the interface or an unreachable route occurs, the IP Track will notice the VRRP to automatically change the priority of the master and backup line card.

In addition, when the upward or downward link is a multi-link, the AC equipment uses the VRRP and OSPF linkage mechanism. When the link that is being used breaks, the OSPF will reselect a route according to COST value of the link, so as to change the direction of the data traffic, and without the switch of master and backup AC. For more details, please refer to the *VRRP&OSPF Linkage Mechanism White Paper*.

In actual usage scenarios, frequent switch can lead to fluctuations in network, so the detection of Master up time and state is introduced in the Tracking mechanism. For example, after one equipment becomes master one, this equipment raises its priority by the VRRP Master state detection in the Tracking mechanism. After a while, the equipment can raise its priority by the Master-up-time in the Tracking mechanism, which reduces the network fluctuation once a failure occurs and switches the state.

Figure 3-1 Monitoring the uplink and downlink of L3



3.2 Master/Backup Switch and Synchronization

The master and backup line card of an AC can use the out-of-band data to transfer the VRRP heartbeat data and the configuration information synchronization, separating the heartbeat data from the business data. There are two advantages. First of all, business data transmission can be quicker and safer; second, the independent transmission of heartbeat data can ensure timely and effective AC master/backup switch, avoiding frequent switch caused by heartbeat data loss, or even the failure of the whole equipment.

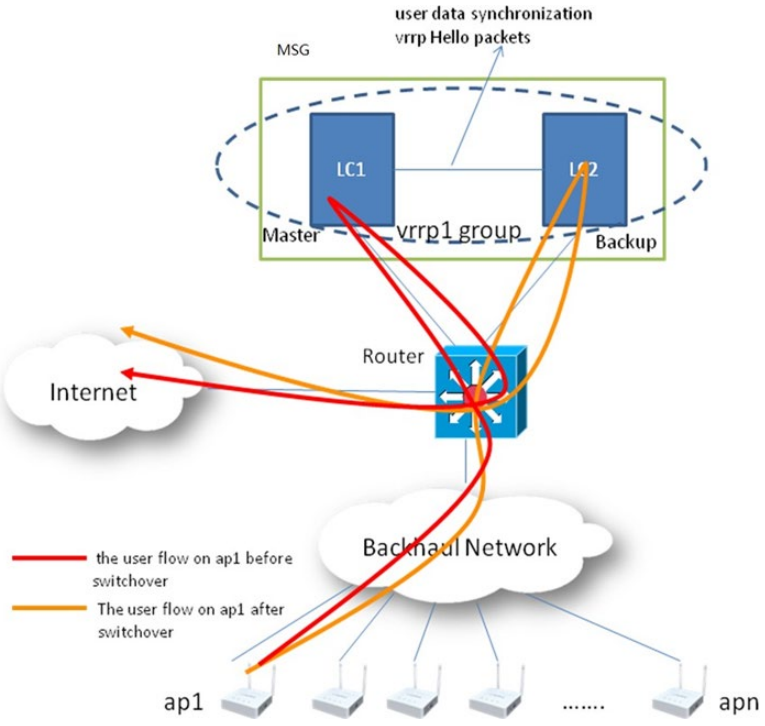
When the master AC equipment fails, and master/backup AC line cards switch, the OSPF will be triggered. It automatically updates the routing information of the corresponding interface and ensures the normal communication between the AC and other routers. For example, when AC's status changes from Master to Backup, AC immediately updates the Metric value of the adjacent OSPF interface to 65535 (MAX Metric) through OSPF protocol, publishes in the territory, and changes the OSPF COST of the adjacent link, so that the data flow will be smoothly switched to the new Master AC. For more details, please refer to the *VRRP&OSPF linkage mechanism White Paper*.

Chapter 4 Networking Mode

This is a logical group based VRRP protocol which supports a number of different network modes according to the division of logical groups.

4.1 1+1 Master/Backup

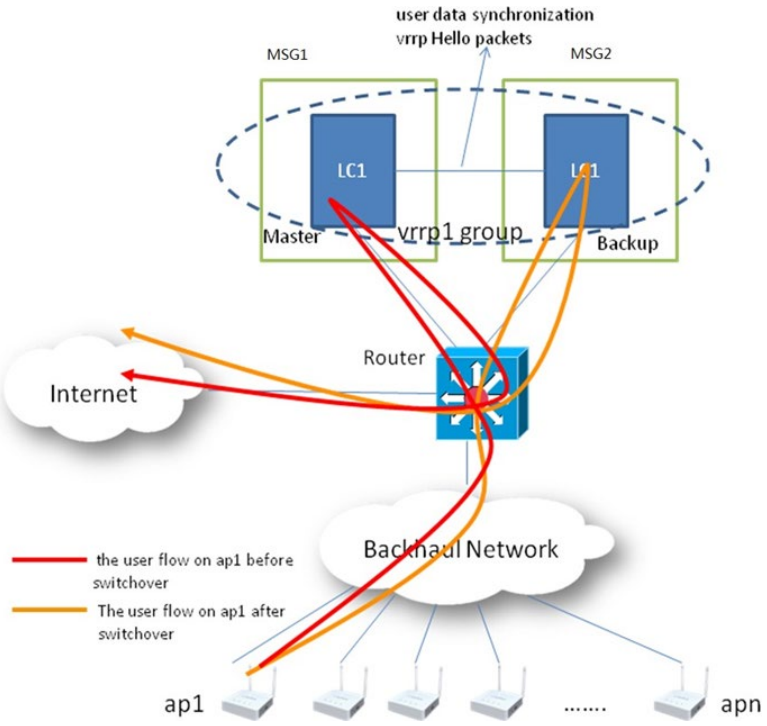
If one line card is specified as Master and another as backup, and these two line cards are in the same VRRP logical group, and then this network mode is 1+1 master/backup network mode. When an AC is in 1+1 master/backup network mode, the line card in Master state will be responsible for business processing and forwarding, and the backup line card is idle.



When a failure occurs in the Master line card or abnormal business link is detected through Track mechanism, the line card in the Master state will revise its VRRP priority, trigger a Master card OSPF module and modify the corresponding cost value to 65535; the line card in the Backup state switches to the master state when perceives the VRRP priority change, and triggers the OSPF module to modify the cost value of the

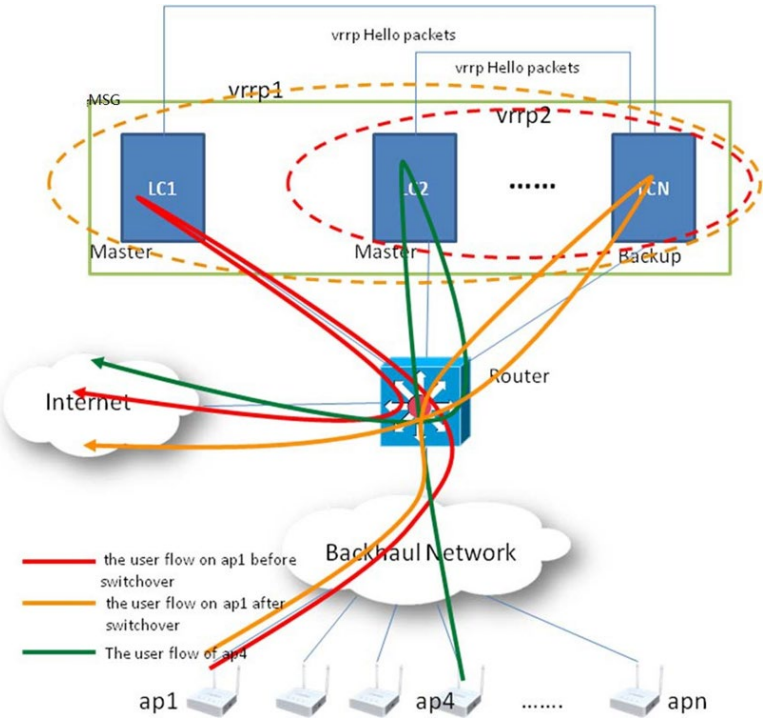
corresponding link, and broadcasts to the OSPF domain. Router receives new Router information and recalculates to get the latest route, switching the user's business flow from LC1 to LC2. Because before the fault occurs, the backup and synchronization of user data have been completed between the master and backup without affection to the users during the switch.

The same group master/backup line cards can be in one MSG or in different MSGs. Its master/backup user business flow switching process is as the same above.



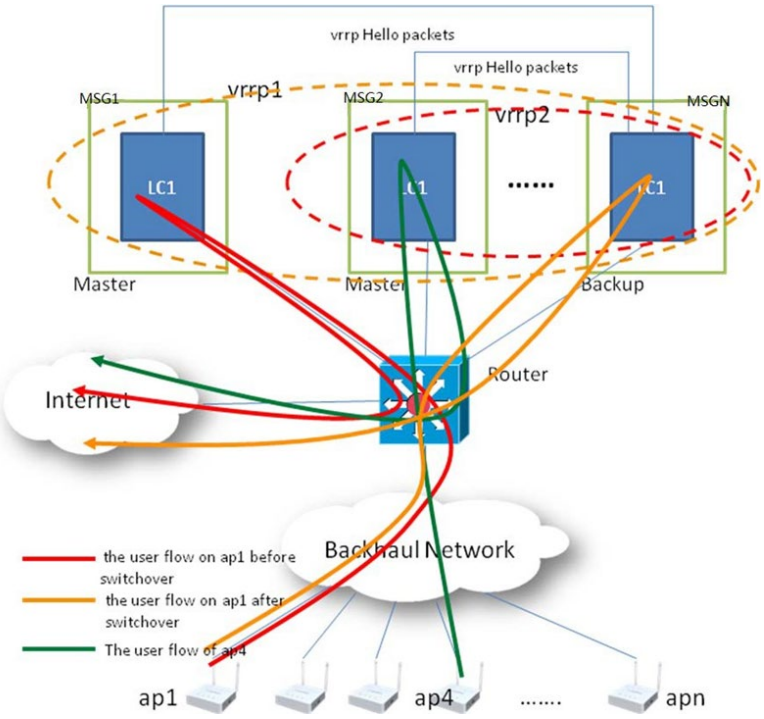
4.2 N+1 Master/Backup

N+1 master/backup mode is an expansion of the 1+1. As shown in the following figure, the specified line card 1 is the Master card, the line card L is Backup. Put the line 1 and line card L in one VRRP logical group1; the rest can be done in the same manner. The specified line card N is the Master card, the line card L is Backup, and put the line card N and line card L in one VRRP logical group N. Business flow will be forwarded from the master card 1 to the line card N, while the backup line card L is in the idle state.



If one Master line card among No.1 to No.N fails, or an abnormal user link is detected through the Track mechanism, the corresponding line card in Master state will modify its level of VRRP, trigger the corresponding OSPF module of the Master card at the same time and change the corresponding link Cost value to 65535. The Backup line card L of the corresponding VRRP virtual group is aware of the master priority change, the line card switches to Master state, triggers the OSPF module to update the corresponding route state, and broadcasts to OSPF domain. The Router in OSPF domain receives new routing information, and recalculates the routing, so as to realize the switch of the user's business flow. Since all the VRRP virtual groups share the same Backup physical line card, after the original Master fault recovery or business link back to normal, the original Master card will be switched back. So the original Master needs to be configured to preemptive mode. In the N+1 master/backup mode, all the VRRP virtual groups use the same Backup physical line card, and there is limited memory and performance; users are unable to perform the data Backup and synchronization. So business will be interrupted during the switch.

The same group master/backup line cards can be in one MSG or in different MSGs. Its master/backup user business flow switching process is as the same above.


vrrp Hello packets
vrrp Hello packets
MSG1
vrrp1
MSG2
vrrp2
MSGN
LC1
LC1
.....
LC1
Master
Master
Backup
Router
Internet
Backhaul Network
the user flow on ap1 before switchover
the user flow on ap1 after switchover
The user flow of ap4
ap1
ap4
.....
apn

Chapter 5 Conclusion

The advantages that the AC series multiple service gateway use VRRP technology are as follows:

- High reliability of redundancy

  If any AC equipment fails or any being used link breaks, the network will not be interrupted, which meets the requirements of the operators.
- Safe information synchronization

  Use out-of-band synchronization heartbeat data to ensure a timely and effective master/backup switch.
- Simplified network management

  The VRRP protocol redundancy protection reduces the complexity of network management and improves the network performance greatly without changing the current network structure, modifying the dynamic routing protocol, or routing discovery protocols, such as configuration information
- Low cost of the network

  Only the master equipment periodically sends VRRP packets.

Document History

The following table describes the update history for this documentation.

Change	Description	Date
Initial release	Initial release of this document.	April, 11, 2016

A Acronyms and Abbreviations

Acronyms and Abbreviations	Full Name
AC	Access Controller
AP	Access Point
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
IETF	Internet Engineering Task Force
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
VRID	Virtual Router ID
VRRP	Virtual Router Redundancy Protocol