Contents

1 Configuring VRRP

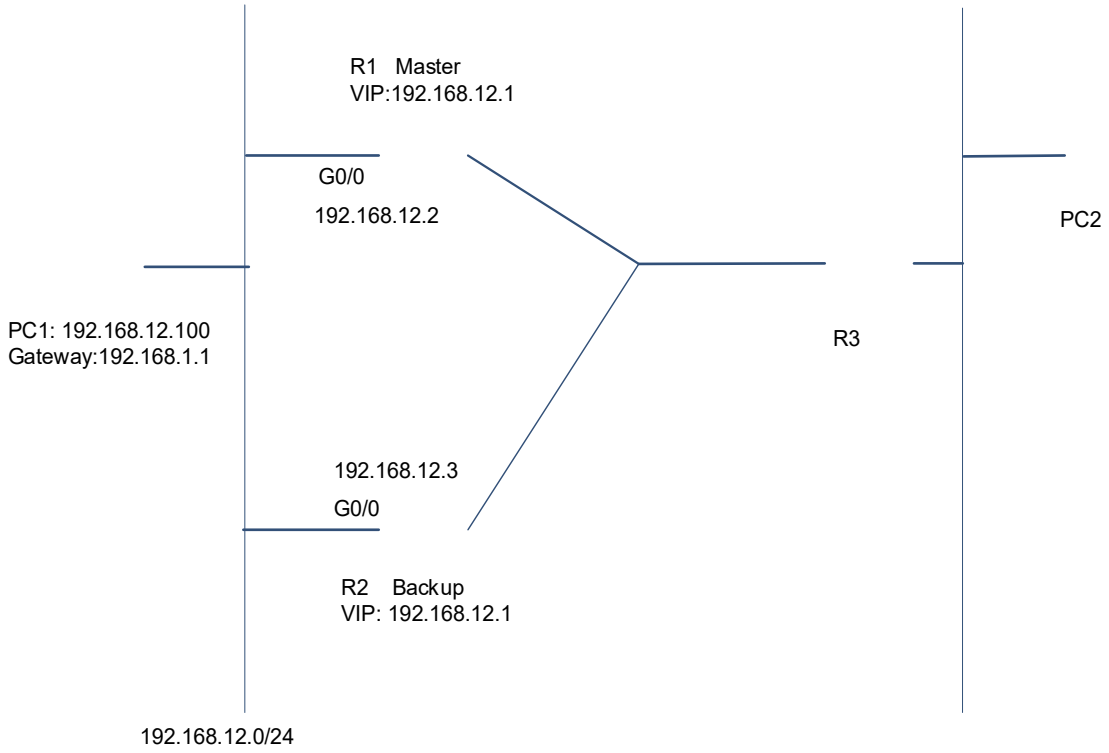
1.1 Introduction

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant routing protocol. When a device used for routing and forwarding on a local area network (LAN) fails, VRRP enables another device to automatically take over services and data of the device, which helps achieve hot backup and fault tolerance of IP routing. In addition, VRRP ensures communication continuity and reliability for the hosts on the LAN. VRRP is applicable to LAN scenarios which require redundant backup of routing egresses.

1.1.1 Basic Concepts

As shown in Figure 1-1, router 1 and router 2 form a VRRP backup group, and the gateway IP address configured for PC 1 is the virtual IP address of the VRRP backup group.

Figure 1-1 **Diagram of Configuring VRRP**



1. VRRP Router

A VRRP router refers to a router running VRRP. It is composed of one or more virtual routers.

2. Virtual Router

A virtual router, also called a VRRP backup group, is usually regarded as the default gateway of hosts on a shared LAN. A VRRP backup group contains a virtual router identifier (VRID) and a set of virtual IP addresses.

3. Master Router

In a VRRP backup group, only the master router responds to Address Resolution Protocol (ARP) requests and forwards IP packets. If a device is the IP address owner, it becomes the master router.

4. Backup Router

In a VRRP backup group, a backup router only monitors the state of the master router but does not respond to ARP requests or forward IP packets. When the master router fails, the backup router takes the chance to become the master router via election.

5. VRID

A virtual router identifier (VRID) is the unique identifier of a virtual router and distinguishes different VRRP back groups. Only a group of routers with the same VRID can form a VRRP backup group.

6. Priority

A VRRP backup group determines the position of each router in the virtual router based on its priority. The configurable priority range is from 1 to 254, and the priority of the VRRP router with the virtual router IP address must be 255. When the priority is 0, the current master node no longer joins the VRRP backup group, and the backup router is triggered to become the master node rapidly without waiting for the current master node to time out.

7. Virtual IP Address

A virtual IP address is the IP address of a virtual router. A virtual router can be configured with one or multiple virtual IP addresses.

8. Virtual MAC Address

A virtual MAC address of VRRP complies with the Request for Comments (RFC) protocol standard. The virtual MAC address of an IPv4 VRRP backup group is "00-00-5E-00-01-{VRID}" (the virtual MAC address of an IPv6 VRRP backup group is “00-00-5E-00-02-{VRID}”), with the first five bytes fixed and the last byte of a VRRP backup group ID. A VRRP backup group responds to an ARP request by using its virtual MAC address instead of the real MAC address of an interface.

9. IP Address Owner

If the virtual IPv4/IPv6 address of a VRRP backup group is consistent with the IPv4/IPv6 address of the Ethernet port on which the VRRP backup group is configured, that is, the VRRP backup group has the real IP address of the Ethernet port, the VRRP backup group is collectively called an IP address owner. In such a case, the priority of the VRRP backup group is 255. If the Ethernet port is available, the VRRP backup group enters the master state automatically. The IP address owner receives and processes the packets whose destination IP address is the IP address of the virtual router.

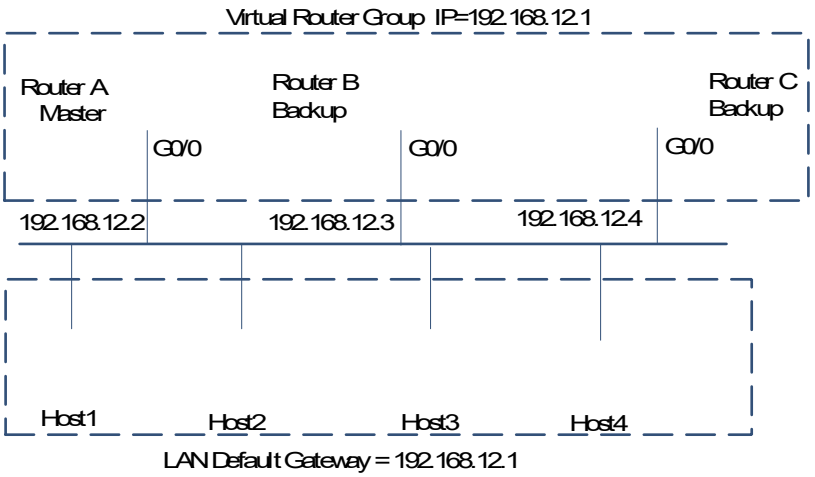
10. Preemption Mode

If a VRRP backup group runs in preemption mode, a backup router with a higher priority replaces the master router with a lower priority to become the master router of the VRRP backup group. If the VRRP backup group runs in the non-preemption mode, as long as the master router runs properly, the backup router does not become the master router even if it is configured with a higher priority later. In some cases, even if the non-preemption mode is configured, a router that is just started in a VRRP backup group will preempt the position of the VRRP master router. The reason is that, when a device is started or the port just becomes active, the VRRP backup group on the port fails to receive the VRRP packet sent by the master device of the same backup group in time. In this case, the above problem can be avoided by delaying the start of the VRRP backup group.

1.1.2 VRRP Application

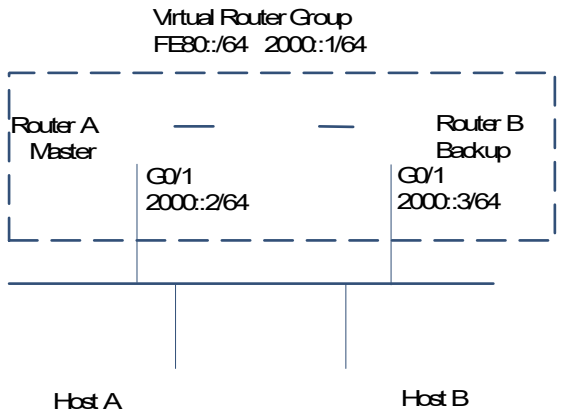
1. Master/Backup Redundancy

Figure 1-1 **IPv4-based VRRP Master/Backup Redundancy**



As shown in Figure 1-1, routers A, B, and C are all connected to the LAN through Ethernet ports, and VRRP is configured on the Ethernet ports connected to the LAN. The routers are in the same VRRP backup group, and the virtual IP address of the VRRP backup group is 192.168.12.1. Router A is elected as the master router of the VRRP backup group, and routers B and C are used as backup routers. Hosts 1, 2 and 3 use the IP address of the virtual router 192.168.12.1 as the gateway address. Packets from a host on the LAN to other networks are forwarded by the master router (router A). If router A fails, a master router is reelected between router B and router C to forward packets, to achieve simple routing redundancy.

Figure 1-2 **IPv6-based VRRP Master/Backup Redundancy**

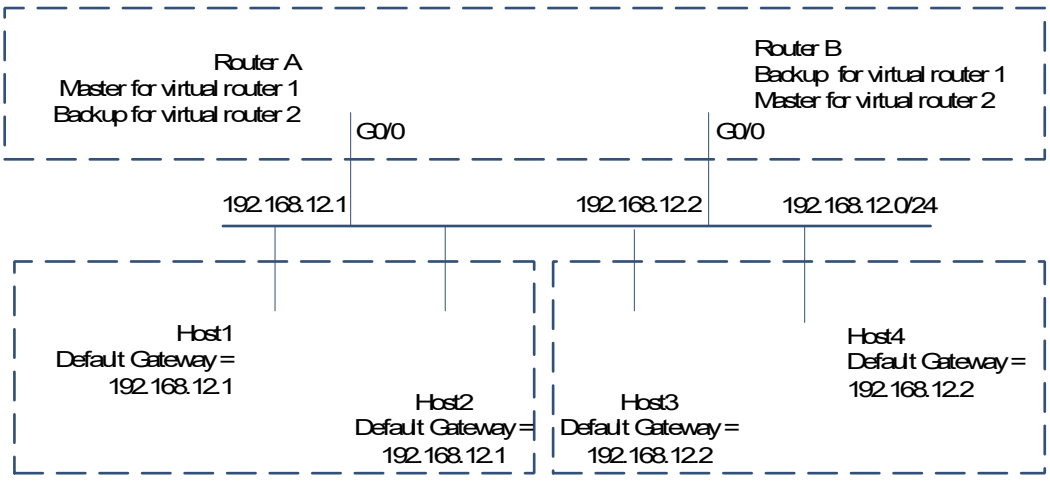


As shown in Figure 1-2, both routers A and B are connected to the LAN through Ethernet ports, and IPv6 VRRP is configured on the Ethernet ports connected to the LAN. The routers are in the same IPv6 VRRP backup group, and the virtual IPv6 addresses of the IPv6 VRRP backup group are FE80::1/64 and 2000::1/64. Router A is elected as the master router of VRRP, and router B functions as a backup router. The hosts on the LAN take the IPv6 link local address FE80::1/64 of the virtual router as the gateway address. Packets from the hosts on the LAN to other networks are forwarded by the master router. If router A fails, router B forwards packets on behalf of router A, achieving simple routing redundancy.

- Before implementation: If the uplink or downlink port of router A fails, the data flow is interrupted, that is, a single point of failure occurs.
- After implementation: If router A fails, VRRP implements switching within seconds to ensure that services are not interrupted. This effectively avoids the problem of network interruption after a single link fails. In addition, you do not need to modify the configuration such as the dynamic routing protocol and routing discovery protocol. You do not need to modify the default gateway configuration for the host node of local link.

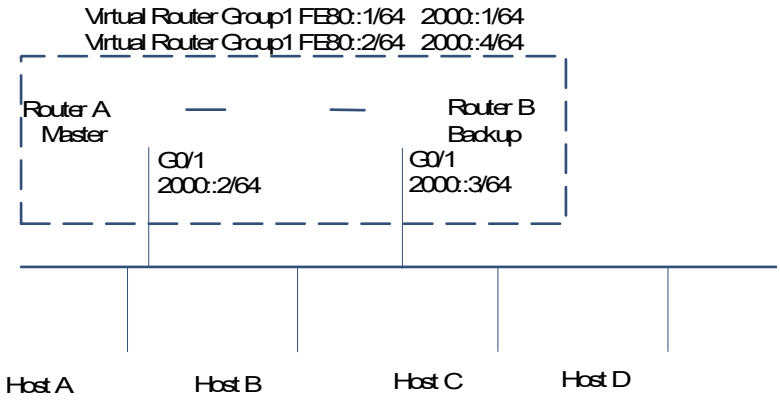
2. Load Balancing

Figure 1-1 **IPv4-based VRRP Load Balancing**



As shown in Figure 1-1, two virtual routers are configured. For virtual router 1, router A uses the IP address 192.168.12.1 of the Ethernet port GigabitEthernet 0/0 as the IP address of the virtual router, so router A becomes the master router and router B becomes the backup router. For virtual router 2, router B takes the IP address 192.168.12.2 of Ethernet port GigabitEthernet 0/0 as the IP address of the virtual router, so router B becomes the master router and router A becomes the backup router. In the LAN, hosts 1 and 2 take the IP address 192.168.12.1 of virtual router 1 as the default gateway address, while hosts 3 and 4 take the IP address 192.168.12.2 of virtual router 2 as the default gateway address. In this application of VRRP, routing redundancy is achieved between routers A and B, and the LAN traffic is shared between them to achieve load balancing.

Figure 1-2 **IPv6-based VRRP Load Balancing**



As shown in Figure 1-2, two virtual routers are configured. For virtual router 1, router A uses the IP address fe80::1/64 of the Ethernet port GigabitEthernet 0/1 as the IP address of the virtual router, so router A becomes the master router and router B becomes the backup router. For virtual router 2, router B takes the IP address fe80::2/64 of Ethernet port GigabitEthernet 0/1 as the IP address of the virtual router, so router B becomes the master router and router A becomes the backup router. On the LAN, hosts A and B use the IP address FE80::1 of virtual router 1 as the default gateway address (manually configured static IPv6 gateway), and hosts C and D use the IP address FE80::2 of virtual router 2 as the default gateway address (manually static configured IPv6 gateway). In this way, routing redundancy is achieved between routers A and B, and the LAN traffic is shared between them to achieve load balancing.

The devices involved are L3 devices or routers. L2 devices are not applicable.

- Before implementation: All traffic goes through the master router, causing a certain burden to the master router. Before the master router fails, the backup router has been always idle, leading to a resource waste.
- After implementation: Each device is not a single master router or backup router, but acts as different roles in different groups. Therefore, the connected devices can be assigned to different groups and forward traffic to different gateways to achieve traffic load balancing. Moreover, no device is kept idle all the time, and resources are fully utilized.

1.1.3 Packet Structure

VRRP has two versions available: VRRPv2 and VRRPv3. VRRPv2 is only applicable to IPv4 networks, and VRRPv3 is applicable to both IPv4 and IPv6 networks. A VRRP packet is used to send the priority and state of the master device to all backup devices in the same backup group in multicast mode (with the destination

address 224.0.0.18). The packet is encapsulated in an IP packet. The source address is the primary IP address (not the virtual IP address) of the packet sending port, the time to live (TTL) is 255, and the protocol ID is 112. Figure 1-1 and Figure 1-2 show the structures of VRRPv2 and VRRPv3 packets respectively.

Figure 1-1 **Structure of VRRPv2 Packets**

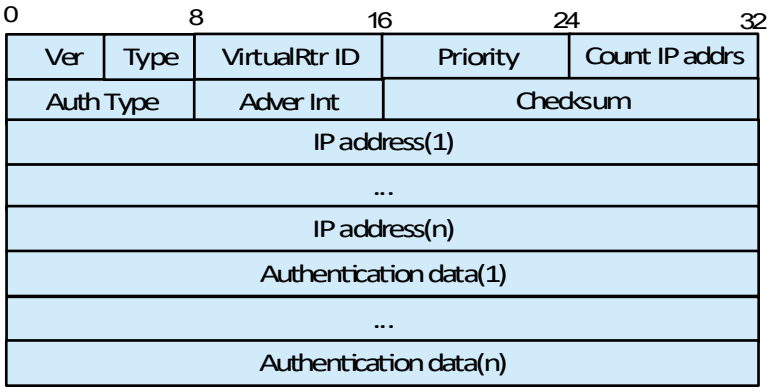


Figure 1-2 **Structure of VRRPv3 Packets**

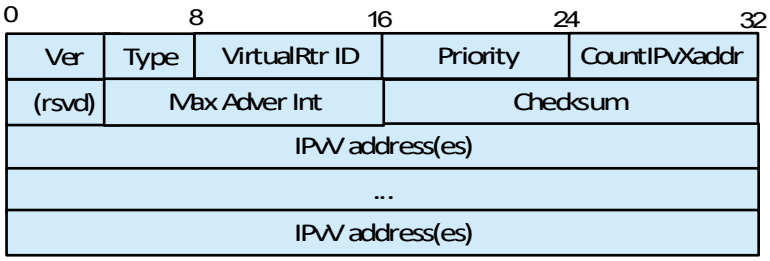


Table 1-1 Fields of VRRP Packets and Description

Packet Field	Description	
	VRRPv2	**VRRPv3**
Ver	Protocol version number. The value is 2.	Protocol version number. The value is 3.
Type	VRRP packet type. The value is 1, indicating that only the advertisement packets of VRRP are supported.	VRRP packet type. The value is 1, indicating that only the advertisement packets of VRRP are supported.
Virtual Rtr ID (VRID)	Virtual router ID (also the backup group ID). The value range is from 1 to 255.	Virtual router ID (also the backup group ID). The value range is from 1 to 255.

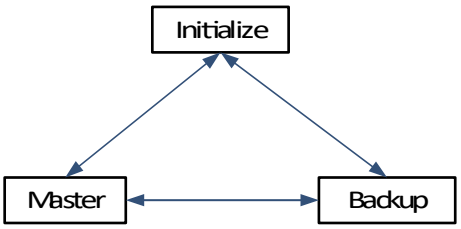
Packet Field	Description	
	VRRPv2	**VRRPv3**
Priority	Priority of the router in the backup group. The value range is from 0 to 255, and the default value is **100**. A larger value indicates a higher priority. When the priority is 0, the current master node no longer joins the VRRP backup group and the backup router is triggered to become the master node, instead of waiting for the current master node to time out. The priority 255 is reserved for the IP address owner, and the configurable range is from 1 to 254 for other routers.	Priority of the router in the backup group. The value range is from 0 to 255, and the default value is **100**. A larger value indicates a higher priority. When the priority is 0, the current master node no longer joins the VRRP backup group and the backup router is triggered to become the master node, instead of waiting for the current master node to time out. The priority 255 is reserved for the IP address owner, and the configurable range is from 1 to 254 for other routers.
Count IP Addrs/Count IPvX Addr	Number of virtual IPv4 addresses in the backup group.	Number of virtual IPv4 or virtual IPv6 addresses in the backup group.
Auth Type	Authentication type. Three authentication types are defined: ● **0**: Indicates no authentication. ● **1**: Indicates simple password (plaintext) authentication. ● **2**: Indicates MD5 authentication.	-
Advertise Interval	Interval of sending advertisement packets, in seconds. The default value is **1** second.	Interval of sending advertisement packets, in centiseconds. The default value is **100** centiseconds, namely, **1** second.
Checksum	16-bit checksum, used to check data corruption in the VRRP packet.	16-bit checksum, used to check data corruption in the VRRP packet.
IP Address/IPvX Address(es)	Virtual IPv4 addresses in the backup group. The number of addresses contained is defined in the **Count IP Addrs** field.	Virtual IPv4 addresses or virtual IPv6 addresses in the VRRP backup group. The number of addresses contained is defined in the **Count IPvX Addrs** field.
Authentication Data	Authentication key of the VRRP packet. At present, the authentication key is only used for simple password authentication. For the other authentication methods, **0** is filled in this field.	-

Packet Field	Description	
	VRRPv2	VRRPv3
rsvd	-	Reserved field for the VRRP packet. The field must be set to **0**.

1.1.4 VRRP State

There are three VRRP states: initialize, backup, and master. Figure 1-1 shows the state transition process.

Figure 1-1 **VRRP State Transition Diagram**



1. Initialize

Initialize is the initial state of VRRP. The system enters this state after startup. It only responds to startup, that is, it does not process VRRP packets.

- When the system is started, if the priority of the local VRRP backup group is 255 (namely, the IP address owner), then:
  - VRRP packets are sent immediately.
  - If the local VRRP backup group is an IPv4 virtual router, gratuitous ARP packets are sent to all the IPv4 addresses of the virtual router. If the local VRRP backup group is an IPv6 virtual router, gratuitous NA packets are sent to all the IPv6 addresses of the virtual router, the routing flag bit is 1, the request flag bit is 0, the coverage flag bit is 1, the target address is the IPv6 address of the virtual router (not destination address), and the link layer address in the target link layer option is the MAC address of the virtual router.
  - The advertisement information timer is configured to send VRRP advertisements regularly, that is, **Adver_Timer** is set to **Advertisement_Interval**.
  - The local VRRP backup group switches to the master state.
- When the system is started, if the priority of the local VRRP backup group is not 255, then:
  - **Master_Adver_Interval** is set to **Advertisement_Interval**.
  - **Master_Down_Timer** is set to **Master_Down_Interval**.
  - The local VRRP backup group switches to the backup state.

2. Backup

A backup virtual router is used to monitor the validity and state of the master virtual router.

- An IPv4 backup virtual router does not respond to the ARP request for the IP address of the virtual router, and an IPv6 backup virtual router does not respond to the neighbor solicitation (NS) packet for the IPv6 address of the virtual router.
- The backup virtual router discards packets whose destination MAC addresses are the MAC address of the VRRP backup group and packets whose destination IP addresses are the IP address of the VRRP backup group.
- The backup virtual router does not send protocol packets. It must receive the VRRP multicast packets sent by the master router to know the state of the master router.
- When a shutdown event is received, the backup virtual router deletes the host timeout timer and switches to the initialize state.
- If a timeout event of the host timeout timer is received, the backup virtual router sends VRRP advertisement information immediately. If the backup virtual router is an IPv4 virtual router, it broadcasts ARP packets to all the IPv4 addresses of the virtual router. If the backup virtual router is an IPv6 virtual router, it computes and joins the solicited-node multicast address for the IPv6 address associated with the virtual router, and sends non-request (gratuitous) NA packets to all the IPv6 addresses of the virtual router. The routing flag bit is 1, the request flag bit is 0, the coverage flag bit is 1, the target address is the IPv6 address of the virtual router (not destination address), and the link layer address in the target link layer option is the MAC address of the virtual router. **Adver_Timer** is set to **Advertisement_Interval**, and the virtual router switches to the master state.
- If a VRRP packet is received and the priority is 0, the host timeout timer **Master_Down_Timer** is reset to **Skew_Time**; if the priority of the received VRRP packet is greater than 0, and preemption is not allowed or the priority of the packet is greater than or equal to the priority of the local virtual router, **Adver Interval** is set to the **Master_Adver_Interval** field value in the packet and **Master_Down_Interval** is set to **Master_Down_Timer**, otherwise the packet is discarded.

3. Master

As the forwarding role in a VRRP backup group, the virtual router in the master state forwards virtual gateway packets.

- It sends VRRP multicast packets regularly, and forwards relevant packets passing through the virtual IP address and packets whose destination MAC address is the VRRP virtual MAC address.
- If the virtual router is an IPv4 virtual router, the VRRP virtual MAC address must be used to respond to the ARP requests whose destination IP addresses are the virtual IP address of the virtual router. If the virtual router is an IPv6 virtual router, it must respond to the NS packets whose destination IP addresses are the virtual IPv6 address of the virtual router and must be a member of the solicited-node multicast address for the IPv6 address associated with the virtual router.
- If **Accept_Mode** or **IPvX Owner** is configured, that is, the virtual router is the IPv4/IPv6 address owner, the packets whose destination IP addresses are the virtual IP address of the virtual router must be received, otherwise the packets are discarded.
- When the network port where the VRRP virtual router is located receives a shutdown event, the virtual router deletes the regular advertisement timer, removes the value of **Adver_Timer**, immediately sends a VRRP advertisement packet with priority 0, and switches to the initialize state.
- If the timer for sending VRRP packets times out or a VRRP packet with priority 0 is received, the VRRP advertisement message is sent immediately, the timer for sending VRRP packets is reset, and **Adver_Timer**

is assigned to **Advertisement_Interval**.

- If the priority of the received VRRP packet is greater than or equal to that of the corresponding VRRP virtual router at the local end and the source IP address of the received packet is greater than the primary IP address at the local end, the host timeout timer is reset, the regular advertisement timer is configured, and the virtual router switches to the backup state.
- If none of the above requirements is met, the packets are discarded.

1.1.5 VRRP Election

VRRP provides a simple mechanism for electing the master router, which provides the actual routing and forwarding service. The master router is elected in the following order:

(1) VRRP judges whether the VRRP device is an IP address owner. If so, VRRP switches to the master state.

(2) VRRP judges the VRRP priority in the same VRRP backup group. The device with a larger priority is in the master state.

(3) VRRP judges the primary IP address of the network port. The device with a larger primary IP address changes to the master state.

(4) The backup device determines whether to switch the state by monitoring the VRRP packet regularly sent by the master device. It switches the state in the following two cases:

- If the received advertisement state of the master device is normal, the priority of the master device's advertisement is lower than that of the backup device, and the preemption mode has been configured, the backup device switches to the master state.
- If no state advertisement is received from the master device within the timeout period and the preemption mode is configured, the backup device switches to the master state.

1.1.6 VRRP Timer

The main VRRP timers include the VRRP advertisement sending interval timer and the VRRP preemption delay timer.

- VRRP advertisement sending interval timer

You can adjust the time interval for the master router to send VRRP advertisement packets by configuring the VRRP advertisement sending interval timer. If the backup router still fails to receive a VRRP advertisement packet after waiting for at least three intervals, it regards itself as the master router, and sends a VRRP advertisement packet to reelect the master router.

- VRRP preemption delay timer

To avoid frequent master/backup switching between the members of the backup group and allow the backup router to have enough time to collect necessary information (such as the routing information), the backup router does not immediately preempt the position of the master router after receiving the advertisement packet with a priority lower than the local priority, but waits for a period of time (preemption delay) before sending a VRRP advertisement packet to take the place of the original master router.

1.1.7 VRRP Tracking

By correlating with the tracking function, VRRP monitors port state changes and the IP host accessibility and automatically adjusts the priority of the backup group to trigger role competition in the backup group, which

causes state switching in the backup group and achieves fault monitoring and automatic switching. In this way, the network traffic is not interrupted. Two detection methods are available:

- Port state: VRRP detects the port state by receiving port state change messages. When a port is no longer in the up state, the priority of the current master router is automatically reduced to enable other backup routers to have the opportunity to become the master router. This avoids the failure of the entire virtual router due to the disconnection of a certain line.
- Host accessibility: Internet Control Message Protocol (ICMP) detection packets are sent regularly, and the time interval for sending detection packets, timeout time for waiting for responses, and continuous timeout count are configured to judge accessibility of the destination addresses.

Caution

- A monitored port must be a routable L3 logical port (for example, a routed port, an SVI, a loopback port, or a tunnel port). If a VRRP backup group is an IPv6 group, the IPv6 function needs to be enabled on the port first.
- The decrease in the priority value must be greater than the priority difference between the master and backup devices; otherwise the priority of the master device may be the same as that of the backup device after priority adjustment, and the master/backup state cannot be switched.

1.1.8 Protocols and Standards

- RFC2338: Virtual Router Redundancy Protocol
- RFC3768: Virtual Router Redundancy Protocol (VRRP)
- RFC5798: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

1.2 Restrictions and Guidelines

- The IPv6 VRRP and IPv4 VRRP backup groups share the VRRP backup group ID. One VRRP backup group ID is applicable to an IPv4 VRRP backup group and an IPv6 VRRP backup group configured on the same port.
- When the IPv4 VRRP and IPv6 VRRP backup groups of the same port use the same VRRP backup group ID, two VRRP backup group IDs are used.

1.3 Configuration Task Summary

VRRP configuration includes the following tasks:

(1) Configuring IPv4 VRRP

(2) Configuring IPv6 VRRP

(3) Configuring IPv4 VRRP Tracking

(4) Configuring IPv6 VRRP Tracking

(5) (Optional) Configuring VRRP Attributes

All the following configuration tasks are optional and may be selected as needed.

- Configuring VRRP Basic Attributes
- Configuring a Method of Sending IPv4 VRRP Packets on a Super VLAN Port

- Configuring the Dual-Active Mode for an IPV4 VRRP Group
- Configuring the IPv4 VRRP Packet Version

1.4 Configuring IPv4 VRRP

1.4.1 Overview

IPv4 VRRP creates a backup group on a specified LAN segment after the backup group ID and virtual IPv4 address are configured, and then the VRRP single backup function is enabled on the corresponding port. You can configure multiple VRRP backup groups on the same Ethernet port to achieve load balancing and offer more stable and reliable network services through mutual backup.

1.4.2 Restrictions and Guidelines

- To achieve VRRP, the routers in a VRRP backup group must be configured with the same virtual IPv4 address.
- To achieve mutual backup between multiple IPv4 VRRP backup groups, configure multiple same IPv4 VRRP backup groups with different priorities on ports so that they act as the master and backup groups mutually.
- Enable VRRP on L3 ports.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L3 interface configuration mode.

interface *interface-type interface-number*

(4) Enable IPv4 VRRP.

vrrp *group-id* **ip** *ipv4-address* [**secondary**]

IPv4 VRRP is disabled on a port by default.

(5) Configure a priority for the IPv4 VRRP backup group.

vrrp *group-id* **priority** *priority*

The default priority of an IPv4 VRRP backup group is **100**.

(6) (Optional) Configure a VRRP packet standard for the IPv4 VRRP backup group.

vrrp *group-id* **version** { **2** | **3** }

IPv4 VRRP adopts the VRRPv2 standard by default.

(7) (Optional) Configure an authentication string for the IPv4 VRRP backup group.

vrrp *group-id* **authentication** *authentication-string*

No authentication string of IPv4 VRRP is configured by default.

(8) (Optional) Configure a name for the IPv4 VRRP backup group.

vrrp *group-id* **description** *group-name*

No VRRP group name is configured by default.

(9) (Optional) Configure a VRRP advertisement interval for the IPv4 VRRP master router.

vrrp *group-id* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

The default VRRP advertisement interval of the VRRP master router is **1** second.

(10) (Optional) Enable the IPv4 VRRP timer learning function.

vrrp *group-id* **timers learn**

The advertisement interval timer learning function is disabled for an IPv4 VRRP backup group by default.

(11) (Optional) Configure the preemption mode for the IPv4 VRRP backup group.

vrrp *group-id* **preempt** [**delay** *delay-seconds*]

IPv4 VRRP runs in the preemption mode without preemption delay by default.

(12) (Optional) Configure a startup delay for the VRRP backup group on the port.

vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }

No VRRP group startup delay is configured by default.

1.5 Configuring IPv6 VRRP

1.5.1 Overview

IPv6 VRRP creates a backup group on a specified LAN segment after the backup group ID and virtual IPv6 address are configured, and then the VRRP single backup function is enabled on the corresponding port. You can configure multiple VRRP backup groups on the same Ethernet port to achieve load balancing and offer more stable and reliable network services through mutual backup.

1.5.2 Restrictions and Guidelines

- The first configured virtual address for IPv6 VRRP must be a link-local address, which can be deleted only after other virtual addresses are deleted.
- The IPv6 function must be enabled on a port before IPv6 VRRP is configured.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the L3 interface configuration mode.

interface *interface-type interface-number*

(4) Enable the IPv6 function on the port.

ipv6 enable

(5) Enable IPv6 VRRP.

vrrp *group-id* **ipv6** *ipv6-address*

IPv6 VRRP is disabled on a port by default.

(6) Enable the function of receiving packets whose destination addresses are the IPv6 address of the virtual router.

vrrp ipv6 accept_mode

By default, an IPv6 VRRP group in the master state is not permitted to receive packets whose destination addresses are the IPv6 address of a virtual router, except the IPv6 VRRP group in owner state or the received NA/NS packets.

(7) Configure a priority for the IPv6 VRRP backup group.

vrrp ipv6 *group-id* **priority** *priority*

The default priority of an IPv6 VRRP backup group is **100**.

(8) (Optional) Configure a name for the IPv6 VRRP backup group.

vrrp ipv6 *group-id* **description** *group-name*

No VRRP group name is configured by default.

(9) (Optional) Configure a VRRP advertisement interval for the IPv6 VRRP master router.

vrrp ipv6 *group-id* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

The default VRRP advertisement interval of the VRRP master router is **1** second.

(10) (Optional) Enable the IPv6 VRRP timer learning function.

vrrp ipv6 *group-id* **timers learn**

The advertisement interval timer learning function is disabled for an IPv6 VRRP group by default.

(11) (Optional) Configure the preemption mode for the IPv6 VRRP backup group.

vrrp ipv6 *group-id* **preempt** [**delay** *delay-seconds*]

IPv6 VRRP runs in the preemption mode without preemption delay by default.

1.6 Configuring IPv4 VRRP Tracking

1.6.1 Overview

IPv4 VRRP tracking monitors the changes in port state and the IPv4 host accessibility. You can configure the optional packet detection parameter and bidirectional forwarding detection (BFD) correlation. The priority of a backup group can be adjusted dynamically to implement automatic switching and recovery of the backup group in case of a failure monitored.

1.6.2 Restrictions and Guidelines

- A monitored port must be a routable L3 logical port (for example, a routed port, an SVI, a loopback port, or a tunnel port).
- If a VRRP group uses the actual IP address of an Ethernet port (in the owner state), the group priority is 255, and the monitored IP address or port can be configured, but the priority of the VRRP group is not changed.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure a port to be monitored by an IPv4 VRRP backup group.

vrrp *group-id* **track** { *interface-type interface-number* | **bfd** *interface-type interface-number ipv4-address* } [*priority*]

No port to be monitored by an IPv4 VRRP backup group is configured by default. If a port to be monitored by an IPv4 VRRP backup group is configured and the priority parameter is not specified, the priority change value is 10.

(5) Configure an IP address to be monitored by the IPv4 VRRP backup group.

vrrp *group-id* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

No IP address to be monitored by an IPv4 VRRP backup group is configured by default. If an IP address to be monitored by an IPv6 VRRP group is configured, the time interval for sending detection packets is 3 seconds, and the timeout time for waiting for a response to a sent detection packet is 1 second, and the consecutive timeout count for judging that a tracked IP address is unreachable is 3.

(6) Configure BFD correlation with the IPv4 VRRP group.

vrrp *group-id* **bfd** *ip-address*

BFD correlation with an IPv4 VRRP group is not configured on a port by default.

(7) Return to the global configuration mode.

exit

(8) Configure global IPv4 VRRP BFD.

vrrp bfd *interface-type interface-number ip-address*

By default, no global BFD mode is configured for IPv4 VRRP to detect whether the master device is active.

1.7 Configuring IPv6 VRRP Tracking

1.7.1 Overview

IPv6 VRRP tracking monitors the changes in port state and the IPv6 host accessibility. You can configure the optional packet detection parameter to dynamically adjust the priority of a backup group and implement automatic switching and recovery of the backup group in case of a failure monitored.

1.7.2 Restrictions and Guidelines

- A monitored port must be a routable L3 logical port (for example, a routed port, an SVI, a loopback port, or a tunnel port).
- The IPv6 function needs to be first enabled on a port.
- If a tracked host IP address is a link-local address, specify a network port.
- If a VRRP group (in the owner state) uses the actual IP address of an Ethernet port, the group priority is 255, and the monitored IP address or port can be configured, but the priority of the VRRP group is not changed.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the IPv6 function on the port.

ipv6 enable

(5) Configure a port to be monitored by an IPv6 VRRP group.

vrrp ipv6 *group-id* **track** { *interface-type interface-number* | **bfd** *interface-type interface-number peer-ipv6-address* } [*priority*]

No port to be monitored by an IPv6 VRRP group is configured by default. If a port to be monitored by an IPv6 VRRP group is configured and the priority parameter is not specified, the priority change value is 10.

(6) Configure an IPv6 address to be monitored by the IPv6 VRRP backup group.

vrrp ipv6 *group-id* **track** { *ipv6-global-address* | *ipv6-linklocal-address interface-type interface-number* } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

No IP address to be monitored by an IPv6 VRRP group is configured by default. If an IP address to be monitored by an IPv6 VRRP group is configured, the time interval for sending detection packets is 3 seconds, the timeout time for waiting for a response to a sent detection packet is 1 second, and the consecutive timeout count for judging that a tracked IP address is unreachable is 3.

(7) Configure the BFD support for IPv6 VRRP on an Interface.

vrrp ipv6 *group-id* **bfd** *ipv6-address*

By default, the linkage between an IPv6 VRRP and BFD is not configured on an interface. To enable such linkage, please configure this item.

(8) Exit back to the global configuration mode.

exit

(9) Configure the global IPv6 VRRP BFD.

vrrp ipv6 bfd *interface-type interface-number ipv6-address*

By default, global IPv6 VRRP BFD is not used to detect whether a master router is active. To enable this, please configure this item.

1.8 Configuring VRRP Attributes

1.8.1 Overview

If a VRRP backup group has been set up, you can configure enhancement to increase the usability of the VRRP backup group.

1.8.2 Configuration Tasks

The VRRP attribute configuration includes the following tasks:

All the following configuration tasks are optional and may be selected as needed.

- Configuring VRRP Basic Attributes
- Configuring a Method of Sending IPv4 VRRP Packets on a Super VLAN Port
- Configuring the Dual-Active Mode for an IPV4 VRRP Group
- Configuring the IPv4 VRRP Packet Version

1.8.3 Configuring VRRP Basic Attributes

1. Overview

If a VRRP backup group has been set up, you can configure basic attributes according to the actual situation.

2. Prerequisites

A VRRP backup group has been set up.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure VRRP basic attributes according to the actual situation.

- Configure a priority for the IPv4 VRRP backup group.

  vrrp *group-id* **priority** *priority*

  The default priority of an IPv4 VRRP backup group is **100**.

- Configure an authentication string of IPv4 VRRP.

  vrrp *group-id* **authentication** *authentication-string*

  No authentication string of IPv4 VRRP is configured by default.

- Configure a VRRP advertisement interval for the IPv4 VRRP master router.

  vrrp *group-id* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

  The default VRRP advertisement interval of the VRRP master router is **1** second.

- Configure the preemption mode for the IPv4 VRRP backup group.

  vrrp *group-id* **preempt** [**delay** *delay-seconds*]

  IPv4 VRRP runs in the preemption mode without preemption delay by default.

- Enable the IPv4 VRRP timer learning function.

  vrrp *group-id* **timers learn**

  The advertisement interval timer learning function is disabled for an IPv4 VRRP backup group by default.

- Configure a name for the IPv4 VRRP group.

vrrp *group-id* **description** *group-name*

No VRRP group name is configured by default.

- Configure a startup delay for the VRRP backup group on a port.

  vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }

  No VRRP group startup delay is configured by default.

1.8.4 Configuring a Method of Sending IPv4 VRRP Packets on a Super VLAN Port

1. Overview

The IPv4 VRRP protocol packets can be sent by the following three methods in a super VLAN. You can configure the method of sending advertisement packets.

- Sending IPv4 VRRP packets only to the first up sub VLAN in a super VLAN.
- Sending IPv4 VRRP packets to a specified sub VLAN in a super VLAN.
- Sending IPv4 VRRP packets to all the sub VLANs in a super VLAN.

2. Restrictions and Guidelines

- The configuration is effective only on super VLAN ports.
- If VRRP and VRRP plus are both enabled on a super VLAN port, VRRP packets are sent to all the up sub VLAN ports of the super VLAN port.

3. Prerequisites

VRRP has been enabled on a super VLAN port.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VLAN interface mode.

interface vlan *vlan-id*

(4) Configure the super VLAN mode.

supervlan

The super VLAN mode is not configured by default.

(5) Configure a sub VLAN range.

subvlan *vlan-range*

No sub VLAN range is configured by default.

(6) Configure a method of sending IPv4 VRRP packets on a super VLAN port.

vrrp detection-vlan { **first-subvlan** | *subvlan-id* }

The IPv4 VRRP packets on a super VLAN port are sent to the first up sub VLAN only by default.

1.8.5 Configuring the Dual-Active Mode for an IPV4 VRRP Group

1. Overview

A VRRP group works in master/backup mode by default. To set both ends of a VRRP group in the master state and avoid sending keepalive packets, configure the dual-active mode for the VRRP group.

2. Restrictions and Guidelines

- The dual-active mode can be configured only on a VLAN port.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VLAN interface mode.

interface vlan *vlan-id*

(4) Configure a VRRP group to work in dual-active state and configure the VRRP group not to send keepalive packets.

vrrp mode dual-active

A VRRP group works in master/backup mode by default.

1.8.6 Configuring the IPv4 VRRP Packet Version

1. Overview

The devices belonging to the same VRRP group should send packets according to the unified packet protocol: VRRPv2 or VRRPv3. By default, VRRPv2 is used for sending packets. VRRPv3 routers can recognize VRRPv2 packets, but VRRPv2 routers cannot recognize VRRPv3 packets. Configuring this function enables VRRPv3 routers to send VRRPv2 packets so as to communicate with VRRPv2 routers.

2. Restrictions and Guidelines

- The configuration is applicable to IPv4 VRRP only.
- If simple authentication has been configured for a VRRP group and the VRRP group is configured to send VRRPv2 packets, the authentication information is carried. If a VRRP group is configured to send VRRPv3 packets, the authentication information is not carried.
- The configuration only applies to the sending mode of VRRP packets and does not affect the receiving mode. For example, a VRRPv3 router can identify both VRRPv2 and VRRPv3 packets.

3. Prerequisites

IPv4 VRRP has been configured.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the VRRP packet standard for an IPv4 VRRP backup group.

vrrp *group-id* **version** { **2** | **3** }

IPv4 VRRP adopts the VRRPv2 standard by default.

1.9 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

You can run the **debug** command to output debugging information.

Caution

- The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1 VRRP Monitoring

Command	Purpose
show [**ipv6**] **vrrp** [**brief** | *group-id*]	Displays the brief or detailed information of IPv4/IPv6 VRRP.
show [**ipv6**] **vrrp interface** *interface-type interface-number* [**brief**]	Displays the information of an IPv4/IPv6 VRRP group on a specified port.
show vrrp packet statistics [*interface-type interface-number*]	Displays the statistics of VRRP packets.
debug [**ipv6**] **vrrp**	Debugs VRRP errors, events, packets, and state.
debug [**ipv6**] **vrrp errors**	Debugs VRRP errors.
debug [**ipv6**] **vrrp events**	Debugs VRRP events.
debug vrrp packets [**acl** *acl-id* **|** [**icmp** | **protocol**] **interface** *interface-type interface-number* [*group-id*]] **debug ipv6 vrrp packets** [**acl** *acl-name* | [**icmp** | **protocol**] **interface** *interface-type interface-number* [*group-id*]]	Debugs VRRP packets.
debug [**ipv6**] **vrrp state**	Debugs VRRP state.

1.10 Configuration Examples

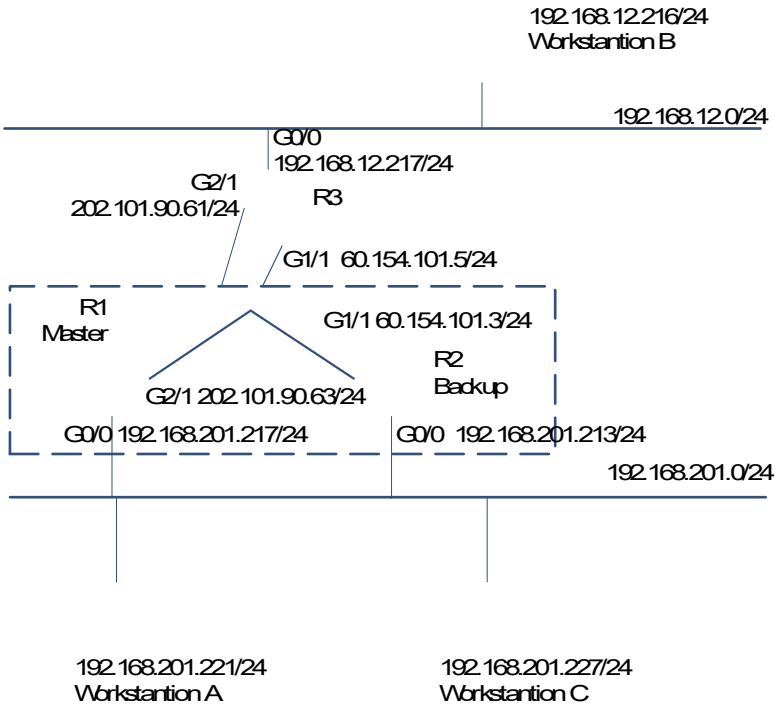
1.10.1 Configuring IPv4 VRRP

1. Requirements

An IPv4 VRRP group and a to-be-monitored port need to be configured.

2. Topology

Figure 1-1 **Topology for Configuring a VRRP Group and a To-Be-Monitored Port**



3. Notes

- Configure the work station cluster (192.168.201.0/24) to use the backup group composed of routers R1 and R2 and set the gateway address to the virtual router IP address configured for the backup group (192.168.201.1) so that the work station cluster accesses the remote work station cluster (192.168.12.0 /24) through the virtual router 192.168.201.1.
- On router R1, configure GigabitEthernet 2/1 as a VRRP monitored port.
- No VRRP but an ordinary routing function is configured on router 3.

4. Procedure

Perform the following configuration on router 3:

```
R3> enable
R3# configure terminal
R3(config)# interface GigabitEthernet 0/0
R3(config-if-GigabitEthernet 0/0)# no switchport
```

```
R3(config-if-GigabitEthernet 0/0)# ip address 192.168.12.217 255.255.255.0
R3(config-if-GigabitEthernet 0/0)# exit
R3(config)# interface GigabitEthernet 1/1
R3(config-if-GigabitEthernet 1/1)# no switchport
R3(config-if-GigabitEthernet 1/1)# ip address 60.154.101.5 255.255.255.0
R3(config-if-GigabitEthernet 1/1)# exit
R3(config)# interface GigabitEthernet 2/1
R3(config-if-GigabitEthernet 2/1)# no switchport
R3(config-if-GigabitEthernet 2/1)# ip address 202.101.90.61 255.255.255.0
R3(config-if-GigabitEthernet 2/1)# exit
R3(config)# router ospf
R3(config-router)# network 202.101.90.0 0.0.0.255 area 10
R3(config-router)# network 192.168.12.0 0.0.0.255 area 10
R3(config-router)# network 60.154.101.0 0.0.0.255 area 10
```

Perform the following configuration on router 1:

```
R1> enable
R1# configure terminal
R1(config)# interface GigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)# ip address 192.168.201.217 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# vrrp 1 priority 120
R1(config-if-GigabitEthernet 0/0)# vrrp 1 timers advertise 3
R1(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.201.1
R1(config-if-GigabitEthernet 0/0)# vrrp 1 track GigabitEthernet 2/1 30
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)# interface GigabitEthernet 2/1
R1(config-if-GigabitEthernet 2/1)# ip address 202.101.90.63 255.255.255.0
R1(config-if-GigabitEthernet 2/1)# exit
R1(config)# router ospf
R1(config-router)# network 202.101.90.0 0.0.0.255 area 10
R1(config-router)# network 192.168.201.0 0.0.0.255 area 10
```

Perform the following configuration on router 2:

```
R2> enable
R2# configure terminal
R2(config)# interface GigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)# ip address 192.168.201.213 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.201.1
R2(config-if-GigabitEthernet 0/0)# vrrp 1 timers advertise 3
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)# interface GigabitEthernet 1/1
R2(config-if-GigabitEthernet 1/1)# no switchport
R2(config-if-GigabitEthernet 1/1)# ip address 60.154.101.3 255.255.255.0
R2(config-if-GigabitEthernet 1/1)# exit
R2(config)# router ospf
R2(config-router)# network 60.154.101.0 0.0.0.255 area 10
R2(config-router)# network 192.168.201.0 0.0.0.255 area 10
```

5. Verification

Run the **show vrrp** command to verify the configuration.

Check whether router 1, which acts as the master router, reduces its VRRP backup group priority from 120 to 90 when GigabitEthernet2/1 connected to the wide area network (WAN) is unavailable. If yes, router 2 becomes the master router.

Check whether router 1 resumes its VRRP backup group priority from 30 to 120 when GigabitEthernet 2/1 connected to the WAN recovers. If yes, router 1 is reelected as the master router.

```
R1# show vrrp
GigabitEthernet 0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.201.217 (local), priority is 120
  Master Down interval is 10.59 sec
  Tracking state of 1 interface, 1 up:
up   GigabitEthernet 2/1 priority decrement=30
```

Check the configuration on router 2.

```
R2# show vrrp
GigabitEthernet 0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is 192.168.201.217 , priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

6. Configuration Files

- Device R1 configuration file

```
hostname R1
!
interface GigabitEthernet 0/0
 no switchport
 ip address 192.168.201.217 255.255.255.0
 vrrp 1 priority 120
 vrrp 1 timers advertise 3
 vrrp 1 ip 192.168.201.1
```

```
 vrrp 1 track GigabitEthernet 2/1 30
!
interface GigabitEthernet 2/1
 no switchport
 ip address 202.101.90.63 255.255.255.0
!
router ospf
 network 202.101.90.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
end
```

- Device R2 configuration file

```
hostname R2
!
interface GigabitEthernet 0/0
 no switchport
 ip address 192.168.201.213 255.255.255.0
 vrrp 1 timers advertise 3
 vrrp 1 ip 192.168.201.1
!
interface GigabitEthernet 1/1
 no switchport
 ip address 60.154.101.3 255.255.255.0
!
router ospf
 network 60.154.101.0 0.0.0.255 area 10
 network 192.168.201.0 0.0.0.255 area 10
!
end
```

- Device R3 configuration file

```
hostname R3
!
interface GigabitEthernet 0/0
 no switchport
 ip address 192.168.12.217 255.255.255.0
!
interface GigabitEthernet 1/1
 no switchport
 ip address 60.154.101.5 255.255.255.0
!
interface GigabitEthernet 2/1
 no switchport
 ip address 202.101.90.61 255.255.255.0
!
router ospf
```

```
 network 202.101.90.0 0.0.0.255 area 10
 network 192.168.12.0 0.0.0.255 area 10
 network 60.154.101.0 0.0.0.255 area 10
!

end
```

7. Common Errors

- Different virtual IP addresses of VRRP are configured on the routers in the same VRRP group, resulting in multiple master routers in the group.
- Different VRRP advertisement transmission intervals are configured on the routers in the same VRRP group and the timer learning function is not configured. As a result, multiple master routers arise in the group.
- Different VRRP packet versions are configured on the routers in the same VRRP group, resulting in multiple master routers in the group.
- For VRRPv2, the Ethernet ports of the routers in the same VRRP group all use the plaintext password authentication mode but use different authentication strings. As a result, multiple master routers arise in the group.

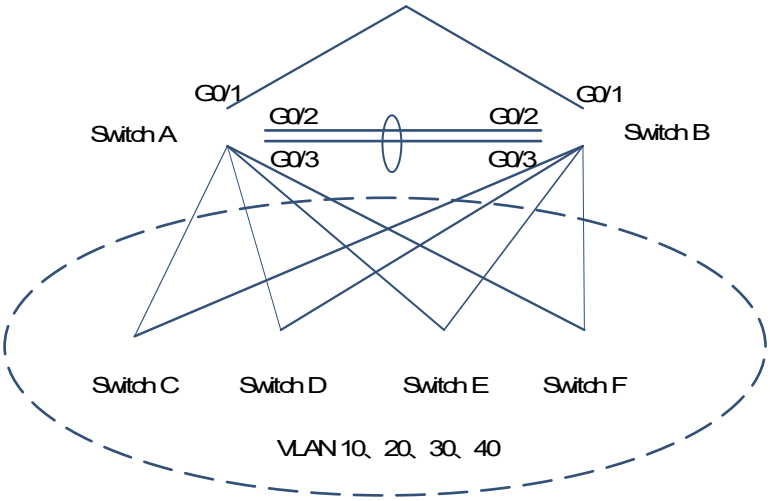
1.10.2 Configuring VRRP + MSTP

1. Requirements

As shown in Figure 1-1, VRRP and Multiple Spanning Tree Protocol (MSTP) can be configured to build a dual link backup network by using access devices and aggregation devices.

2. Topology

Figure 1-1 **Topology for Configuring VRRP + MSTP**



3. Notes

- Enable MSTP on devices (switches A, B, C, D, E, and F in this example). Configure VLAN-instance mappings (map VLANs 10 and 20 to instance 1, VLANs 30 and 40 to instance 2, and the rest VLANs to

instance 0), and configure gateway devices (switches A and B in this example) as the root bridges of corresponding instances.

- Add the SVIs of all VLANs to corresponding VRRP backup groups, and set gateways to the master and backup routers of corresponding backup groups.Table 1-1 lists the configuration details in the example.

Table 1-1 Parameters for VRRP + MSTP Topology Configuration

Gateway	VLAN ID	SVI	Backup Group	Virtual IP Address	State
Switch A	10	192.168.10.2	VRRP 10	192.168.10.1	Master
Switch B		192.168.10.3			Backup
Switch A	20	192.168.20.2	VRRP 20	192.168.20.1	Master
Switch B		192.168.20.3			Backup
Switch A	30	192.168.30.2	VRRP 30	192.168.30.1	Backup
Switch B		192.168.30.3			Master
Switch A	40	192.168.40.2	VRRP 40	192.168.40.1	Backup
Switch B		192.168.40.3			Master

- Configure the uplink ports (port GigabitEthernet 0/1 of switches A and B in the example) of master routers in backup groups as the monitored ports of the master routers.
  - Create VLANs. Create VLANs 10, 20, 30, and 40 on switches A and B.
  - Configure MST regions. Map VLANs 10 and 20 to instance 1, VLANs 20 and 30 to instance 2, and the rest VLANs to instance 0 on switches A and B.
  - Configure switch A as the root bridge of MST 0 and MST 1, and switch B as the root bridge of MST 2.
  - Enable MSTP.
  - Configure SVIs for all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the backup groups. Table 1-1 provides the corresponding configuration parameters.
  - Configure master routers and backup routers for all the groups.
  - Configure the uplink ports of master routers in VRRP backup groups as monitored ports (which must be L3 ports) of the VRRP groups.
  - Configure the interconnected ports of the core routers as an aggregate port (AP).

4. Procedure

(1) Perform the following configuration on Switch A:

Create VLANs 10, 20, 30, and 40.

```
SwitchA> enable
SwitchA# configure terminal
SwitchA(config)# vlan range 10,20,30,40
SwitchA(config)# exit
```

Map VLANs 10 and 20 to instance 1, VLANs 30 and 40 to instance 2, and the rest VLANs to instance 0.

```
SwitchA(config)# spanning-tree mst configuration
SwitchA(config-mst)# instance 1 vlan 10,20
SwitchA(config-mst)# instance 2 vlan 30,40
SwitchA(config-mst)# exit
```

On switch A, set the priority of MST 0 and MST 1 to **4096**, and the priority of MST 2 to **8192**.

```
SwitchA(config)# spanning-tree mst 0 priority 4096
SwitchA(config)# spanning-tree mst 1 priority 4096
SwitchA(config)# spanning-tree mst 2 priority 8192
```

Enable MSTP.

```
SwitchA(config)# spanning-tree
```

Configure SVIs for all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the backup groups.

```
SwitchA(config)# interface vlan 10
SwitchA(config-if-VLAN 10)# ip address 192.168.10.2 255.255.255.0
SwitchA(config-if-VLAN 10)# vrrp 10 ip 192.168.10.1
SwitchA(config-if-VLAN 10)# exit
SwitchA(config)# interface vlan 20
SwitchA(config-if-VLAN 20)# ip address 192.168.20.2 255.255.255.0
SwitchA(config-if-VLAN 20)# vrrp 20 ip 192.168.20.1
SwitchA(config-if-VLAN 20)# exit
SwitchA(config)# interface vlan 30
SwitchA(config-if-VLAN 30)# ip address 192.168.30.2 255.255.255.0
SwitchA(config-if-VLAN 30)# vrrp 30 ip 192.168.30.1
SwitchA(config-if-VLAN 30)# exit
SwitchA(config)# interface vlan 40
SwitchA(config-if-VLAN 40)# ip address 192.168.40.2 255.255.255.0
SwitchA(config-if-VLAN 40)# vrrp 40 ip 192.168.40.1
SwitchA(config-if-VLAN 40)# exit
```

Increase the priority of backup groups 10 and 20 on switch A to **120**.

```
SwitchA(config)# interface vlan 10
SwitchA(config-if-VLAN 10)# vrrp 10 priority 120
SwitchA(config-if-VLAN 10)# exit
SwitchA(config)# interface vlan 20
SwitchA(config-if-VLAN 20)# vrrp 20 priority 120
SwitchA(config-if-VLAN 20)# exit
```

Configure the port GigabitEthernet 0/1 of switch A as a route port, and set the IP address to10.10.1.1/24.

```
SwitchA(config)# interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)# no switchport
SwitchA(config-if-GigabitEthernet 0/1)# ip address 10.10.1.1 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)# exit
```

Configure the port GigabitEthernet 0/1 of switch A as the monitored port of backup groups 10 and 20, and set *Priority decrement* to 30.

```
SwitchA(config)# interface vlan 10
SwitchA(config-if-VLAN 10)# vrrp 10 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 10)# exit
SwitchA(config)# interface vlan 20
SwitchA(config-if-VLAN 20)# vrrp 20 track gigabitEthernet 0/1 30
SwitchA(config-if-VLAN 20)# exit
```

Configure the ports GigabitEthernet 0/2 and GigabitEthernet 0/3 to belong to an AP, and configure the AP as a trunk port.

```
SwitchA(config)# interface range gigabitEthernet 0/2-3
SwitchA(config-if-range)# port-group 1
SwitchA(config)# interface aggregateport 1
SwitchA(config-if-AggregatePort 1)# switchport mode trunk
```

(2) Perform the following configuration on switch B:

Create VLANs 10, 20, 30, and 40.

```
SwitchB> enable
SwitchB# configure terminal
SwitchB(config)# vlan range 10,20,30,40
SwitchB(config-vlan-range)# exit
```

Map VLANs 10 and 20 to instance 1, VLANs 30 and 40 to instance 2, and the rest VLANs to instance 0.

```
SwitchB(config)# spanning-tree mst configuration
SwitchB(config-mst)# instance 1 vlan 10,20
SwitchB(config-mst)# instance 2 vlan 30,40
SwitchB(config-mst)# exit
```

On switch B, set the priority of MST 2 to **4096**, and the priority of MST 0 and MST 1 to **8192**.

```
SwitchB(config)# spanning-tree mst 2 priority 4096
SwitchB(config)# spanning-tree mst 0 priority 8192
SwitchB(config)# spanning-tree mst 1 priority 8192
```

Enable MSTP.

```
SwitchB(config)# spanning-tree
```

Configure SVIs for all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the backup groups.

```
SwitchB(config)# interface vlan 10
SwitchB(config-if-VLAN 10)# ip address 192.168.10.3 255.255.255.0
SwitchB(config-if-VLAN 10)# vrrp 10 ip 192.168.10.1
SwitchB(config-if-VLAN 10)# exit
SwitchB(config)# interface vlan 20
SwitchB(config-if-VLAN 20)# ip address 192.168.20.3 255.255.255.0
SwitchB(config-if-VLAN 20)# vrrp 20 ip 192.168.20.1
SwitchB(config-if-VLAN 20)# exit
SwitchB(config)# interface vlan 30
SwitchB(config-if-VLAN 30)# ip address 192.168.30.3 255.255.255.0
SwitchB(config-if-VLAN 30)# vrrp 30 ip 192.168.30.1
SwitchB(config-if-VLAN 30)# exit
```

```
SwitchB(config)# interface vlan 40
SwitchB(config-if-VLAN 40)# ip address 192.168.40.3 255.255.255.0
SwitchB(config-if-VLAN 40)# vrrp 40 ip 192.168.40.1
SwitchB(config-if-VLAN 40)# exit
```

Increase the priority of VRRP 30 and VRRP 40 on switch B to **120**.

```
SwitchB(config)# interface vlan 30
SwitchB(config-if-VLAN 30)# vrrp 30 priority 120
SwitchB(config-if-VLAN 30)# exit
SwitchB(config)# interface vlan 40
SwitchB(config-if-VLAN 40)# vrrp 40 priority 120
SwitchB(config-if-VLAN 40)# exit
```

Configure the port GigabitEthernet 0/1 of switch B as a route port, and set the IP address to 10.10.2.1/24.

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)# no switchport
SwitchB(config-if-GigabitEthernet 0/1)# ip address 10.10.2.1 255.255.255.0
SwitchB(config-if-GigabitEthernet 0/1)# exit
```

Configure the port GigabitEthernet 0/1 of switch B as the monitored port of backup groups 30 and 40, and set *Priority decrement* to 30.

```
SwitchB(config)# interface vlan 30
SwitchB(config-if-VLAN 30)# vrrp 30 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 30)# exit
SwitchB(config)# interface vlan 40
SwitchB(config-if-VLAN 40)# vrrp 40 track gigabitEthernet 0/1 30
SwitchB(config-if-VLAN 40)# exit
```

Configure the ports GigabitEthernet 0/2 and GigabitEthernet 0/3 to belong to an AP, and configure the AP as a trunk port.

```
SwitchB (config)# interface range gigabitEthernet 0/2-3
SwitchB (config-if-range)# port-group 1
SwitchB (config)# interface aggregateport 1
SwitchB (config-if-AggregatePort 1)# switchport mode trunk
```

5. Verification

Run the **show run** and **show vrrp brief** commands to check whether the configuration is correct.

```
SwitchA# show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
```

```
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.2 255.255.255.0
 vrrp 10 priority 120
 vrrp 10 ip 192.168.10.1
 vrrp 10 track GigabitEthernet 0/1 30
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.2 255.255.255.0
 vrrp 20 priority 120
 vrrp 20 ip 192.168.20.1
 vrrp 20 track GigabitEthernet 0/1 30
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.2 255.255.255.0
 vrrp 30 ip 192.168.30.1
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.2 255.255.255.0
 vrrp 40 ip 192.168.40.1
```

Check the VRRP state of device A.

```
SwitchA# show vrrp brief
```

```
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   120  3      -    P    Master  192.168.10.2  192.168.10.1
VLAN 20    20   120  3      -    P    Master  192.168.20.2  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.3  192.168.40.1
```

Disconnect the uplink of switch A and check the VRRP state of the device.

```
SwitchA# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   90   3      -    P    Backup  192.168.10.3  192.168.10.1
VLAN 20    20   90   3      -    P    Backup  192.168.20.3  192.168.20.1
VLAN 30    30   100  3      -    P    Backup  192.168.30.3  192.168.30.1
VLAN 40    40   100  3      -    P    Backup  192.168.40.3  192.168.40.1
```

Check the configuration of switch B.

```
SwitchB# show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
```

```
 no ip proxy-arp
 ip address 192.168.10.3 255.255.255.0
 vrrp 10 ip 192.168.10.1
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 priority 120
 vrrp 30 ip 192.168.30.1
 vrrp 30 track GigabitEthernet 0/1 30
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 priority 120
 vrrp 40 ip 192.168.40.1
 vrrp 40 track GigabitEthernet 0/1 30
```

Check the VRRP state of device B.

```
SwitchB# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Backup  192.168.10.2  192.168.10.1
VLAN 20    20   100  3      -    P    Backup  192.168.20.2  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

Disconnect the uplink of switch B and check the VRRP state of the device.

```
SwitchB# show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State   Master addr   Group addr
VLAN 10    10   100  3      -    P    Master  192.168.10.3  192.168.10.1
VLAN 20    20   100  3      -    P    Master  192.168.20.3  192.168.20.1
VLAN 30    30   120  3      -    P    Master  192.168.30.3  192.168.30.1
VLAN 40    40   120  3      -    P    Master  192.168.40.3  192.168.40.1
```

6. Configuration Files

- Switch A configuration file

```
hostname SwitchA
!
vlan 10
!
vlan 20
!
```

```
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 4096
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 8192
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.2 255.255.255.0
 vrrp 10 priority 120
 vrrp 10 ip 192.168.10.1
 vrrp 10 track GigabitEthernet 0/1 30
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.2 255.255.255.0
 vrrp 20 priority 120
 vrrp 20 ip 192.168.20.1
 vrrp 20 track GigabitEthernet 0/1 30
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.2 255.255.255.0
 vrrp 30 ip 192.168.30.1
!
interface VLAN 40
```

```
 no ip proxy-arp
 ip address 192.168.40.2 255.255.255.0
 vrrp 40 ip 192.168.40.1
```

- Switch B configuration file

```
hostname SwitchB
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.3 255.255.255.0
 vrrp 10 ip 192.168.10.1
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface VLAN 30
```

```
 no ip proxy-arp
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 priority 120
 vrrp 30 ip 192.168.30.1
 vrrp 30 track GigabitEthernet 0/1 30
!
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 priority 120
 vrrp 40 ip 192.168.40.1
 vrrp 40 track GigabitEthernet 0/1 30
```

7. Common Errors

- Different VRRP authentication modes are configured on the Ethernet ports of routers in the same VRRP group, resulting in multiple master routers in the group.
- For VRRPv2, the Ethernet ports of the routers in the same VRRP group all use the plaintext password authentication mode but use different authentication strings. As a result, multiple master routers arise in the group.
- Different VRRP advertisement transmission intervals are configured on the routers in the same VRRP group and the timer learning function is not configured. As a result, multiple master routers arise in the group.
- Different virtual IP addresses of VRRP are configured on the routers in the same VRRP group, resulting in multiple master routers in the group.