Reliability

QSR-1920, QSR-2920, QSR-3920

Оглавление

1. HA

1.1. Overview

HA (High Availability) is one high-availability management platform on the device. The service card can be swapped via the command, and also can be directly pulled out manually. When one slot is re-inserted with one service card that is the same as the previous one, the configuration on the service card will restore automatically. When one slot is inserted with one service card that is different from the previous one, the configuration is restored to null.

1.2. HA Function Configuration

Table 1-1 HA function configuration list

Configuration Task	
The hot-swap function of the service card	The hot-swap function of the service card

1.2.1. Hot-Swap Function

Configuration Conditions

Before using the hot-swap function of the card, first complete the following tasks:

- The device needs to be started stably.
- Besides, the configuration is loaded completely.

Hot-swap the Service Card

The hot-swap of the service card includes hot-swap by the command and physical hot-swap. The hot-swap function on the device is that when the user needs to upgrade the service processing capability of the card, do not need to power off and restart the device, but just need to pull out the previous card, insert the new hardware card, and configure as desired. The process has small influence for the data communication of the other service card in the system. When the user service or the network plan needs to be improved, you can directly pull out the previous slot card, insert the new card, and configure the card. Similarly, the process has small influence for the data communication of the other service cards in the system.

Besides, when the hardware of one card in the system fails, you can pull out the card to maintain, but do not need to power off or restart the device. This can ensure that the service communication not related with the card is not interrupted and also has small influence for the system stability.

Table 1-2 Hot-swap the service card

Step	**Command**	**Description**
Hot-swap the service card	**hotswap lpu** *lpuNo* **in** | **out**	Mandatory

Caution:

- In order to avoid affecting the stable operation of the system and the service life of the connector, it is not recommended to manually hot-swap the board. It is recommended to use the command or swap the board through the hot-swap button on the board.
- It is strictly prohibited to perform hot-swap of the board while the board is loading or unloading. Otherwise, the normal operation of the system service may be affected.

2. VRRP

2.1. Overview

VRRP (Virtual Router Redundancy Protocol) is one fault tolerance protocol. It ensures that when the next-hop device of the host fails, it can be replaced by another device in time, so as to ensure the continuity and reliability of the communication. To make VRRP work, first create one virtual IP address and MAC address. In this way, add one virtual device in the network. However, when the host in the network communicates with the virtual device, do not need to know any information of the physical device on the network. One virtual device comprises one host (master) and several slave devices (backup). The master device realizes the real forwarding function. When the master device fails, the slave device becomes the new master device and takes over its work.

The master device mentioned in the following text is replaced by “Master” and the slave device is replaced by “Backup”.

2.2. VRRP Function Configuration

Table 2-1 VRRP function configuration list

Configuration Task	
Configure the VRRP basic functions	Enable the VRRP protocol
	Configure the VRRP priority
	Configure the VRRP preemption mode
	Configure the virtual MAC address of VRRP
Configure the VRRP association group	Configure the VRRP association group
Configure the VRRP network authentication	Configure the VRRP simple text authentication
Configure VRRP to link with Track	Configure VRRP to link with Track to monitor the Master uplink line
	Configure VRRP to link with Track to monitor the Master and Backup interconnection line

2.2.1. Configure VRRP Basic Functions

In the configuration tasks of VRRP, first enable the VRRP protocol and the virtual IP address of the VRRP group needs to be in the same segment as the IP address of the interface so that the configured other functions can take effect.

Configuration Condition

Before configuring the VRRP basic functions, first complete the following task:

- Configure the IP address of the interface

Enable VRRP Protocol

To enable the VRRP function, you need to create the VRRP group and configure the virtual IP address in the interface.

Table 2-2 Enable the VRRP protocol

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the VRRP group	**vrrp** *vrid* **ip** *ip-address*	Mandatory Enable the VRRP protocol. The vrid is the VRRP group number. ip-address is the virtual IP address.

Configure VRRP Priority

After configuring VRRP and if not setting priority, the default priority is 100. The device with high priority is elected as the Master for forwarding the packet and the other become Backup. If the priorities of all devices are equal, elect according to the interface IP address of the device. The one with large interface IP address becomes Master. We can set the VRRP priority as desired. The larger the value is, the higher the priority is.

Table 2-3 Configure the VRRP priority

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the VRRP group priority	**vrrp** *vrid* **priority** *priority*	Mandatory Configure the VRRP priority. The default priority is 100.

Note:

- When the interface IP address is the same as the virtual IP address, it immediately becomes Master and the priority is always 255.

Configure VRRP Preemption Mode

After configuring VRRP, in the preemption mode, once other device in the VRRP group discovers that its priority is higher than that of the current Master, it becomes Master; in non-preemption mode, as long as Master does not fail, even the other device has higher priority, it cannot become Master.

Table 2-4 Configure the VRRP preemption mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the VRRP group as the preemption mode	**vrrp** *vrid* **preempt**	Mandatory By default, enable the preemption mode

Configure Virtual MAC Address of VRRP

One virtual router in the VRRP group has one virtual MAC address. According to RFC2338, the format of the virtual MAC address is 00-00-5E-00-01-{vrid}. When the virtual router replies the ARP request, the replied is virtual MAC address, but not the real MAC address of the interface. By default, the used is the real MAC address of the interface.

Table 2-5 Configure the virtual MAC address of VRRP

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure VRRP to use the virtual MAC address	**vrrp** *vrid* **use-vmac**	Mandatory By default, use the real MAC address.

Note:

- By default, after configuring VRRP, the used is the real MAC address. After configuring the command of this section, use the virtual MAC, that is, when the host sends the packet, forward by the virtual MAC address; after deleting the command of this section, use the real MAC address, that is, when the host sends the packet, use the real MAC address to forward.

2.2.2. Configure VRRP Link Group

Enable the VRRP link group on the sub interface of the VRRP device. The Active group in the link group sends the packet. The non-active group status keeps consistent with the Active group status, that is, if the Active group status switches, the non-Active group status also switches.

Configuration Condition

Before configuring the VRRP link group, first complete the following task:

- Configure multiple VRRP groups

Configure VRRP Link Group

To configure the VRRP link group, first create one VRRP link group and then add the configured common VRRP group to the created link group. When the common VRRP group is added to the link group, it can be added in the Active or non-Active group form, but one link group should have one Active group and can only have one Active group.

Table 2-6 Configure the VRRP link group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the link group	**vrrp linkgroup** *lgid* [**interval** *Interval-time*]	Mandatory By default, the Interval-time value is 1000ms
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Add the VRRP general group to the link group by the Active mode	**vrrp** *vrid* **linkgroup** *lrid* [**active**]	Mandatory If not selecting active, add by the non-active mode.

Note:

- Besides the link group, multiple VRRP groups also can realize the load balance. For details, refer to the chapter of “Configure VRRP Load Balance” in “VRRP Typical Configuration Example”.
- In the link group, after the VRRP general group is added, the general group timer becomes invalid, that is, the sending period of the general group VRRP packets takes the timer of the link group as reference.

2.2.3. Configure VRRP Network Authentication

VRRP supports the simple text authentication. The set length of the text authentication cannot 8-bit authentication word.

Configuration Condition

Before configuring the VRRP network authentication, first complete the following task:

- Configure one VRRP group

Configure VRRP Simple Text Authentication

Table 2-7 Configure the VRRP simple text authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the VRRP simple text authentication	**vrrp** *vrid* **authentication text** *string*	Mandatory By default, do not enable the simple text authentication function.

2.2.4. Configure VRRP to Link with Track

VRRP can monitor the status of the uplink line and Master, Backup interconnection line to improve the VRRP reliability.

Configuration Condition

Before configuring VRRP to link with Track, first complete the following task:

- Configure one VRRP group

Configure VRRP to Link with Track to Monitor Master Uplink Line

On Master, configure linking with Track. It can associate with the interface via Track, or associate with BFD, RTR to make it concern the status of the uplink interface. After the uplink interface is down, VRRP can reduce the Master priority via the configured decrement. Here, after Backup receives, it automatically switches to Master (note that the Master priority is lower than Backup priority). If it is necessary to switch Backup fast, we can configure receiving low-priority fast switching command on Backup. For details, refer to the following figure.

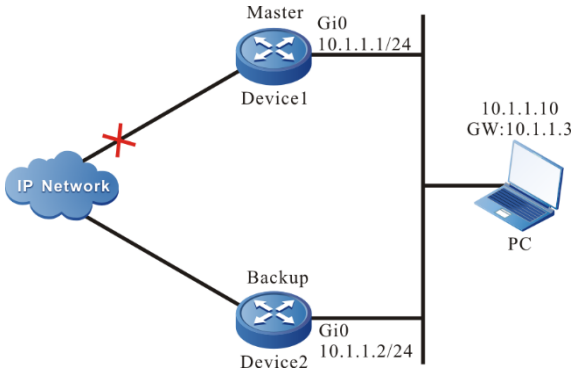

Figure 2-1 Configure VRRP to link with Track to monitor Master uplink line

Configure VRRP to Link with Track to Associate with Uplink Interface

Associate VRRP with the concerned uplink interface via Track. When the uplink interface is down, Master automatically reduces its own priority. Here, Backup receives the low-priority VRRP

packet and switches to Master. If the user is configured with “Receive low-priority packet fast switching”, that is, low-pri-master function, Backup fast switches to Master.

Table 2-8 Configure VRRP to link with Track to associate with uplink interface (configure on Master)

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure VRRP to associate with the uplink interface	**vrrp** *vrid* **track** *interface-name* [*decrement*]	Mandatory By default, the priority consumption value is 10.
Configure VRRP receiving low-priority packet fast switching function	**vrrp** *vrid* **switchover low-pri-master**	Optional The command is configured on Backup to switch fast when the Master priority is reduced.

Configure VRRP to Link with Track (Track Linking with BFD, RTR and so on)

If Track is associated with BFD, RTR and so on, Master can directly associate with Track, so as to monitor the line. When the line fails, Master reduces its own priority. Here, Backup receives the low-priority VRRP packet and switches to Master. If the user is configured with “Receive low-priority packet fast switching”, that is, low-pri-master function, Backup fast switches to Master.

Table 2-9 Configure Master to link with Track (Track linking with BFD, RTR and so on)

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure VRRP to associate with the uplink interface	**vrrp** *vrid* **track** *track-id* [*decrement*]	Mandatory By default, the priority consumption value is 10.

Step	Command	Description
Configure VRRP receiving low-priority packet fast switching function	**vrrp** *vrid* **switchover low-pri-master**	Optional The command is configured on Backup to switch fast when the Master priority is reduced.

Note:

- For the configuration method of creating Track, Track associating with BFD or RTR, refer to Track configuration manual-the Track chapter.
- If the low-pri-master function is configured and when Backup receives the low-priority packet, it switches fast. If the function is not configured when receiving the low-priority packet, Backup switches after the next timeout. If the switching time requirement is not strict, do not need to configure the low-pri-master function, but if the switching time requirement is strict, the function can make the switching time reach the ms level.

Configure VRRP to Associate with Track to Monitor Master and Backup Interconnection Line

Configure VRRP to associate with track to monitor Master and Backup interconnection line. If the line between Master and Backup is down, Backup fast switches to Master. For details, refer to the following figure.

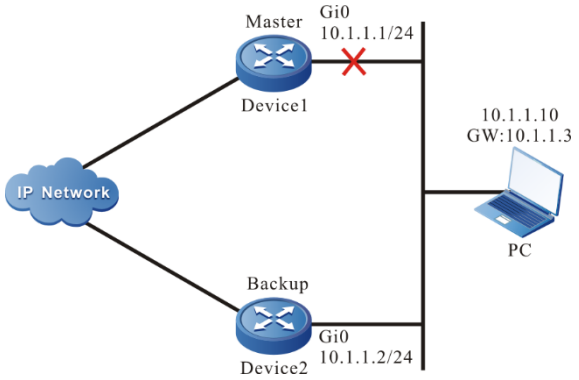

Figure 2-2 Configure VRRP to associate with track to monitor Master and Backup interconnection line

Table 2-10 Configure VRRP to associate with track to monitor Master and Backup interconnection line

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the fast switching function when Backup VRRP device finds that the line between Master and Backup is down	**vrrp** *vrid* **track** *track-id* **switchover**	Mandatory

Note:

- For the configuration of Track associating BFD and RTR, refer to Track Configuration Manual-the Track chapter.
- Track can associate with BFD to monitor the status of the line between Master and Backup.

2.2.5. VRRP Monitoring and Maintaining

Table 2-11 VRRP monitoring and maintaining

Command	Description
show vrrp [**interface** ***interface-name***] | [**linkgroup** [*linkgroup-number*]] | [**timer**]	Display the VRRP configuration information, including virtual IP address information, virtual MAC address information, device status, device priority, dependent device interface address, link group information and so on.

2.3. VRRP Typical Configuration Example

2.3.1. Configure VRRP Single-backup Group

Network Requirements

- On Device1 and Device2, create one single VRRP backup group so that Device1 and Device2 share one virtual IP address, realizing the backup for the default gateway of the user host and reducing the interruption time of the network.

Network Topology

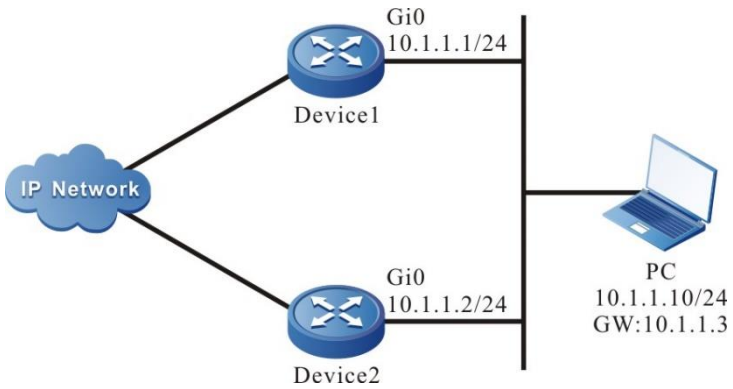

Figure 2-3 Networking of configuring VRRP single backup group

Configuration Steps

Step 1: Configure the IP address of the interface.(Omitted)

Step 2: Create the VRRP group.

#On Device1, configure VRRP group 1, the virtual IP address is 11.1.3, and configure the priority as 110.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device1(config-if-gigabitethernet0)#vrrp 1 priority 110
Device1(config-if-gigabitethernet0)#exit
```

#On Device2, configure VRRP group1 and the virtual IP address is 11.1.3.

```
Device2#configure terminal
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device1(config-if-gigabitethernet0)#exit
```

Step 3: Check the result.

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface gigabitethernet0 (Flags 0x1)
 Pri-addr : 11.1.1
 Vrf : 0
 Virtual router : 1
  Virtual IP address : 11.1.3
```

```
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:11.1.1/24
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1s
Authentication Mode : None
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface gigabitethernet0 (Flags 0x1)
 Pri-addr : 11.1.2
 Vrf : 0
 Virtual router : 1
  Virtual IP address : 11.1.3
  Virtual MAC address : 00-00-5e-00-01-01
  Depend prefix:11.1.2/24
  State : Backup
  Master addr : 11.1.1
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1 s
  Authentication Mode : None
```

We can see that the VRRP status of Device1 is Master and the VRRP status of Device2 is Backup. Device1 and Device2 share one virtual IP address. The host communicates with the network via the address. When Device1 fails, Device2 switches to Master at once for forwarding data.

Note:

- The election principle of the VRRP status is by priority. The one with large priority is Master. If the priorities are the same, compare according to the IP address of the interface. The one with large IP address is Master.
- By default, VRRP works in the preemption mode. The default priority is 100.

2.3.2. Configure VRRP Multi-Backup Group

Network Requirements

- VRRP multi-backup group is the VRRP link group. On Device1 and Device2 sub interfaces, enable VRRP and add to the link group. Only the Active group in the link group interacts the protocol packets.
- The VRRP status of the non-Active keeps consistent with the VRRP status of the Active group. When the Active group status switches, the non-Active group also switches.

Network Topology

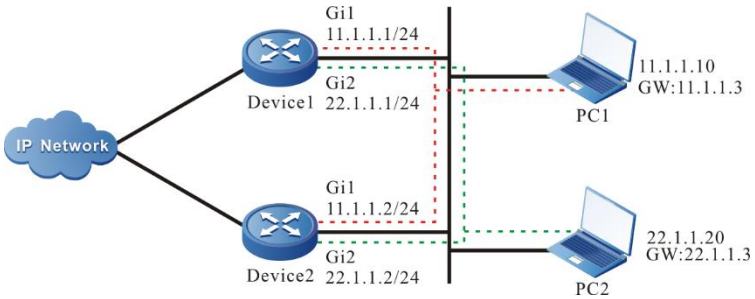

Figure 2-4 VRRP multi-backup group networking

Configuration Steps

Step 1: Configure the IP address of the interface.(Omitted)

Step 2: Create one VRRP link group.

#Configure VRRP link group 1 on Device1.

```
Device1#configure terminal
Device1(config)#vrrp linkgroup 1
```

#Configure VRRP link group 1 on Device2.

```
Device2#configure terminal
Device2(config)#vrrp linkgroup 1
```

Step 3: Create the VRRP group.

#Configure the virtual IP address of the VRRP group 1 as 11.1.1.3 on Device1 sub interface.

```
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#vrrp 1 ip 11.1.1.3
Device1(config-if-gigabitethernet1)#exit
```

#Configure the virtual IP address of the VRRP group 2 as 22.1.1.3 on Device1 sub interface.

```
Device1(config)#interface gigabitethernet2
Device1(config-if-gigabitethernet2)#vrrp 2 ip 22.1.1.3
Device1(config-if-gigabitethernet2)#exit
```

#Configure the virtual IP address of the VRRP group 1 as 11.1.1.3 on Device2 sub interface.

```
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#vrrp 1 ip 11.1.1.3
Device1(config-if-gigabitethernet1)#exit
```

#Configure the virtual IP address of the VRRP group 2 as 22.1.1.3 on Device2 sub interface.

```
Device2(config)#interface gigabitethernet2
Device2(config-if-gigabitethernet2)#vrrp 2 ip 22.1.1.3
Device1(config-if-gigabitethernet2)#exit
```

Step 4: Configure VRRP to add to the link group.

#On Device1, the VRRP group 1 is added to the link group in Active mode.

```
Device1(config)#interface gigabitethernet1
Device1(config-if-gigabitethernet1)#vrrp 1 linkgroup 1 active
Device1(config-if-gigabitethernet1)#exit
```

#On Device1, the VRRP group 2 is added to the link group in non-Active mode.

```
Device1(config)#interface gigabitethernet2
Device1(config-if-gigabitethernet2)#vrrp 2 linkgroup 1
Device1(config-if-gigabitethernet2)#exit
```

#On Device2, the VRRP group 1 is added to the link group in Active mode.

```
Device2(config)#interface gigabitethernet1
Device2(config-if-gigabitethernet1)#vrrp 1 linkgroup 1 active
Device1(config-if-gigabitethernet1)#exit
```

#On Device2, the VRRP group 2 is added to the link group in non-Active mode.

```
Device2(config)#interface gigabitethernet2
Device2(config-if-gigabitethernet2)#vrrp 2 linkgroup 1
Device1(config-if-gigabitethernet2)#exit
```

Step 5: Check the result.

#View the VRRP status on Device1.

```
Device1#show vrrp
Interface gigabitethernet1 (Flags 0x1)
  Pri-addr : 11.1.1.1
  Vrf : 0
  Virtual router : 1
    Linkgroup : 1
    Active : TRUE
    Virtual IP address : 11.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1.1/24
    State : Backup
    Master addr : 11.1.1.2
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None

Interface gigabitethernet2 (Flags 0x1)
  Pri-addr : 22.1.1.1
  Vrf : 0
  Virtual router : 2
    Linkgroup : 1
    Active : FALSE
    Virtual IP address : 22.1.1.3
    Virtual MAC address : 00-00-5e-00-01-02
    Depend prefix:22.1.1.1/24
    State : Backup
    Master addr : 0.0.0.0
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
Authentication Mode : None
#View the VRRP status on Device2.
```

```
Device2#show vrrp
Interface gigabitethernet1 (Flags 0x1)
  Pri-addr : 11.1.1.2
  Vrf : 0
  Virtual router : 1
    Linkgroup : 1
    Active : TRUE
    Virtual IP address : 11.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1.2/24
    State : Master
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1
    Authentication Mode : None

Interface gigabitethernet2 (Flags 0x1)
  Pri-addr : 22.1.1.2
  Vrf : 0
  Virtual router : 2
    Linkgroup : 1
    Active : FALSE
    Virtual IP address : 22.1.1.3
    Virtual MAC address : 00-00-5e-00-01-02
    Depend prefix:22.1.1.2/24
    State : Master
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
  Authentication Mode : None
```

We can see that the VRRP status of the non-Active group and Active group keep consistent.

Step 6: Configure the priority of sub interface 1 in Device1 as 110, making the status change.

```
Device1(config)#interface gigabitethernet1
```

```
Device1(config-if-gigabitethernet1)#vrrp 1 priority 110
Device1(config-if-gigabitethernet1)#exit
```

#View the VRRP status on Device1.

```
Device1#show vrrp
Interface gigabitethernet1 (Flags 0x1)
  Pri-addr : 11.1.1.1
  Vrf : 0
  Virtual router : 1
    Linkgroup : 1
    Active : TRUE
    Virtual IP address : 11.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1.1/24
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None

Interface gigabitethernet2 (Flags 0x1)
  Pri-addr : 22.1.1.1
  Vrf : 0
  Virtual router : 2
    Linkgroup : 1
    Active : FALSE
    Virtual IP address : 22.1.1.3
    Virtual MAC address : 00-00-5e-00-01-02
    Depend prefix:22.1.1.1/24
    State : Master
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
```

```
        Authentication Mode : None
```

#View the VRRP status on Device2.

```
    Device2#show vrrp
    Interface gigabitethernet1 (Flags 0x1)
      Pri-addr : 11.1.1.2
      Vrf : 0
      Virtual router : 1
        Linkgroup : 1
        Active : TRUE
        Virtual IP address : 11.1.1.3
        Virtual MAC address : 00-00-5e-00-01-01
        Depend prefix:11.1.1.2/24
        State : Backup
        Master addr : 11.1.1.1
        Normal priority : 100
        Currnet priority : 100
        Priority reduced : 0
        Preempt-mode : YES
        Advertise-interval : 1 s
        Authentication Mode : None

    Interface gigabitethernet2 (Flags 0x1)
      Pri-addr : 22.1.1.2
      Vrf : 0
      Virtual router : 2
        Linkgroup : 1
        Active : FALSE
        Virtual IP address : 22.1.1.3
        Virtual MAC address : 00-00-5e-00-01-02
        Depend prefix:22.1.1.2/24
        State : Backup
        Master addr : 0.0.0.0
        Normal priority : 100
        Currnet priority : 100
        Priority reduced : 0
        Preempt-mode : YES
        Advertise-interval : 1 s
```

```
Authentication Mode : None
```

We can see that when the status of the Active group switches, the non-Active group also changes and keeps consistent with the Active group. The Active group in the link group is responsible for sending the protocol packets, but the non-Active group does not send packets. This can reduce the interacting of the protocol packets and the network load.

Note:

- The sending interval granularity can be smaller. The minimum can be configured to the ms level, so as to reach the 50ms fast switching.

2.3.3. Configure VRRP to Link with Track

Network Requirements

- Enable VRRP between Device1 and Device2; Device1 and Device2 share one virtual IP address, realizing the backup of the default gateway of the user host.
- Device1 monitors the status of the interface gigabitethernet1 via Track. When the uplink port gigabitethernet1 of Device1 is down, VRRP can feel and switch the status, making Backup become new Master for forwarding data.

Network Topology

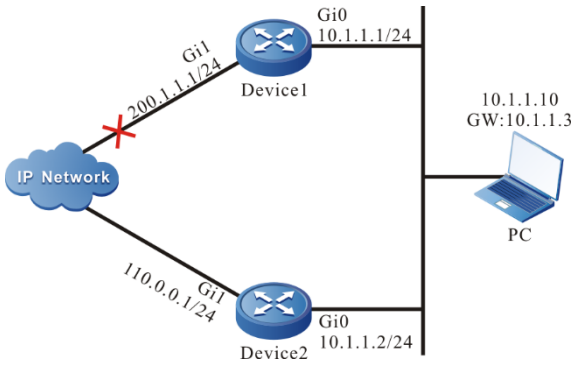

Figure 2-5 Networking of VRRP linking with Track

Configuration Steps

Step 1: Configure the IP address of the interface.(Omitted)

Step 2: Create the VRRP group.

#Configure the VRRP group 1 on Device1; the virtual IP address is 11.1.3 and the priority is 110.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device1(config-if-gigabitethernet0)#vrrp 1 priority 110
Device1(config-if-gigabitethernet0)#exit
```

#Configure the VRRP group 1 on Device2; the virtual IP address is 11.1.3.

```
Device2#configure terminal
Device2(config)#interface gigabitethernet0
```

```
Device2(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device1(config-if-gigabitethernet0)#exit
```

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface gigabitethernet0 (Flags 0x1)
  Pri-addr : 11.1.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 11.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1/24
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface gigabitethernet0 (Flags 0x1)
  Pri-addr : 11.1.2
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 11.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.2/24
    State : Backup
    Master addr : 11.1.1
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
  Authentication Mode : None
```

Step 3: Configure VRRP to link with Track.

#On Device1, configure VRRP to link with Track and monitor the uplink interface gigabitethernet1; configure the priority decrement as 20.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#vrrp 1 track gigabitethernet1 20
Device1(config-if-gigabitethernet0)#exit
```

View the VRRP status of Device1.

```
Device1#show vrrp
Interface gigabitethernet0 (Flags 0x1)
  Pri-addr : 11.1.1.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 11.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1.1/24
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None
      Track interface : gigabitethernet1
      Reduce : 20
      Reduce state : NO
```

When the uplink interface gigabitethernet1 of Device1 is down, the VRRP priority is reduced by 20. Here, the priority of Device2 is high, so the status changes.

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface gigabitethernet0 (Flags 0x1)
  Pri-addr : 11.1.1.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 11.1.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1.1/24
    State : Backup
```

```
    Master addr : 11.1.2
    Normal priority : 110
    Currnet priority : 90
    Priority reduced : 20
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None
      Track interface : gigabitethernet1
      Reduce : 20
      Reduce state : YES
  #View the VRRP status of Device2.
  Device2#show vrrp
  Interface gigabitethernet0 (Flags 0x1)
    Pri-addr : 11.1.2
    Vrf : 0
    Virtual router : 1
      Virtual IP address : 11.1.3
      Virtual MAC address : 00-00-5e-00-01-01
      Depend prefix:11.1.2/24
      State : Master
      Normal priority : 100
      Currnet priority : 100
      Priority reduced : 0
      Preempt-mode : YES
      Advertise-interval : 1 s
  Authentication Mode : None
```

Note:

- If the association of VRRP and Track needs to reach the fast switching, we can configure switchover low-pri-master on Backup.

2.3.4. Configure VRRP to Link with BFD

Network Requirements

- Enable VRRP between Device1 and Device2.
- The VRRP status switching time of Device1 and Device2 needs at least 3s and the service interruption time is long. It is necessary to configure the VRRP and BFD association on Device1 and Device2, realizing the ms-level switching.

Network Topology

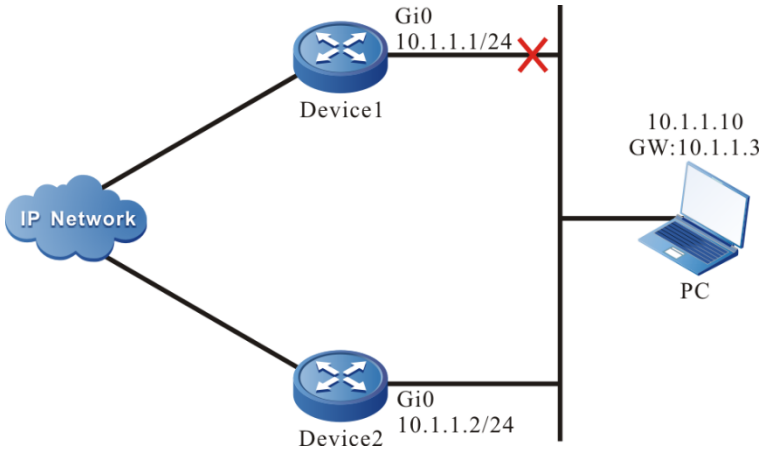

Figure 2-6 Networking of VRRP linking with BFD

Configuration Steps

Step 1: Configure the IP address of the interface.(Omitted)

Step 2: Create the VRRP group.

#Configure the VRRP group 1 on Device1; the virtual IP address is 11.1.3 and the priority is 105.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device1(config-if-gigabitethernet0)#vrrp 1 priority 105
Device1(config-if-gigabitethernet0)#exit
```

#Configure the VRRP group 1 on Device2; the virtual IP address is 11.1.3.

```
Device2#configure terminal
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device2(config-if-gigabitethernet0)#exit
```

#View the VRRP status of Device1.

```
Device1#show vrrp
Interface gigabitethernet0 (Flags 0x1)
  Pri-addr : 11.1.2
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 11.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.2/24
    State : Master
    Normal priority : 105
```

```
    Currnet priority : 105
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None
```

#View the VRRP status of Device2.

```
Device2#show vrrp
Interface gigabitethernet0 (Flags 0x1)
 Pri-addr : 11.1.2
 Vrf : 0
 Virtual router : 1
  Virtual IP address : 11.1.3
  Virtual MAC address : 00-00-5e-00-01-01
  Depend prefix:11.1.2/24
  State : Backup
  Master addr : 11.1.1
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1 s
Authentication Mode : None
```

Step 3: Configure Track to link with BFD.

#Configure Track to link with BFD on Device1.

```
Device1(config)#track 1
Device1(config-track)#bfd interface gigabitethernet0 remote-ip 11.1.2 local-ip 11.1.1
Device1(config-track)#exit
```

#Configure Track to link with BFD on Device2.

```
Device2#configure terminal
Device2(config)#track 1
Device2(config-track)#bfd interface gigabitethernet0 remote-ip 11.1.1 local-ip 11.1.2
Device2(config-track)#exit
```

#View the BFD status on Device1.

```
Device1#show bfd session
```

```
OurAddr          NeighAddr        LD/RD        State        Holddown
interface
11.1.1           11.1.2           6/7          UP           5000
gigabitethernet0
```

#View the BFD status on Device2.

```
Device2#show bfd session
OurAddr          NeighAddr        LD/RD        State        Holddown
interface
11.1.2           11.1.1           7/6          UP           5000
gigabitethernet0
```

Step 4: Configure VRRP to link with Track.

#Configure VRRP to link with Track on Device2 and configure switchover.

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#vrrp 1 track 1 switchover
Device2(config-if-gigabitethernet0)#exit
```

Step 5: Check the result.

#View the VRRP status on Device2.

```
Device2#show vrrp
 Interface gigabitethernet0 (Flags 0x1)
  Pri-addr : 11.1.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 11.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1/24
    State : Backup
    Master addr : 11.1.2
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None
     Track object : 1
     Switchover state : NO
```

When Device1 line fails, BFD session is down and Track also becomes down. Device2 feels at once and switches to Master forwarding data.

#View the BFD and VRRP status on Device2.

```
Device2#show bfd session
OurAddr         NeighAddr         LD/RD      State      Holddown      interface
11.1.2          11.1.1            7/0        DOWN       5000          gigabitethernet0
Device2#show vrrp
Interface gigabitethernet0 (Flags 0x1)
  Pri-addr : 11.1.2
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 11.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.2/24
    State : Master
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None
     Track object : 1
     Switchover state : YES
```

Note:

- When VRRP links with Track, Switchover needs to be configured on Backup. Once finding Track down, switch to Master at once.

2.3.5. Configure VRRP Load Balance

Network Requirements

- Device1 and Device2 belong to two VRRP groups at the same time; Device1 is Master in group1 and Backup in group2; Device2 is Backup in group1 and Master in group2.
- PC1 forwards data via Device1 and PC2 forwards data via Device2, realizing the load balance.

Network Topology

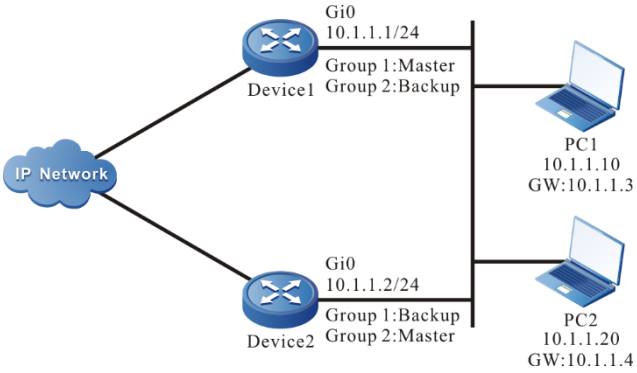

Figure 2-7 VRRP load balance networking

Configuration Steps

Step 1: Configure the IP address of the interface.(Omitted)

Step 2: Create the VRRP group 1.

#Configure the VRRP group 1 on Device1; the virtual IP address is 11.1.3 and the priority is 110.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device1(config-if-gigabitethernet0)#vrrp 1 priority 110
Device1(config-if-gigabitethernet0)#exit
```

#Configure the VRRP group 1 on Device2; the virtual IP address is 11.1.3.

```
Device2#configure terminal
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device2(config-if-gigabitethernet0)#exit
```

Step 3: Create VRRP group 2.

#Configure the virtual IP address of VRRP group2 as 11.1.4 on Device1.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#vrrp 2 ip 11.1.4
Device1(config-if-gigabitethernet0)#exit
```

#Configure the virtual IP address of VRRP group2 as 11.1.4 on Device2 and configure the priority as 110.

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#vrrp 2 ip 11.1.4
Device2(config-if-gigabitethernet0)#vrrp 2 priority 110
Device2(config-if-gigabitethernet0)#exit
```

Step 4: Check the result.

#View the status of VRRP in group1 and group2 on Device1.

```
Device1#show vrrp
Interface gigabitethernet0 (Flags 0x1)
  Pri-addr : 11.1.1
  Vrf : 0
  Virtual router : 1
    Virtual IP address : 11.1.3
    Virtual MAC address : 00-00-5e-00-01-01
    Depend prefix:11.1.1/24
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
    Authentication Mode : None

  Virtual router : 2
    Virtual IP address : 11.1.4
    Virtual MAC address : 00-00-5e-00-01-02
    Depend prefix:11.1.1/24
    State : Backup
    Master addr : 11.1.2
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 1 s
  Authentication Mode : None
```

#View the status of VRRP in group1 and group2 on Device2.

```
Device2#show vrrp
Interface gigabitethernet0 (Flags 0x1)
  Pri-addr : 11.1.2
  Vrf : 0
  Virtual router : 1
```

Virtual IP address : 11.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:11.1.2/24
State : Backup
Master addr : 11.1.1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None

Virtual router : 2
Virtual IP address : 11.1.4
Virtual MAC address : 00-00-5e-00-01-02
Depend prefix:11.1.2/24
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1 s
Authentication Mode : None

We can see that Device1 serves as Master of VRRP group1 and Backup of VRRP group2. In contrast with Device1, Device2 serves as Master of VRRP group 2 and Backup of VRRP group 2. When one device fails, two PCs forward data via the other device. This realizes the load balance and backup for each other.

3. VRRPV3

3.1. Overview

VRRPv3 (short for Virtual Router Redundancy Protocol Version 3) is one fault tolerance protocol. It ensures that when the next-hop device of the host fails, it can be replaced by another device in time, so as to ensure the continuity and reliability of the communication. To make VRRPv3 work, first create one virtual IP address and MAC address. In this way, add one virtual device in the network. However, when the host in the network communicates with the virtual device, do not need to know any information of the physical device on the network. One virtual device comprises one host (master) and several slave devices (backup). The master device realizes the real forwarding function. When the master device fails, the slave device becomes the new master device and takes over its work.

The master device mentioned in the following text is replaced by “Master” and the slave device is replaced by “Backup”.

3.2. VRRPv3 Function Configuration

Table 3-1 VRRPv3 function configuration list

Configuration Task	
Configure VRRPv3 basic functions	Enable the VRRPv3 protocol
	Configure the VRRPv3 priority
	Configure the VRRPv3 preemption mode
	Configure the virtual MAC address of VRRPv3
Configure VRRPv3 to link with Track	Configure VRRPv3 to link with Track to monitor the Master uplink line
	Configure VRRPv3 to link with Track to monitor the Master and Backup interconnection line

3.2.1. Configure VRRPv3 Basic Functions

In the configuration tasks of VRRPv3, first enable the VRRPv3 protocol and the virtual IPv6 address of the VRRPv3 group needs to be in the same segment as the IPv6 link-local address of the interface so that the configured other functions can take effect.

Configuration Condition

Before configuring the VRRPv3 basic functions, first complete the following task:

- Enable the IPv6 link-local address of the interface

Enable VRRPv3 Protocol

To enable the VRRPv3 function, you need to create the VRRP group and configure the IPv6 link-local virtual address in the interface. To configure the global virtual address, the segment of the virtual address should be in the same segment as the global real address on the interface.

Table 3-2 Enable the VRRPv3 protocol

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the link-local virtual address of the VRRPv3 group	**ipv6 vrrp** *vrid* **ip** *ip-address* **link-local**	Mandatory By default, do not enable VRRPv3.
Configure the global virtual address of VRRPv3 group	**ipv6 vrrp** *vrid* **ip** *ip-address*	Optional The configured global virtual address should be in the same segment as the global real address on the interface. By default, do not enable the global virtual address.

Configure VRRPv3 Priority

After configuring VRRPv3 and if not setting priority, the default priority is 100. The device with high priority is elected as the Master for forwarding the packet and the other become Backup. If the priorities of all devices are equal, elect according to the interface IPv6 link-local address of the device. The one with large interface IPv6 link-local address becomes Master. We can set the VRRPv3 priority as desired. The larger the value is, the higher the priority is.

Table 3-3 Configure the VRRPv3 priority

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the priority of the VRRPv3 group	**ipv6 vrrp** *vrid* **priority** *priority*	Mandatory By default, the priority of VRRPv3 is 100.

Configure VRRPv3 Preemption Mode

After configuring VRRPv3, in the preemption mode, once other device in the VRRPv3 group discovers that its priority is higher than that of the current Master, it becomes Master; in non-preemption mode, as long as Master does not fail, even the other device has higher priority, it cannot become Master.

Table 3-4 Configure the VRRPv3 preemption mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the VRRPv3 group as the preemption mode	**ipv6 vrrp** *vrid* **preempt**	Mandatory By default, enable the preemption function.

Configure Virtual MAC Address of VRRPv3

One virtual router in the VRRPv3 group has one virtual MAC address. According to RFC5798, the format of the virtual MAC address is 00-00-5E-00-02-{vrid}. By default, the used is the real MAC address of the interface.

Table 3-5 Configure the virtual MAC address of VRRPv3

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure VRRPv3 to use the virtual MAC address	**ipv6 vrrp** *vrid* **use-vmac**	Mandatory By default, VRRPv3 uses the real MAC address.

Note:

- By default, after configuring VRRPv3, the used is the real MAC address. After configuring the command of this section, use the virtual MAC, that is, when the host sends the packet, forward by the virtual MAC address; after deleting the command of this section, use the real MAC address, that is, when the host sends the packet, use the real MAC address to forward.

3.2.2. Configure VRRPv3 to Link with Track

VRRPv3 can monitor the status of the uplink line and Master, Backup interconnection line to improve the VRRPv3 reliability.

Configuration Condition

Before configuring VRRPv3 to link with Track, first complete the following task:

- Configure one VRRPv3 group

Configure VRRPv3 to Link with Track to Monitor Master Uplink Line

On Master, configure linking with Track. It can link with the interface via Track, or link with BFD, RTR to make it concern the status of the uplink interface. After the uplink interface is down, VRRPv3 can reduce the Master priority via the configured decrement. Here, after Backup receives, it automatically switches to Master (note that the Master priority is lower than Backup priority). If it is necessary to switch Backup fast, we can configure receiving low-priority fast switching command on Backup. For details, refer to the following figure.

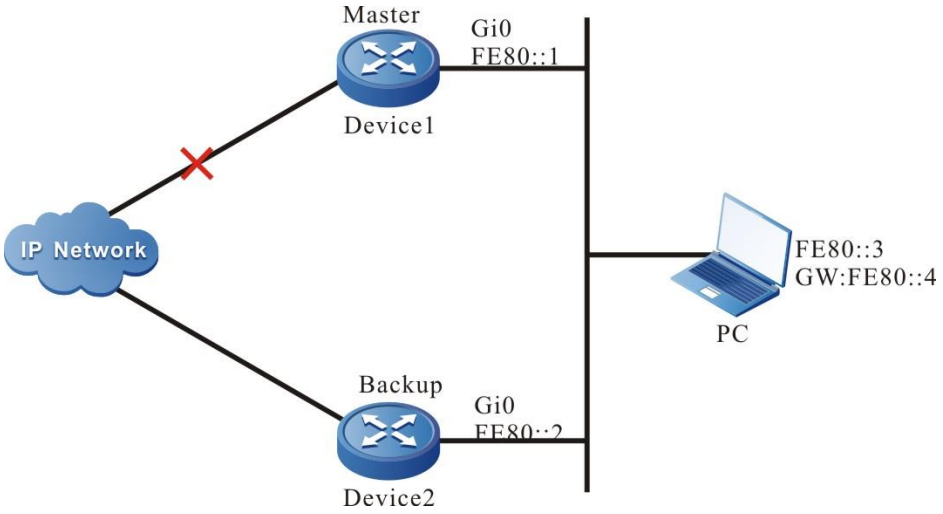

Figure 3-1 Configure VRRPv3 to link with Track to monitor Master uplink line

Configure VRRPv3 to Link with Track to Link with Uplink Interface

Associate VRRPv3 with the concerned uplink interface via Track. When the uplink interface is down, Master automatically reduces its own priority. Here, Backup receives the low-priority VRRPv3 packet and switches to Master. If the user is configured with “Receive low-priority packet fast switching”, that is, low-pri-master function, Backup fast switches to Master.

Table 3-6 Configure VRRPv3 to link with Track to link with uplink interface (configure on Master)

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure VRRPv3 to link with the uplink interface	**ipv6 vrrp** *vrid* **track** *interface-name* [*decrement*]	Mandatory By default, VRRPv3 does not link with Track.
Configure the fast switching function when VRRPv3 receives the low-priority packet	**ipv6 vrrp** *vrid* **switchover low-pri-master**	Optional By default, do not enable the low-pri-master function. The command is configured on Backup to switch fast when the Master priority is reduced.

Configure VRRPv3 to Link with Track (Track Linking with BFD, RTR and so on)

If Track is associated with BFD, RTR and so on, Master can directly link with Track, so as to monitor the line. When the line fails, Master reduces its own priority. Here, Backup receives the low-priority VRRPv3 packet and switches to Master. If the user is configured with “Receive low-priority packet fast switching”, that is, low-pri-master function, Backup fast switches to Master.

Table 3-7 Configure Master to link with Track (Track linking with BFD, RTR and so on)

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure VRRPv3 to link with the uplink interface	**ipv6 vrrp** *vrid* **track** *track-id* [*decrement*]	Mandatory By default, VRRPv3 does not link with Track.
Configure fast switching function when VRRPv3 receives low-priority packet	**ipv6 vrrp** *vrid* **switchover low-pri-master**	Optional By default, do not enable the low-pri-master function. The command is configured on Backup to switch fast when the Master priority is reduced.

Note:

- For the configuration method of creating Track, Track associating with BFD or RTR, refer to Track configuration manual.
- If the low-pri-master function is configured and when Backup receives the low-priority packet, it switches fast. If the function is not configured when receiving the low-priority packet, Backup switches after the next timeout. If the switching time requirement is not strict, do not need to configure the low-pri-master function, but if the switching time requirement is strict, the function can make the switching time reach the ms level.

Configure VRRPv3 to Link with Track to Monitor Master and Backup Interconnection Line

Configure VRRPv3 to link with track to monitor Master and Backup interconnection line. If the line between Master and Backup is down, Backup fast switches to Master. For details, refer to the following figure.

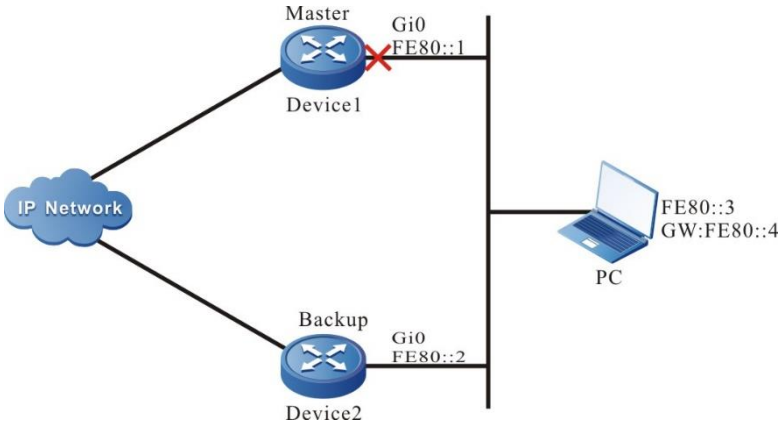

Figure 3-2 Configure VRRPv3 to link with track to monitor Master and Backup interconnection line

Table 3-8 Configure VRRPv3 to link with track to monitor Master and Backup interconnection line

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the fast switching function when Backup VRRPv3 device finds that the line between Master and Backup is down	**ipv6 vrrp** *vrid* **track** *track-id* **switchover**	Mandatory By default, VRRPv3 does not link with Track.

Note:

- For the configuration of Track associating BFD and RTR, refer to Track Configuration Manual.
- Track can link with BFD to monitor the status of the line between Master and Backup.

3.2.3. VRRPv3 Monitoring and Maintaining

Table 3-9 VRRPv3 monitoring and maintaining

Command	Description
show ipv6 vrrp [**interface** *interface-name*]	[**brief**]	Display the VRRPv3 configuration information, including virtual IP address information, virtual MAC address information, device status, device priority, dependent device interface address, link group information and so on.

3.3. VRRPv3 Typical Configuration Example

3.3.1. Configure IPv6-based VRRP Single-backup Group

Network Requirements

- On Device1 and Device2, create one single IPv6-based VRRP backup group so that Device1 and Device2 share the same virtual IPv6 link-local address and global address, realizing the backup for the default gateway of the user host and reducing the interruption time of the network.

Network Topology

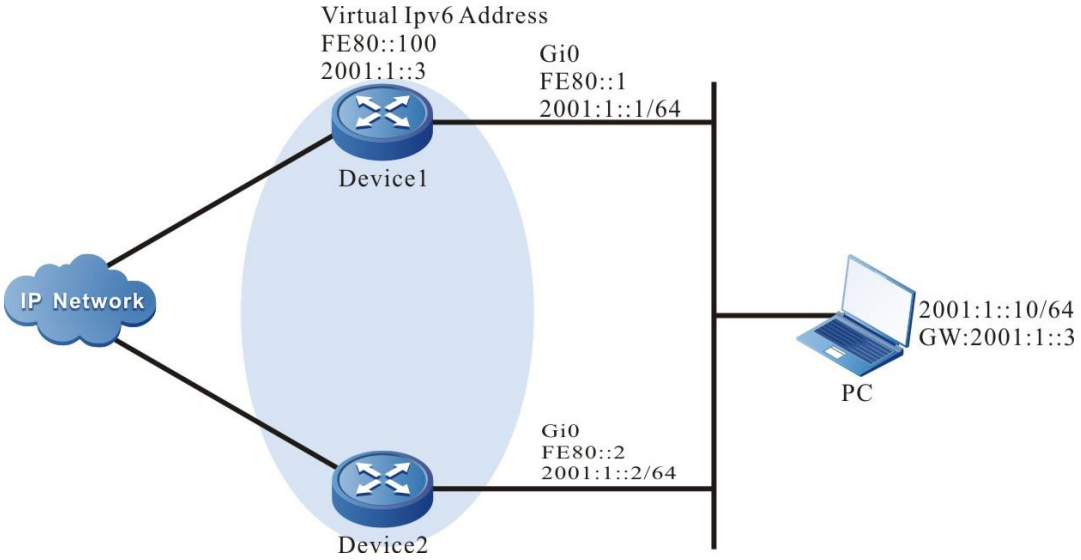

Figure 3-3 Networking of configuring IPv6-based VRRP single backup group

Configuration Steps

Step 1: Configure the IPv6 address of the interface. Enable the switch of the RA response and RA periodical sending.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ipv6 address fe80::1 link-local
Device1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
```

```
Device1(config-if-gigabitethernet0)#no ipv6 nd suppress-ra period
Device1(config-if-gigabitethernet0)#no ipv6 nd suppress-ra response
Device1(config-if-gigabitethernet0)#exit
Device2#configure terminal
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 address fe80::2 link-local
Device2(config-if-gigabitethernet0)#ipv6 address 2001:1::2/64
Device2(config-if-gigabitethernet0)#no ipv6 nd suppress-ra period
Device2(config-if-gigabitethernet0)#no ipv6 nd suppress-ra response
Device2(config-if-gigabitethernet0)#exit
```

Step 2: Create the IPv6-based VRRP group.

#On Device1, configure VRRPv3 group 1, the virtual IP address is 2001:1::3 and fe80::100, and configure the priority as 110.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 priority 110
Device1(config-if-gigabitethernet0)#exit
```

#On Device2, configure VRRPv3 group1 and the virtual IP address is 2001:1::3 and fe80::100.

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-gigabitethernet0)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-gigabitethernet0)#exit
```

Step 3: Check the result.

#View the IPv6 VRRP status of Device1.

```
Device1#show ipv6 vrrp
Interface gigabitethernet0 (Flags 0x9)
  Pri-addr : fe80::1
  Vrf : 0
  Pri-matchaddr : fe80::1
  Virtual router : 1
    Mac mode: real mac mode
    Virtual IP address : fe80::100
    Global address count:1
      Global Match address : 2001:1::1
        Global Virtual IP address : 2001:1::3
```

```
    Virtual MAC address : 00-00-5e-00-02-01
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 100
    Authentication Mode : None
```

#View the IPv6 VRRP status of Device2.

```
Device2#show ipv6 vrrp
Interface gigabitethernet0 (Flags 0x9)
  Pri-addr : fe80::2
  Vrf : 0
  Pri-matchaddr : fe80::2
  Virtual router : 1
    Mac mode: real mac mode
    Virtual IP address : fe80::100
    Global address count:1
      Global Match address : 2001:1::2
        Global Virtual IP address : 2001:1::3
    Virtual MAC address : 00-00-5e-00-02-01
    State : Backup
    Master addr : fe80::1
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 100
    Authentication Mode : None
```

We can see that the VRRPv3 status of Device1 is Master and the VRRPv3 status of Device2 is Backup. Device1 and Device2 share one virtual IP address. The host communicates with the network via the address. When Device1 fails, Device2 switches to Master at once for forwarding data.

Note:

- The election principle of the VRRPv3 status is by priority. The one with large priority is Master. If the priorities are the same, compare according to the IP link-local address of the interface. The one with large IP address is Master.
- By default, VRRPv3 works in the preemption mode. The default priority is 100.

3.3.2. Configure IPv6-based VRRP to Link with Track

Network Requirements

- On Device1 and Device2, create IPv6 VRRP single backup group; Device1 and Device2 share one virtual IPv6 link-local address and global address, realizing the backup of the default gateway of the user host, so as to reduce the network interruption time.
- Device1 monitors the status of the interface gigabitethernet1 via Track. When the uplink port gigabitethernet1 of Device1 is down, VRRPv3 can feel the down event of the monitor interface and reduce its own priority, making Backup become the new Master and continue to forward the data.

Network Topology

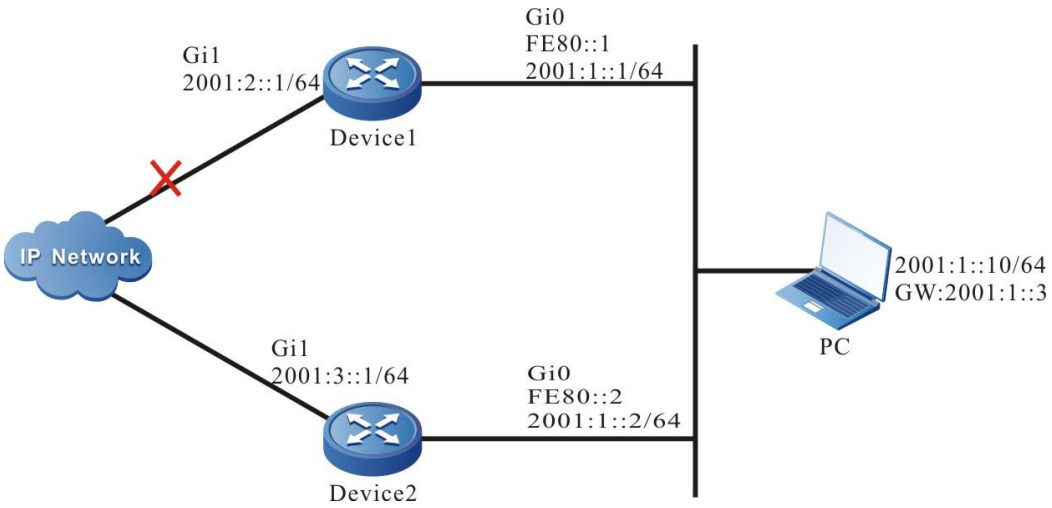

Figure 3-4 Networking of IPv6 VRRP linking with Track

Configuration Steps

Step 1: Configure the IPv6 address of the interface, and enable the switch of the RA response and the RA periodical sending.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ipv6 address fe80::1 link-local
Device1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
Device1(config-if-gigabitethernet0)#no ipv6 nd suppress-ra period
Device1(config-if-gigabitethernet0)#no ipv6 nd suppress-ra response
Device1(config-if-gigabitethernet0)#exit
Device2#configure terminal
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 address fe80::2 link-local
Device2(config-if-gigabitethernet0)#ipv6 address 2001:1::2/64
Device2(config-if-gigabitethernet0)#no ipv6 nd suppress-ra period
Device2(config-if-gigabitethernet0)#no ipv6 nd suppress-ra response
Device2(config-if-gigabitethernet0)#exit
```

Step 2: Create one IPv6 VRRP group.

#On Device1, configure VRRPv3 group 1, the virtual IP address is 2001:1::3 and fe80::100, and configure the priority as 110.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 priority 110
Device1(config-if-gigabitethernet0)#exit
```

#On Device2, configure VRRPv3 group 1, and the virtual IP address is 2001:1::3 and fe80::100.

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-gigabitethernet0)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-gigabitethernet0)#exit
```

#View the IPv6 VRRP status of Device1.

```
Device1# show ipv6 vrrp
Interface gigabitethernet0 (Flags 0x9)
  Pri-addr : fe80::1
  Vrf : 0
  Pri-matchaddr : fe80::1
  Virtual router : 1
    Mac mode: real mac mode
    Virtual IP address : fe80::100
    Global address count:1
       Global Match address : 2001:1::1
          Global Virtual IP address : 2001:1::3
    Virtual MAC address : 00-00-5e-00-02-01
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 100
    Authentication Mode : None
```

#View the IPv6 VRRP status of Device2.

```
Device2#show ipv6 vrrp
Interface gigabitethernet0 (Flags 0x9)
  Pri-addr : fe80::2
```

```
Vrf : 0
Pri-matchaddr : fe80::2
Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
     Global Match address : 2001:1::2
        Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Backup
  Master addr : fe80::1
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

Step 3: Configure VRRPv3 to link with Track.

#On Device1, configure VRRPv3 to link with Track, monitor the uplink interface gigabitethernet1, and configure the reduced value of the priority as 20.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 track gigabitethernet 1 20
Device1(config-if-gigabitethernet0)#exit
```

#View the IPv6 VRRP status of Device1.

```
Device1#show ipv6 vrrp
Interface gigabitethernet0 (Flags 0x9)
  Pri-addr : fe80::1
  Vrf : 0
  Pri-matchaddr : fe80::1
  Virtual router : 1
    Mac mode: real mac mode
    Virtual IP address : fe80::100
    Global address count:1
       Global Match address : 2001:1::1
          Global Virtual IP address : 2001:1::3
    Virtual MAC address : 00-00-5e-00-02-01
```

```
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
  Track interface : gigabitethernet1
  Reduce : 20
  Reduce state : NO
```

Step 4: Check the result.

When the monitor interface gigabitethernet1 of Device1 is down, the VRRPv3 priority is reduced by 20. Here, the Device2 priority is high, and preempts as Master, and the status switches.

#View the IPv6 VRRP status of Device1.

```
Device1#show ipv6 vrrp
Interface gigabitethernet0 (Flags 0x9)
  Pri-addr : fe80::1
  Vrf : 0
  Pri-matchaddr : fe80::1
  Virtual router : 1
    Mac mode: real mac mode
    Virtual IP address : fe80::100
    Global address count:1
       Global Match address : 2001:1::1
          Global Virtual IP address : 2001:1::3
    Virtual MAC address : 00-00-5e-00-02-01
    State : Backup
    Master addr : fe80::2
    Normal priority : 110
    Currnet priority : 90
    Priority reduced : 20
    Preempt-mode : YES
    Advertise-interval : 100
    Authentication Mode : None
      Track interface : gigabitethernet1
      Reduce : 20
      Reduce state : YES
```

#View the IPv6 VRRP status of Device2.

```
Device2#show ipv6 vrrp
Interface gigabitethernet0 (Flags 0x9)
  Pri-addr : fe80::2
  Vrf : 0
  Pri-matchaddr : fe80::2
  Virtual router : 1
    Mac mode: real mac mode
    Virtual IP address : fe80::100
    Global address count:1
      Global Match address : 2001:1::2
        Global Virtual IP address : 2001:1::3
    Virtual MAC address : 00-00-5e-00-02-01
    State : Master
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 100
    Authentication Mode : None
```

3.3.3. Configure IPv6-based VRRP Load Balance

Network Requirements

- On Device1 and Device2, create IPv6 VRRP two backup groups; Device1 and Device2 belong to two VRRPv3 groups at the same time. Device1 is Master in group1 and Backup in group 2; Device2 is Backup in group1 and Master in group 2.
- PC1 forwards data via Device1, and PC2 forwards data via Device2, realizing the load balance.

Network Topology

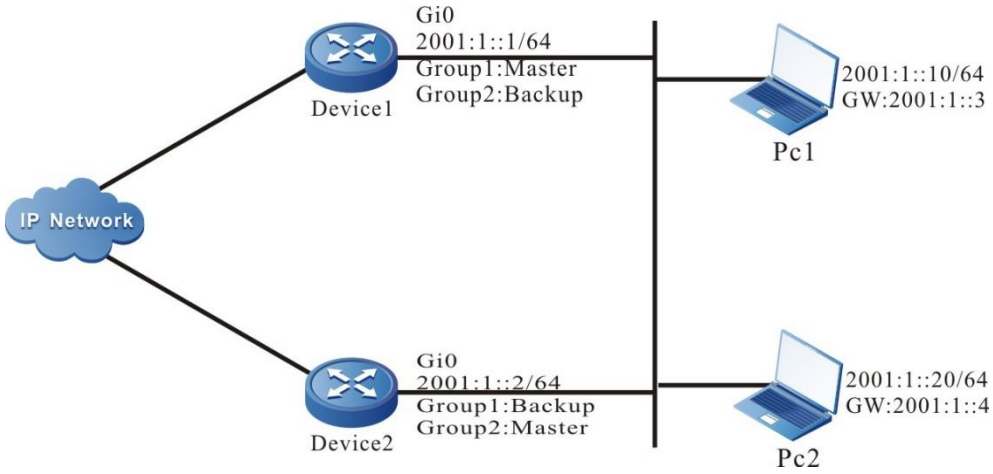

Figure 3-5 Networking of IPv6 VRRP load balance

Configuration Steps

Step 1: Configure the IPv6 address of the interface, and enable the switch of the RA response and RA periodical sending.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ipv6 address fe80::1 link-local
Device1(config-if-gigabitethernet0)#ipv6 address 2001:1::1/64
Device1(config-if-gigabitethernet0)#no ipv6 nd suppress-ra period
Device1(config-if-gigabitethernet0)#no ipv6 nd suppress-ra response
Device1(config-if-gigabitethernet0)#exit
Device2#configure terminal
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 address fe80::2 link-local
Device2(config-if-gigabitethernet0)#ipv6 address 2001:1::2/64
Device2(config-if-gigabitethernet0)#no ipv6 nd suppress-ra period
Device2(config-if-gigabitethernet0)#no ipv6 nd suppress-ra respons
Device2(config-if-gigabitethernet0)#exit
```

Step 2: Create IPv6 VRRP group 1.

#On Device1, configure VRRPv3 group 1, the virtual IP address is 2001:1::3 and fe80::100, and configure the priority as 110.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-gigabitethernet0)#ipv6 vrrp 1 priority 110
Device1(config-if-gigabitethernet0)#exit
```

#On Device1, configure VRRPv3 group 1, and the virtual IP address is 2001:1::3 and fe80::100.

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-gigabitethernet0)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-gigabitethernet0)#exit
```

Step 3: Create IPv6 VRRP group 2.

#On Device1, configure VRRPv3 group2, and the virtual IP address is 2001:1::4 and fe80::200.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ipv6 vrrp 2 ip fe80::200 link-local
Device1(config-if-gigabitethernet0)#ipv6 vrrp 2 ip 2001:1::4
Device1(config-if-gigabitethernet0)#exit
```

#On Device2, configure VRRPv3 group2, the virtual IP address is 2001:1::4 and fe80::200, and configure the priority as 110.

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#ipv6 vrrp 2 ip fe80::200 link-local
Device2(config-if-gigabitethernet0)#ipv6 vrrp 2 ip 2001:1::4
Device2(config-if-gigabitethernet0)#ipv6 vrrp 2 priority 110
Device2(config-if-gigabitethernet0)#exit
```

Step 4: Check the result.

#On Device1, view the status of the IPv6 VRRP group 1 and group 2.

```
Device1#show ipv6 vrrp
Interface gigabitethernet0 (Flags 0x9)
  Pri-addr : fe80::1
  Vrf : 0
  Pri-matchaddr : fe80::1
  Virtual router : 1
    Mac mode: real mac mode
    Virtual IP address : fe80::100
    Global address count:1
       Global Match address : 2001:1::1
          Global Virtual IP address : 2001:1::3
    Virtual MAC address : 00-00-5e-00-02-01
    State : Master
    Normal priority : 110
    Currnet priority : 110
    Priority reduced : 0
```

```
    Preempt-mode : YES
    Advertise-interval : 100
    Authentication Mode : None

  Pri-matchaddr : fe80::1
  Virtual router : 2
    Mac mode: real mac mode
    Virtual IP address : fe80::200
    Global address count:1
      Global Match address : 2001:1::1
        Global Virtual IP address : 2001:1::4
    Virtual MAC address : 00-00-5e-00-02-02
    State : Backup
    Master addr : fe80::2
    Normal priority : 100
    Currnet priority : 100
    Priority reduced : 0
    Preempt-mode : YES
    Advertise-interval : 100
    Authentication Mode : None
```

#On Device2, view the status of the IPv6 VRRP group 1 and group 2.

```
Device2#show ipv6 vrrp
Interface gigabitethernet0 (Flags 0x9)
  Pri-addr : fe80::2
  Vrf : 0
  Pri-matchaddr : fe80::2
  Virtual router : 1
    Mac mode: real mac mode
    Virtual IP address : fe80::100
    Global address count:1
      Global Match address : 2001:1::2
        Global Virtual IP address : 2001:1::3
    Virtual MAC address : 00-00-5e-00-02-01
    State : Backup
    Master addr : fe80::1
    Normal priority : 100
    Currnet priority : 100
```

```
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None

Pri-matchaddr : fe80::2
Virtual router : 2
  Mac mode: real mac mode
  Virtual IP address : fe80::200
  Global address count:1
     Global Match address : 2001:1::2
        Global Virtual IP address : 2001:1::4
  Virtual MAC address : 00-00-5e-00-02-02
  State : Master
  Normal priority : 110
  Currnet priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

You can see that Device1 serves as Master of VRRPv3 group 1 and becomes Backup of VRRPv3 group 2, while Device2 serves as Master of VRRPv3 group2 and Backup of VRRPv3 group 1. When one device fails, two PCs forward data via the other device. This not only takes effect of load balance, but also realizes the mutual backup.

4. VBRP

4.1. Overview

VBRP (Virtual Backup Router Protocol) provides one backup function for the gateway, used by multiple routers to maintain the continuous forwarding of the virtual gateway. VBRP maps the referred multiple routers to one virtual router and ensures that there is only one router to represent for the virtual router to forward packets. When the router for forwarding data cannot work normally because of some reason, another standby router replaces the virtual router to forward packets, while the router that cannot work normally does not bear the forwarding task any more. The switching process is short and it is transparent for the host in the LAN, so as to reach the backup function for the gateway.

The active device mentioned in the following text is replaced by “Active” and the standby device is replaced by “Standby”.

4.2. VBRP Function Configuration

Table 4-1 VBRP function configuration list

Configuration Task	
Configure the VBRP basic functions	Enable the VBRP protocol
	Enable the VBRP priority
	Enable the VBRP preemption mode
	Configure the VBRP virtual MAC address
Configure the VBRP network authentication	Configure the VBRP simple text authentication
	Configure the VBRP MD5 authentication
Configure VBRP to link with Track to associate with the uplink interface	Configure VBRP to link with Track to associate with the uplink interface

4.2.1. Configure VBRP Basic Functions

In the configuration tasks of VBRP, first enable the VBRP function and the virtual IP address of the VBRP group needs to be in the same segment as the interface IP address so that the configured other functions can take effect.

Configuration Condition

Before configuring the VBRP basic functions, first complete the following task:

- Configure the interface IP address

Enable VBRP Protocol

To enable the VBRP function, we need to create the VBRP group in the interface and add the VBRP router to the group.

Table 4-2 Enable the VBRP protocol

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the VBRP group	**standby** [*group-number*] **ip** [*ip-address*]	Mandatory Configure the router to add to the VBRP group. The default value of *group-number* is 0. *ip-address* is the virtual IP address.

Configure VBRP Priority

After configuring VBRP and if not setting the priority, the default priority is 100. The device with high priority is elected as Active for forwarding the packet and the other become Standby. If the priorities of all devices are equal, elect according to the interface IP address of the device. The one with large interface IP address becomes Active. We can set the VBRP priority as desired. The larger the value, the higher the priority.

Table 4-3 Configure the VBRP priority

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the priority of the VBRP group	**standby** [*group-number*] **priority** *value*	Mandatory Configure the VBRP priority. By default, the VBRP priority is 100.

Configure VBRP Preemption Mode

In the preemption mode, once other device in the VBRP group discovers that its priority is higher than that of the current Active, it becomes Active; in non-preemption mode, as long as Active does not fail, even the other device has higher priority, it cannot become Active.

Table 4-4 Configure the VBRP preemption mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the VBRP group as the preemption mode	**standby** [*group-number*] **preempt** [**delay** *delay-time*]	Mandatory Configure the VBRP preemption mode. By default, it is the non-preemption mode.

Configure VBRP Virtual MAC Address

After configuring VBRP and if it is necessary to make the VBRP group use the virtual MAC address, we need to use the following command to configure. When the virtual router replies the ARP request, the replied is virtual MAC address, but not the real MAC address of the interface. By default, the used is the real MAC address.

Table 4-5 Configure the VBRP virtual MAC

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure VBRP as the virtual MAC	**standby** [*group-number*] **use-vmac**	Mandatory By default, use the real MAC address.

Note:

- By default, after configuring VBRP, the used is the real MAC address. After configuring the command **standby use-vmac**, use the virtual MAC, that is, when the host sends the packet, forward by the virtual MAC address; after configuring the command **no standby**

use-vmac, use the real MAC address of the interface, that is, when the host sends the packet, use the real MAC address to forward.

4.2.2. Configure VBRP Network Authentication

VBRP has two modes, that is, simple text authentication and MD5 authentication. The set length of the simple text authentication cannot exceed eight authentication words. The set length of the MD5 authentication is the authentication word not exceeding 64 bits.

Configuration Condition

Before configuring the VBRP basic functions, first complete the following task:

- Configure the VBRP group

Configure VBRP Simple Text Authentication

Configure the VBRP authentication to check and verify the validity of the VBRP packet. We can use the following command to configure the VBRP simple text authentication mode.

Table 4-6 Configure the VBRP simple text authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the VBRP simple text authentication	**standby** *group-number* **authentication** { *string* }	Mandatory The configured authentication word is string and the length cannot exceed 8-bit authentication word. By default, do not enable the simple text authentication.

Configure VBRP MD5 Authentication

Configure the VBRP authentication to check and verify the validity of the VBRP packet. We can use the following command to configure the VBRP MD5 authentication mode.

Table 4-7 Configure the VBRP MD5 authentication

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the VBRP MD5 authentication	**standby** *group-number* **authentication** { **md5** { **key-id** *key-identifier* **key-string** *key-string* } **|** { **key-string** *key-string* } }	Mandatory Configure the MD5 network authentication and the length cannot exceed 8-bit authentication word. By default, do not enable the MD5 authentication.

4.2.3. Configure VBRP to Associate with Uplink Port via Track

Associate VBRP with the concerned uplink interface via Track. When the uplink interface is down, Active automatically reduces its own priority. Here, Standby receives the low-priority packet and switches to Active. For details, refer to the following figure.

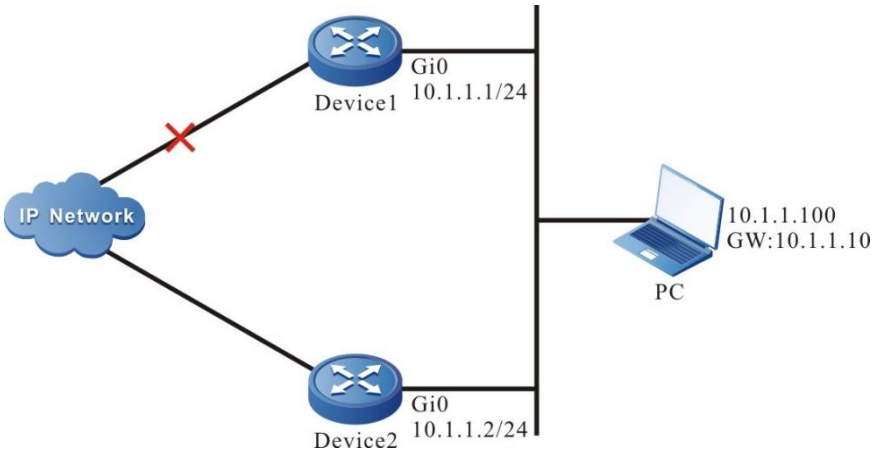

Figure 3–1 Configure VBRP to link with Track to monitor Active uplink line

Configuration Condition

Before configuring the VBRP basic functions, first complete the following task:

- Configure the VBRP group

Configure VBRP to Link with Track to Associate with Uplink Interface

Associate VBRP with the concerned uplink interface via Track. When the uplink interface is down, Active automatically reduces its own priority. Here, Standby receives the low-priority packet and switches to Active.

Table 4-8 Configure VBRP to link with Track to associate with the uplink interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure VBRP to link with Track to associate with the uplink interface	**standby** [*group-number*] **track** { { *interface-name*} | *track-id* } [*decrement*]	Mandatory Configure associating with the *interface-name* interface. When the interface is down, the priority reduces by decrement. By default, reduce the priority to 10.

Configure VBRP to Link with Track to Associate with BFD and RTR

If Track is associated with BFD, RTR and so on, Active can directly associate with the Track group, so as to monitor the line. When the line fails, Active reduces its own priority. Here, Standby receives the low-priority VBRP packet, switch to Active.

Table 4-9 Configure VBRP to link with Track to associate with BFD and RTR

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure VBRP to link with Track to associate with the uplink interface	**standby** [*group-number*] **track** { *track-id* } [*decrement*]	Mandatory Configure associating with Track *track-id.* The Track is associated with BFD, RTR and so on. By default, the priority is reduced by 10.

Note:

- For the configuration method of associating Track with BFD, RTR and so on, refer to Track Configuration Manual-the Track chapter.

4.2.4. VBRP Monitoring and Maintaining

Table 4-10 VBRP monitoring and maintaining

Command	Description
show standby [**all**] | [**interface** *interface-name*]	Display the VBRP configuration information, including virtual IP address information, virtual MAC address information, device status, device priority, dependent device interface address, link group information and so on.

4.3. VBRP Typical Configuration Example

4.3.1. Configure VBRP Basic Mode

Network Requirements

- Enable VBRP between Device1 and Device2; Device1 and Device2 share one virtual IP address, realizing the backup for the default gateway of the user host and reducing the network interruption time.

Network Topology

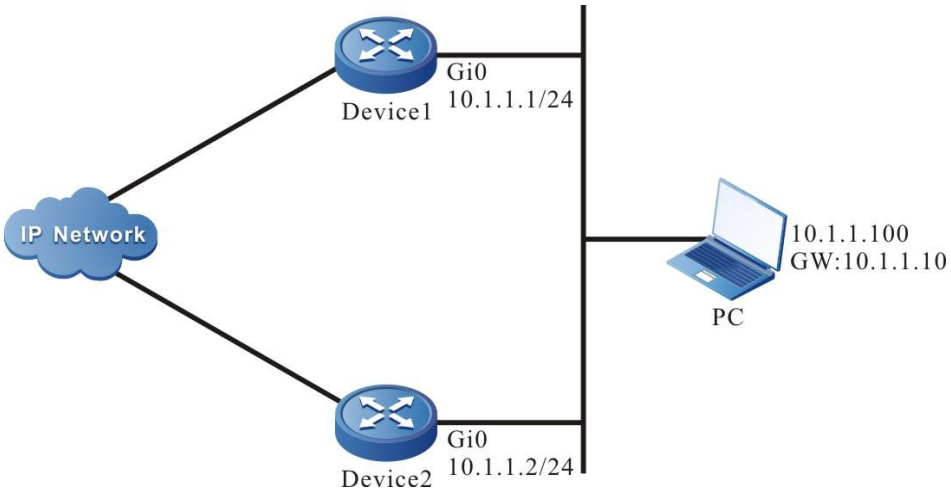

Figure 4-2 Networking of VBRP basic mode

Configuration Steps

Step 1: Configure the IP address of the interface.(Omitted)

Step 2: Create the VBRP group.

#Configure VBRP group 1 on Device1; the virtual IP address is 11.1.10; enable the preemption mode; configure the priority as 110.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#standby 1 ip 11.1.10
Device1(config-if-gigabitethernet0)#standby 1 preempt
```

```
Device1(config-if-gigabitethernet0)#standby 1 priority 110
```

#Configure VBRP group 1 on Device2; the virtual IP address is 11.1.10; enable the preemption mode;

```
Device2#configure terminal
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#standby 1 ip 11.1.10
Device2(config-if-gigabitethernet0)#standby 1 preempt
```

Step 3: Check the result.

#View the VBRP status of Device1.

```
Device1#show standby
Interface gigabitethernet0
  Primary address 11.1.1, state up
Group 1
  State is Active
  Virtual IP address is 11.1.10
  Refer to local IP prefix 11.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.666680 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 11.1.2, priority 100 (expires in 8.866672 secs)
  Priority 110 (configured 110)
```

```
#View the VBRP status of Device2.
Device2#show standby
Interface gigabitethernet0
  Primary address 11.1.2, state up
Group 1
  State is Standby
  Virtual IP address is 11.1.10
  Refer to local IP prefix 11.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.450022 secs
```

```
Preemption enabled, delay 0 sec
Active router is 11.1.1, priority 110 (expires in 7.266656 secs)
Standby router is local
Priority 100 (configured 100)
```

From the VBRP status, we can see that the VBRP priority of Device1 is 110, the status is Active, and the VBRP status of Device2 is Standby. After Device1 fails, Device2 automatically switches to Active for forwarding data.

Note:

- The election principle of the VRRP status is by priority. The one with large priority is Active. If the priorities are the same, compare according to the IP address of the interface. The one with large IP address is Active.
- By default, VBRP works in the non-preemption mode. The preemption mode needs to be configured manually. It is recommended to configure as the preemption mode.

The default priority of VBRP is 100.

4.3.2. Configure VBRP to Link with Track

Network Requirements

- Enable VBRP between Device1 and Device2.
- Device1 monitors the interface gigabitethernet1 status via Track. When the uplink port gigabitethernet1 of Device1 is down, VBRP can feel and switch the status, making Standby become new Active for forwarding data.

Network Topology

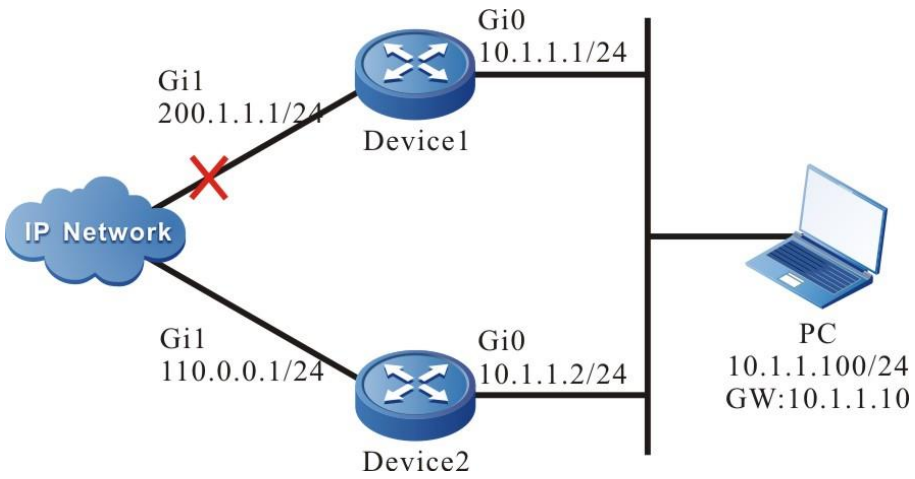

Figure 4-3 Networking of configuring VBRP to link with Track

Configuration Steps

Step 1: Configure the IP address of the interface.(Omitted)

Step 2: Create the VBRP group.

#Configure the virtual IP address of VBRP group 1 on Device1 as 11.1.10, enable the preemption function, and configure the priority as 110.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
```

```
Device1(config-if-gigabitethernet0)#standby 1 ip 11.1.10
Device1(config-if-gigabitethernet0)#standby 1 preempt
Device1(config-if-gigabitethernet0)#standby 1 priority 110
```

#Configure the virtual IP address of VBRP group1 on Device2 as 11.1.10 and enable the preemption function.

```
Device2#configure terminal
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#standby 1 ip 11.1.10
Device2(config-if-gigabitethernet0)#standby 1 preempt
```

#View the VBRP status of Device1.

```
Device1#show standby
Interface gigabitethernet0
  Primary address 11.1.1, state up
Group 1
  State is Active
  Virtual IP address is 11.1.10
  Refer to local IP prefix 11.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.933336 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 11.1.2, priority 100 (expires in 9.599976 secs)
  Priority 110 (configured 110)
```

#View the VBRP status of Device2.

```
Device2#show standby
Interface gigabitethernet0
  Primary address 11.1.2, state up
Group 1
  State is Standby
  Virtual IP address is 11.1.10
  Refer to local IP prefix 11.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
```

```
Current MAC type BIA
Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.216658 secs
Preemption enabled, delay 0 sec
Active router is 11.1.1, priority 110 (expires in 7.550018 secs)
Standby router is local
Priority 100 (configured 100)
```

Step 3: Configure VBRP to link with Track.

#On Device1, configure VBRP to link with Track, monitor the uplink interface gigabitethernet1, and configure the priority decrement as 20.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#standby 1 track gigabitethernet1 20
```

#View the VBRP status of Device1.

```
Device1#show standby
Interface gigabitethernet0
  Primary address 11.1.1, state up
Group 1
  State is Active
  Virtual IP address is 11.1.10
  Refer to local IP prefix 11.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.716678 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 11.1.2, priority 100 (expires in 8.166660 secs)
  Priority 110 (configured 110)
    Track interface gigabitethernet1 state Up decrement 20
```

#When the uplink port gigabitethernet1 of Device1 is down, the VBRP priority is reduced by 20. Here, the priority of Device2 is high, so the status switches.

#View the VBRP status of Device1.

```
Device1#show standby
Interface gigabitethernet0
  Primary address 11.1.1, state up
```

```
Group 1
  State is Standby
  Virtual IP address is 11.1.10
  Refer to local IP prefix 11.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.49998 secs
  Preemption enabled, delay 0 sec
  Active router is 11.1.2, priority 100 (expires in 8.233324 secs)
  Standby router is local
  Priority 90 (configured 110)
    Track interface gigabitethernet1 state Down decrement 20
```

#View the VBRP status on Device2.

```
Device2#show standby
Interface gigabitethernet0
  Primary address 11.1.2, state up
Group 1
  State is Active
  Virtual IP address is 11.1.10
  Refer to local IP prefix 11.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.699972 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 11.1.1, priority 90 (expires in 8.516646 secs)
  Priority 100 (configured 100)
```

4.3.3. Configure VBRP Load Balance Mode

Network Requirements

- Device1 and Device2 belong to two VBRP groups at the same time; Device1 is Active in group1 and Standby in group2; Device2 is Standby in group1 and Active in group2.
- PC1 forwards data via Device1 and PC2 forwards data via Device2, realizing the load balance.

Network Topology

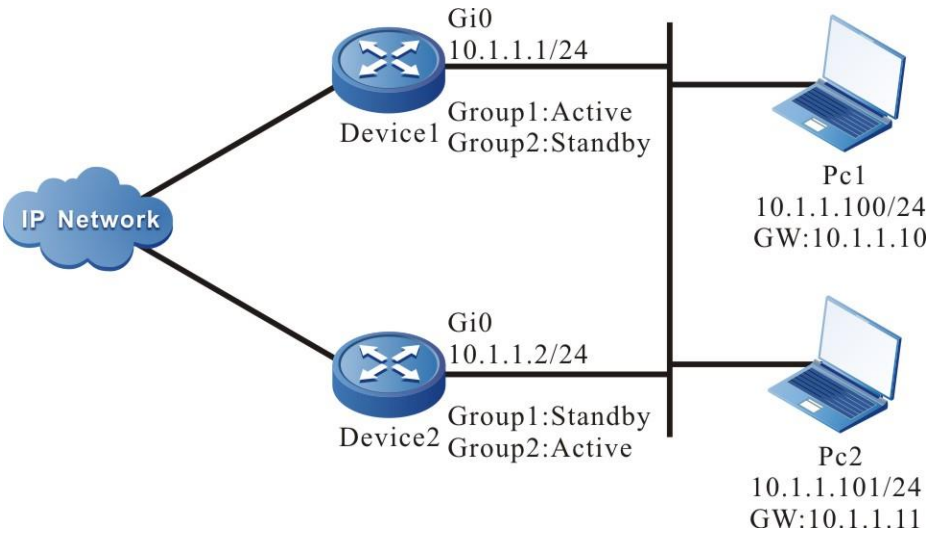

Figure 4-4 Networking of VBRP load balance

Configuration Steps

Step 1: Configure the IP address of the interface.(Omitted)

Step 2: Create VBRP group1.

#Configure the virtual IP address of VBRP group 1 on Device1 as 11.1.10, enable the preemption function, and configure the priority as 110.

```
Device1#configure terminal
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#standby 1 ip 11.1.10
Device1(config-if-gigabitethernet0)#standby 1 preempt
Device1(config-if-gigabitethernet0)#standby 1 priority 110
```

#Configure the virtual IP address of VBRP group1 on Device2 as 11.1.10 and enable the preemption function.

```
Device2#configure terminal
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#standby 1 ip 11.1.10
Device2(config-if-gigabitethernet0)#standby 1 preempt
```

Step 3: Create VBRP group2.

#Configure the virtual IP address of VBRP group 2 on Device1 as 11.1.11, and enable the preemption function.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#standby 2 ip 11.1.11
```

```
Device1(config-if-gigabitethernet0)#standby 2 preempt
```

#Configure the virtual IP address of VBRP group 1 on Device2 as 11.1.11, enable the preemption function, and configure the priority as 120.

```
Device2(config)#interface gigabitethernet0
Device2(config-if-gigabitethernet0)#standby 2 ip 11.1.11
Device2(config-if-gigabitethernet0)#standby 2 preempt
Device2(config-if-gigabitethernet0)#standby 2 priority 120
```

Step 4: Check the result.

#View the status of VBRP in group 1 and group 2 on Device1.

```
Device1#show standby
Interface gigabitethernet0
  Primary address 11.1.1, state up
Group 1
  State is Active
  Virtual IP address is 11.1.10
  Refer to local IP prefix 11.1.1/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.633348 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 11.1.2, priority 100 (expires in 7.83370 secs)
  Priority 110 (configured 110)
Group 2
  State is Standby
  Virtual IP address is 11.1.11
  Refer to local IP prefix 11.1.1/24
  Local virtual MAC address is 0000.0c07.ac02
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.950002 secs
  Preemption enabled, delay 0 sec
  Active router is 11.1.2, priority 120 (expires in 7.300028 secs)
  Standby router is local
Priority 100 (configured 100)
```

#View the status of VBRP in group 1 and group 2 on Device2.

```
Device2#show standby
Interface gigabitethernet0
  Primary address 11.1.2, state up
Group 1
  State is Standby
  Virtual IP address is 11.1.10
  Refer to local IP prefix 11.1.2/24
  Local virtual MAC address is 0000.0c07.ac01
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.600016 secs
  Preemption enabled, delay 0 sec
  Active router is 11.1.1, priority 110 (expires in 7.700012 secs)
  Standby router is local
  Priority 100 (configured 100)
Group 2
  State is Active
  Virtual IP address is 11.1.11
  Refer to local IP prefix 11.1.2/24
  Local virtual MAC address is 0000.0c07.ac02
  Current MAC type BIA
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.816674 secs
  Preemption enabled, delay 0 sec
  Active router is local
  Standby router is 11.1.1, priority 100 (expires in 8.33332 secs)
  Priority 120 (configured 120)
```

We can see that Device1 serves as Active of VBRP group1 and Standby of VBRP group2. In contrast with Device1, Device2 serves as Active of VBRP group 2 and Standby of VBRP group 1. When one device fails, two PCs forward data via the other device. This realizes the load balance and backup for each other.

5. VRRP LOAD-BALANCE PROTOCOL

5.1. Overview

VRRP load-balance protocol (Load-Balance Virtual Router Redundancy Protocol) supports the clients configured with the same gateway to be loaded dynamically under the condition of multiple gateway exports in LAN. Meanwhile, it takes into account the redundancy backup feature.

The main devices mentioned below are replaced by "Master" and the backup devices are replaced by "Backup".

5.2. VRRP Load-balance Protocol Function Configuration

Table 5-1 VRRP load-balance protocol function configuration list

Configuration tasks	
Configure the VRRP current mode	Enable the VRRP load balance mode
Configure the basic functions of the VRRP load balance protocol	Enable the VRRP load balance protocol
	Configure the priority of the VRRP load balance protocol
	Configure the virtual MAC address of the VRRP load balance protocol
Configure the timer of the VRRP load balance protocol	Configure the period interval of the Hello packet
	Configure the period interval of the Keep packet
	Configure the zombie timer of the virtual mac address
	Configure the age timer of the forwarding terminal
	Configure the detection timer of the forwarding terminal

5.2.1. Configure the Current Mode of the VRRP Load-balance Protocol

In the configuration tasks of VRRP load balancing protocol, the VRRP load balancing protocol mode must be enabled, which is mutually exclusive with the VRRP standard protocol.

Configuration Conditions

None

Enable VRRP Load-Balance Protocol Mode

Table 5-2 Enable the VRRP load-balance protocol mode

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Global configuration mode	**vrrp mode load-balance**	Mandatory

5.2.2. Configure the Basic Functions of VRRP Load-Balance Protocol

In the configuration tasks of the VRRP load-balance protocol, the VRRP load-balance protocol must be enabled first, and the virtual IP address of the VRRP load-balance protocol group needs to be in the same network segment as the IP address of the interface, so the other configured functions can take effect.

Configuration Conditions

Before configuring the VRRP basic functions, first complete the following tasks:

- Configure the IP address of the interface

Enable the VRRP Load-Balance Protocol

To enable the VRRP load-balance protocol function, it is necessary to create one VRRP load-balance protocol group in the interface and configure the virtual IP address.

Table 5-3 Enable the VRRP protocol

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the VRRP load-balance protocol group	**vrrp** *vrid* **ip** *ip-address*	Mandatory Enable the VRRP load-balance protocol. Here, vrid is the VRRP load-balance protocol group number, and ip-address is the virtual IP address.

Note:

- In the VRRP load-balance protocol mode, you cannot configure the virtual IP to be the same as the interface IP.

Configure the VRRP Load Balancing Protocol Priority

If the priority is not configured after configuring VRRP load balancing protocol, its default priority is 100; the device with high priority will be elected as Master responsible for forwarding packets, and the others will be Backup; if the priorities of all devices are equal, elect according to the interface IP address of each device, and the interface with the large IP address will be Master; you can set the priority of the VRRP load-balance protocol according to the need. The larger the priority value is, the higher the priority is.

Table 5-4 Configure the priority of the VRRP load-balance protocol group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the priority of the VRRP load-balance protocol group	**vrrp** *vrid* **priority** *priority*	Mandatory By default, the priority is 100.

Configure Simple Text Authentication of VRPP Load Balancing Protocol

After configuring VRRP load balancing protocol, if simple text authentication is not set, the simple text authentication function is not enabled by default; only when the authentication in VRRP load balancing protocol group is consistent can the neighbor be established successfully.

Table 5-5 Configure the simple text authentication of the VRRP load balancing protocol

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory

Step	Command	Description
Configure the simple text authentication of the VRRP load balancing protocol	**vrrp** *vrid* **authentication text** *string*	Mandatory By default, do not enable the simple text authentication function. The authentication password is 8 characters at most.

Configure the Virtual MAC Address of the VRRP Load-balance Protocol

Each virtual router in a VRRP load balancing protocol group has a virtual MAC address. According to the regulations of the VRRP load balancing protocol, the format of the virtual MAC address is 00.01.7a.00. {vrid}. {mid}, and the mid value is assigned by the master. When a virtual router responds to an ARP request, the returned is the virtual MAC address, not the real MAC address of the interface. By default, the real MAC address of the interface is used.

Table 5-6 Configure the virtual MAC address of the VRRP load-balance protocol

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the VRRP load-balance protocol to use the virtual MAC address	**vrrp** *vrid* **use-vmac**	Mandatory By default, use the real MAC address.

Note:

- By default, adopt the real MAC address on the corresponding interface after configuring VRRP. After configuring the command of this section, use the virtual MAC, that is, the host forwards the packet by the virtual MAC address; after deleting the command of this section, use the real MAC address of the corresponding interface, that is, the host sends the packet by the real MAC address.

5.2.3. Configure the Timer of the VRRP Load-Balance Protocol

In the VRRP load-balance protocol, perform the corresponding actions according to the corresponding timer, so as to maintain the relevant state.

Configuration Conditions

Before configuring the timer of the VRRP load-balance protocol, first complete the following tasks:

- Switch the VRRP mode to the VRRP load-balance protocol mode

- Enable the VRRP load-balance protocol group

Configure the Period Interval of the Hello Packet

The Hello packet is mainly responsible for announcing some information to the neighbors and maintaining the relationship between neighbors, so it is necessary to keep the sending periods of the Hello packets consistent among neighbors in the same group.

Table 5-7 Configure the period interval of the Hello packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the period interval of the Hello packet of the VRRP load-balance protocol group	**vrrp** *vrid* **timers hello** *Hello–time* [**hold** *Hold–time* [**preserved** *Preserved–time* [**delay-vote** *Delay-vote–time*]]]	Mandatory Configure the period interval of the Hello packet. Here, vrid is the VRRP group number; Hello–time specifies the sending period of the Hello packet of the VRRP group; Hold–time specifies the hold time of the VRRP group neighbor; Preserved–time specifies the reserve time of the virtual MAC of the VRRP group; Delay-vote–time specifies the delay election time of the VRRP group.

Configure the Period Interval of the Keep Packet

The Keep packet is responsible for advertising the virtual MAC address of the virtual router to the L2 switch, and refreshing the L2 MAC entries of the switch.

Table 5-8 Configure the period interval of the Keep packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the period interval of the Keep packet of the VRRP load-balance protocol group	**vrrp** *vrid* **timers keep** *keep-time*	Mandatory Configure the period interval of the Keep packet. Here, vrid is the VRRP group number; Keep-time specifies the period of sending the Keep packet of the VRRP load-balance protocol group.

Configure the Zombie Timer of the Virtual MAC Address

After the owner of the virtual MAC fails, the virtual MAC will experience the reserved state, and reach the zombie state. The configuration of the zombie state needs the timer larger than the age time of the bottom terminal ARP.

Table 5-9 Configure the zombie timer of the virtual MAC address

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the zombie time of the virtual MAC address of the VRRP load-balance protocol group	**vrrp** *vrid* **timers zombie** *zombie-time*	Mandatory Configure the zombie timer of the virtual MAC address. Here, vrid is the VRRP load-balance protocol group number, and Zombie-time specifies the zombie time of the virtual MAC of the VRRP load-balance protocol group.

Configure the Age Timer of the Forwarding Terminal

If the terminal is not online for a long time when managing the terminal at the forwarding layer, it will be aged to release the resources occupied by the terminal, thereby refreshing the terminal table items of the group.

Table 5-10 Configure the age timer of the terminal at the forwarding layer

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory
Configure the age timer of the forwarding terminal of the VRRP load-balance protocol group	**vrrp** *vrid* **timers forwarding ageing** *forwarding-ageing-time*	Mandatory Configure the age time of the terminal at the forwarding layer. Here, vrid is the VRRP group number, and forwarding-ageing-time specifies the age time of the terminal at the forwarding layer in the VRRP group.

Configure the Detection Timer of the Terminal at the Forwarding Layer

When managing the terminal at the forwarding layer, detect the online state of the terminal regularly, so as to update the state of the terminal at the local.

Table 5-11 Configure the detection timer of the terminal at the forwarding layer

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	Mandatory

Step	Command	Description
Configure the detection timer of the terminal at the forwarding layer in the VRRP load-balance protocol group	**vrrp** *vrid* **timers forwarding dtct** *forwarding-dtct-time*	Mandatory Configure the detection timer of the terminal at the forwarding layer. Here, vrid is the VRRP load-balance protocol group number, and forwarding-dtct-time specifies the detection time of the terminal at the forwarding layer in the VRRP load-balance protocol group.

5.2.4. Monitoring and Maintaining of VRRP Load-balance Protocol

Table 5-12 VRRP monitoring and maintaining

Command	Description
Show vrrp [interface *interface-name*]	Display the VRRP load-balance protocol configuration information, including virtual IP address information, virtual MAC address information, device status, device priority, dependent device interface address, linkage group information, etc.

5.3. VRRP Load-balance Typical Configuration Example

5.3.1. Configure the Basic Functions of the VRRP Load-balance Protocol

Network Requirements

- On Device1 and Device2, create one VRRP load-balance backup group, making Device1 and Device2 share one virtual IP address and realizing the backup for the default gateway of the user host, so as to reduce the interruption time of the network.
- The VRRP load-balance protocol realizes the load function by distributing the traffic from different user hosts to different VRRP devices in a group. The significant difference from the common VRRP is that backup devices in the VRRP load-balance protocol can also forward the traffic, which enables users to configure the same gateway address for all hosts in the network to achieve load balancing.

Network Topology

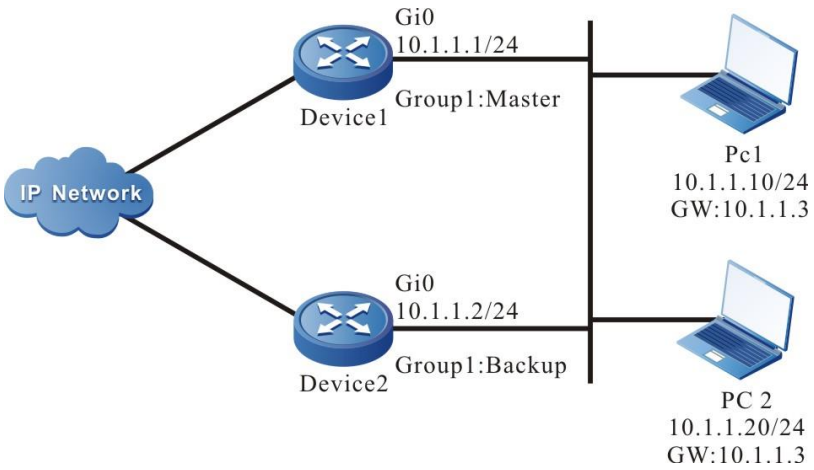

Figure 5-1 Networking of configuring the basic functions of the VRRP load-balance protocol

Configuration Steps

Step 1: Configure the IPv4 address of the interface (omitted).

Step 2: Configure the device as the VRRP load-balance protocol mode.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#vrrp mode load-balance
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#vrrp mode load-balance
```

#Query the VRRP protocol mode of Device1.

```
Device1#show vrrp-pub mode

Current mode:load_balance
Current switch:0
```

#Query the VRRP protocol mode of Device2.

```
Device2#show vrrp-pub mode

Current mode:load_balance
Current switch:0
```

You can see that both Device1 and Device2 run in the VRRP load-balance protocol mode.

Step 3: Create one VRRP load-balance protocol backup group.

#On Device1, create backup group 1. The virtual IP address is 11.1.3, and configure the priority as 110.

```
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device1(config-if-gigabitethernet0)#vrrp 1 priority 110
Device1(config-if-gigabitethernet0)#exit
```

#On Device2, create backup group 1, and the virtual IP address is 11.1.3

```
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#vrrp 1 ip 11.1.3
Device2(config-if-gigabitethernet0)#exit
```

Step 4: Query the status of the VRRP load-balance protocol.

#Query the VRRP load-balance protocol neighbor table of Device1.

```
Device1#show vrrp neighbor

Gid  Neighbor  Priority  Uid     Virtual-ip  Master   Hold-time  Interface
1    11.1.2    100       412780  11.1.3      11.1.1   36         gigabitethernet0
```

From the Neighbor field, you can see that Device1 successfully sets up the neighbor with Device2.

#Query the VRRP load-balance protocol neighbor table of Device2.

```
Device2#show vrrp neighbor

Gid  Neighbor  Priority  Uid     Virtual-ip  Master   Hold-time  Interface
1    11.1.1    110       348619  11.1.3      11.1.1   33         gigabitethernet0
```

From the Neighbor field, you can see that Device2 also sets up the neighbor with Device1 successfully.

#Query the VRRP load-balance protocol status of Device1.

```
Device1#show vrrp
Interface gigabitethernet0
  Vrf:0
  Virtual router : 1
    Mac mode: real mac mode
    Forwording mac :
      00.01.7a.7c.72.26
    Virtual IP address : 11.1.3
    Match address : 11.1.1
    State : Master
    Priority : 110
    Hello interval(sec) :  10
      next hello in 3 secs
```

```
    Hold time(sec) :      40
    Delay vote time(sec) : 40
    Delay delete time(sec) : 20
    Preserve time(sec) :   40
    Keep(min) : 15
    Zombie(min) : 10
    Uid : 348619
    Terminal number : 0/1000
```

From the State field, you can see that Device1 is elected as Master.

#Query the VRRP load-balance protocol status of Device2.

```
Device2#show vrrp
Interface gigabitethernet0
  Vrf:0
  Virtual router : 1
    Mac mode: real mac mode
    Forwording mac :
      00.01.7a.ff.ff.00
    Virtual IP address : 11.1.3
    Match address : 11.1.2
    State : Backup
    master:11.1.1
    Priority : 100
    Hello interval(sec) :  10
      next hello in 6 secs
    Hold time(sec) :      40
    Delay vote time(sec) : 40
    Delay delete time(sec) : 20
    Preserve time(sec) :   40
    Keep(min) : 15
    Zombie(min) : 10
    Uid : 412780
    Terminal number : 0
```

From the State field, you can see that Device2 becomes Backup.

#On Device1, query the VRRP load-balance protocol forwarding the MAC address distributing table.

```
Device1# show vrrp fmac
```

```
Gid  Virtual-ip  Forwarding-mac   Owner     Backup   Owner-state  Timeout  Interface
1    11.1.3     001f.ce7c.7226   11.1.1    -        Active       -        gigabitethernet0
1    11.1.3     001f.ceff.ff00   11.1.2    -        Active       -        gigabitethernet0
```

Only Master has the function of distributing the forwarding MAC address. From the corresponding relationship between Owner and Forwarding-mac, it can be seen that the forwarding MAC address allocated for 11.1.1 is 001f.ce7c.7226, and the forwarding MAC address allocated for 11.1.2 is 001f.ceff.ff00.

Note:

- VRRP load balancing protocol can only work in non-preempt mode.
- VRRP load balancing protocol starts the delay election timer in the init state, and by default, it is four times of the Hello interval. Elect after timeout.
- VRRP load balancing protocol elects according to the priority. The one with the highest priority is elected as Master If the priorities are the same, compare the IP addresses of the interfaces. The one with largest IP address is elected as Master, and the others are Backup.

Step 5: Check the result.

#On PC1 and PC2, ping the gateway to test the connectivity. On Device1, query the gateway forwarding MAC address distributed by Master for the host.

```
Device1#show vrrp terminal

Gid  Virtual-ip  Terminal     Forwarding-mac   Interface

1    11.1.3      11.1.10      001f.ce7c.7226   gigabitethernet0
1    11.1.3      11.1.20      001f.ceff.ff00   gigabitethernet0
```

As shown in the table above, the host terminals PC1 and PC2 are assigned with different gateway forwarding MAC addresses. Combined with the forwarding MAC addresses allocated by Master for Device 1 and Device 2 in Step 4, it can be seen that the traffic of PC1 and PC2 is forwarded by Device 1 and Device 2 respectively to achieve load balancing.

#On Device2, query the forwarding MAC address distributing table of the Backup terminal gateway.

```
Device2#show vrrp terminal

Gid  Virtual-ip  Terminal     Forwarding-mac   Interface
1    11.1.3      11.1.10      001f.ce7c.7226   gigabitethernet0
1    11.1.3      11.1.20      001f.ceff.ff00   gigabitethernet0
```

Master synchronizes the forwarding MAC address distributing table of the terminal gateway to all VRRP devices.

5.3.2. Configure VRRP Load Balancing Protocol Authentication Function

Network Requirement

- Create a VRRP load balancing group on Device1 and Device2. The backup group can be established only after passing the authentication to realize the load function.

Network Topology

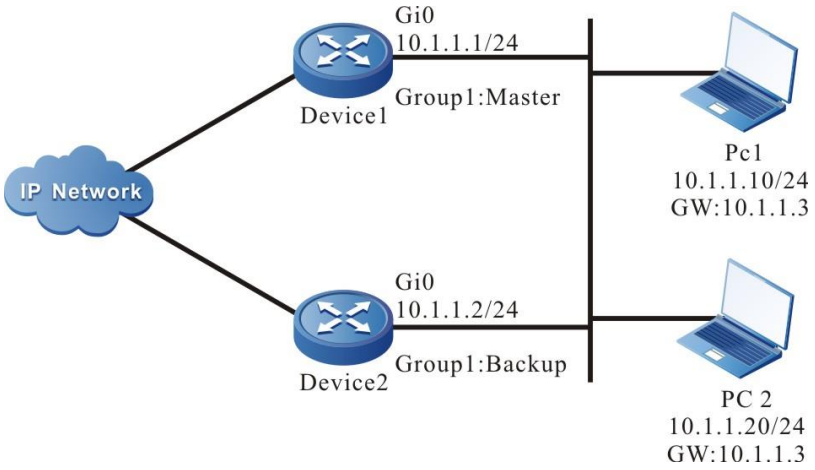

Figure 5-2 Networking of configuring the authentication function of VRRP load balancing protocol

Configuration Steps

Step 1: Configure the IPv4 address of the interface (omitted).

Step 2: Configure the device as the VRRP load-balance protocol mode.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#vrrp mode load-balance
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#vrrp mode load-balance
```

#View the VRRP protocol mode of Device1.

```
Device1#show vrrp-pub mode
Current mode:load_balance
Current switch:0
```

#View the VRRP protocol mode of Device2.

```
Device2#show vrrp-pub mode
Current mode:load_balance
Current switch:0
```

You can see that Device1 and Device2 both run in the VRRP load balancing protocol mode.

Step 3: Create the backup group of the VRRP load balancing protocol.

#On Device1, create backup group 1, virtual IP address is 10.1.1.3, and configure the priority as 110.

```
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#vrrp 1 ip 10.1.1.3
Device1(config-if-gigabitethernet0)#vrrp 1 priority 110
Device1(config-if-gigabitethernet0)# vrrp 1 authentication text 123456
Device1(config-if-gigabitethernet0)#exit
```

#On Device2, create backup group 1, and virtual IP address is 10.1.1.3.

```
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#vrrp 1 ip 10.1.1.3
Device1(config-if-gigabitethernet0)# vrrp 1 authentication text 123456
Device2(config-if-gigabitethernet0)#exit
```

Step 4: View the status of the VRRP load balancing protocol.

#View the neighbor table of the VRRP load balancing protocol on Device1.

```
Device1#show vrrp neighbor
 Gid  Neighbor  Priority  Uid     Virtual-ip  Master    Hold-time  Interface
 1    10.1.1.2  100       412780  10.1.1.3    10.1.1.1  36         gigabitethernet0
```

It can be seen from the neighbor field that Device1 has successfully established the neighbor with Device2.

#View the VRRP load balancing protocol neighbor table of Device2.

```
Device2#show vrrp neighbor
 Gid  Neighbor  Priority  Uid     Virtual-ip  Master    Hold-time  Interface
 1    10.1.1.1  110       348619  10.1.1.3    10.1.1.1  33         gigabitethernet0
```

It can be seen from the neighbor field that Device2 has successfully established the neighbor with Device1.

#View the VRRP load balancing protocol neighbor table of Device1.

```
Device1#show vrrp
Interface gigabitethernet0
  Vrf:0
  Virtual router : 1
    Mac mode: real mac mode
    Forwording mac :
      00.01.7a.7c.72.26
    Virtual IP address : 10.1.1.3
    Match address : 10.1.1.1
```

```
State : Master
Priority : 110
Hello interval(sec) :  10
   next hello in 3 secs
Hold time(sec) :      40
Delay vote time(sec) : 40
Delay delete time(sec) : 20
Preserve time(sec) :   40
Keep(min) : 15
Zombie(min) : 10
Uid : 348619
Terminal number : 0/1000
Authentication mode : Simple text
```

From the state field, you can see that Device1 is elected as master.

#View the VRRP load balancing protocol status of Device2.

```
Device2#show vrrp
Interface gigabitethernet0
  Vrf:0
  Virtual router : 1
    Mac mode: real mac mode
    Forwording mac :
      00.01.7a.ff.ff.00
    Virtual IP address : 10.1.1.3
    Match address : 10.1.1.2
    State : Backup
    master:10.1.1.1
    Priority : 100
    Hello interval(sec) :  10
      next hello in 6 secs
    Hold time(sec) :      40
    Delay vote time(sec) : 40
    Delay delete time(sec) : 20
    Preserve time(sec) :   40
    Keep(min) : 15
    Zombie(min) : 10
    Uid : 412780
    Terminal number : 0
```

Authentication mode : Simple text

From the State field, you can see that Device2 becomes Backup.

Note:

- VRRP load balancing protocol authentication can only be negotiated correctly if the configuration is the same.

6. TRACK

6.1. Overview

Track can be used to monitor some information when the system runs. The other service modules can be associated with Track so that the service module can monitor the change when the system runs. After the service module is associated with Track and when the information monitored by Track changes, Track informs the service module so that the service module can process correspondingly. For example, in the actual application, VRRP and VBRP often monitor the uplink interface status and network availability by associating with Track and adjust its own priority according to the information, so as to realize the active/standby switchover.

6.2. Track Function Configuration

Table 6-1 Track function configuration list

Configuration Task	
Configure the Track group	Configure the Track group
Configure the monitor object	Configure the monitor interface status
	Configure monitoring the direct route of the interface
	Configure monitoring route reachable
	Configure monitoring the RTR group
	Configure monitoring the BFD session

6.2.1. Configure Track Group

Configuration Condition

None

Configure Track Group

The system can configure multiple Track groups. Each Track group is independent from each other. One Track group can include multiple monitor objects.

The Track group has two logics, that is, “and”, “or”:

- When the Track group logic is “and”, all monitor objects in Track group need to be up so that the Track group can be up; on contrast, it is down.
- When the Track group logic is “or”, as long as one monitor object in Track group is up, the Track object status can be up; on contrast, it is down.

Table 6-2 Configure the Track group

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create the Track group	**track** *group-id*	Mandatory
Configure Track group logic	**logic { operator [AND | OR] | reverse }**	Optional **AND**: logic “and” **OR**: logic “or” **reverse**: logic reverse By default, Track group logic is “and”; the logic reverse function does not take effect.

Note:

- When the service module needs to monitor some information via Track, besides configuring the monitor object in the Track group, we also need to refer to the service module configuration manual and configure the service module to associate with Track group.

6.2.2. Configure Monitor Object

Configuration Condition

Before configuring the monitor object, first complete the following task:

- Configure the Track group

Configure Monitoring Interface Status

We can configure the monitor object as the interface status in the Track group. When the interface network layer protocol is up, the monitor object status is up; when the interface network layer protocol is down, the monitor object status is down.

Table 6-3 Configure monitoring interface status

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	-

Step	Command	Description
Configure monitoring interface status	**interface** *interface-name* **line-protocol**	Mandatory

Configure Monitoring Direct Route of Interface

We can configure the monitor object as the direct route of the interface in the Track group. When the interface has IP address and the status is up, the status of the monitor object is up; when the interface does not have IP address or the status is down, the status of the monitor object is down.

Table 6-4 Configure monitoring the direct route of the interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	-
Configure monitoring the direct route of the interface	**interface** *interface-name* **ip-routing** **interface** *interface-name* **ipv6-routing**	Mandatory

Configure Monitoring Interface Bandwidth Utilization Alarm

In the track group, the monitoring object can be configured as the bandwidth utilization alarm in the input or output direction of the interface. When the inbound traffic of the interface is higher than the inbound bandwidth utilization alarm threshold set by the interface, the status of the monitoring object is up; When the inbound traffic of the interface is lower than the inbound bandwidth utilization alarm threshold set by the interface, the status of the monitoring object is down; When the outbound traffic of the interface is higher than the outbound bandwidth utilization alarm threshold set by the interface, the status of the monitoring object is up; When the outbound traffic of the interface is lower than the outbound bandwidth utilization alarm threshold set by the interface, the status of the monitoring object is down.

Table 6-5 Configure monitoring interface bandwidth utilization alarm

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	-
Configure the direct route of the monitoring interface	**interface** *interface-name* **trap-threshold input** **interface** *interface-name* **trap-threshold output**	Mandatory

Configure Monitoring Route Reachable

We can configure the monitor object as the route reachable in the Track group. When there is the route of the configured network, the status of the monitor object is up; when there is no route of the configured network, the status of the monitor object is down.

Table 6-6 Configure monitoring route reachable

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track group-id	-
Configure monitoring route reachable	ip-route network mask [vrf vrf-name] [metric metric-value] ipv6-route network mask [vrf vrf-name] [metric metric-value]	Mandatory When there is the option metric, the route metric to the network needs to be smaller than the configured value so that the status of the monitor object can be up.

Configure Monitoring RTR Group

We can configure the monitor object as the RTR group in the Track group. When the status of the RTR group is reachable, the status of the monitor object is up; when the status of the RTR group is unreachable, the status of the monitor object is down. RTR (Response Time Reporter) is one tool of detecting and monitoring the network. Track can monitor the RTR group to monitor the network communication.

Table 6-7 Configure monitoring the RTR group

Step	Command	Description
Enter the global configuration mode	configure terminal	-
Enter the Track configuration mode	track group-id	-
Configure monitoring the RTR group	rtr rtr-group-id	Mandatory

Note:

- For the configuration of the RTR group, refer to SLA configuration manual.

Configure Monitoring BSM Instance

The configurable monitoring objects in the track group are the slight, normal and severe deterioration of BSM instances. When the BSM instance degradation level is lower than the monitored degradation level, the monitoring object status is up; When the BSM instance degradation is higher than the monitored degradation level, the monitoring object status is down. BSM (business sensitivity measure) calculates the packet loss rate, delay, jitter and other performance indicators of the line by marking and measuring the line packet, so as to analyze the quality of the line. Track can indirectly monitor the network communication by monitoring the slight, normal and serious deterioration of BSM instances.

Table 6-8 Configure monitoring the BSM instance

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	-
Configure monitoring BSM instance	**bsm** *bsm-entity-id* **deteriorate-degree [mild | normal | severe]**	Mandatory

Note:

- For the related configuration of BSM instance, refer to the BSM configuration manual.

Configure Monitoring BFD Session

We can configure the monitor object as the BFD session in the Track group. When the status of the BFD session is up, the status of the monitor object is up; when the status of the BFD session is down, the status of the monitor object is down. The BFD protocol is one set of standard unified

detection mechanism, used to fast detect, monitor the path in the network or the connection status of the IP route forwarding. The network connection status can be monitored indirectly by monitoring the BFD session.

Table 6-9 Configure monitoring the BFD session

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Track configuration mode	**track** *group-id*	-
Configure monitoring the BFD session	**bfd interface** *interface-name* **remote-ip** *ip-address* **local-ip** *ip-address* **bfd interface** *interface-name* **remote-ipv6** *ipv6-address* **local-ipv6** *ipv6-address* **bfd multihop control remote-ip** *ip-address* **local-ip** *ip-address* **bfd multihop echo interface** *interface-name* **remote-ip** *ip-address*	Mandatory When configuring monitoring the BFD session, it needs to be configured at the two sides of the BFD session. Otherwise, the BFD session cannot be set up successfully.

6.2.3. Track Monitoring and Maintaining

Table 6-10 Track monitoring and maintaining

Command	Description
show track object *group-id*	Display the Track group information.
show track bfd-session	Display the BFD session information of the Track monitoring.
show track route-request	Display the route information monitored by Track

7. BFD

7.1. Overview

The BFD (Bidirectional Forwarding Detection) protocol is a set of standard and unified detection mechanism, used to detect and monitor the path in the network or IP route forwarding connection status fast. It provides one universal, standard, medium-independent, and protocol-independent fast fault detection mechanism. It can fast detect the line fault between two devices for the upper-layer protocols, such as routing protocol and MPLS.

BFD can provide the fault detection on any type of path between the systems. One BFD session is set up based on the specific application demand. If multiple application protocols correspond to the same path, you can use one BFD session to detect.

The processing flow of the BFD protocol and the upper application protocol includes:

The upper application protocol sends the neighbor information (including peer IP address, local IP address, interface and so on) to the BFD protocol.

The BFD protocol queries whether there is the corresponding session. If no, create the corresponding session according to the received neighbor information and then the BFD session sends the BFD control packet to drive the running of the status machine. The BFD control packet completes the session via three times handshake mechanism, experiencing the transfer from Down to Init and from Init to Up. When setting up the session, the session parameters are negotiated, including the interval of sending packets and detection interval.

After the session is set up, send the detection packets periodically to detect the path status. If the BFD control packets of the peer device are not received within the detection interval, the BFD protocol regards that the path has fault and informs the fault information to the upper application protocol.

After the upper application protocol receives the fault report, inform the BFD protocol to delete the session when disabling or deleting the neighbor. If no other upper-layer protocol needs to detect the session link, delete the corresponding session.

According to the type of the detection path, it includes the single-hop IP path detection neighboring with the local end and the peer, and the multi-hop IP path detection not neighboring with the local end and peer. Currently, linking OSPF, RIP, EBGP, ISIS, LDP, RSVP-TE, TRACK, and static route protocols with BFD belongs to the single-hop IP path detection. IBGP linking with BFD belongs to multi-hop IP path detection.

7.2. BFD Function Configuration

Table 7-1 BFD function configuration list

Configuration Task	
Configure the BFD basic functions	Configure the minimum sending interval of the single-hop BFD control packets
	Configure the minimum receiving interval of the single-hop BFD control packets
	Configure the detection timeout multiples of the single-hop BFD session
	Configure the minimum sending interval of the non-single-hop BFD control packets
	Configure the minimum receiving interval of the non-single-hop BFD control packets
	Configure the detection timeout multiples of the non-single-hop BFD session

7.2.1. Configure BFD Basic Functions

Configuration Condition

Before configuring the BFD basic functions, first complete the following tasks:

- Configure the IP address of the interface, making the neighboring node network layer reachable
- Configure the upper-layer application associated with BFD

Configure Minimum Sending Interval of Single-hop BFD Control Packets

Table 7-2 Configure the minimum sending interval of BFD control packets

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the minimum sending interval of BFD control packets	**bfd min-transmit-interval** *value*	Optional By default, the minimum sending interval of BFD control packets is 1000ms.

Note:

- The actual sending interval of the peer BFD packets = MAX (minimum sending interval of the peer BFD control packets, the minimum receiving interval of the local BFD control packets)

Configure Minimum Receiving Interval of Single-hop BFD Control Packets

Table 7-3 Configure the minimum receiving interval of the BFD control packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the minimum receiving interval of the BFD control packet	**bfd min-receive-interval** *value*	Optional By default, the minimum receiving interval of the BFD control packets is 1000ms.

Note:

- The actual sending interval of the local BFD packets = MAX (minimum sending interval of the local BFD control packets, the minimum receiving interval of the peer BFD control packets)

Configure Detection Timeout Multiples of Single-hop BFD Session

Table 7-4 Configure the detection timeout multiples of the BFD session

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the interface configuration mode	**interface** *interface-name*	-
Configure the detection timeout multiples of the BFD session	**bfd multiplier** *value*	Optional By default, the detection timeout multiples of the BFD session is 5.

Note:

- To ensure the validity of the BFD session detection, be careful to configure the minimum of the BFD detection timeout multiples.
- Local BFD actual detection time = the detection timeout multiples of the peer BFD session × the actual sending interval of the peer BFD packet

Configure Minimum Sending Interval of Non Single-hop BFD Control Packets

Table 7-5 Configure the minimum sending interval of the non-single-hop BFD control packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the minimum sending interval of the non-single-hop BFD control packet	**bfd non-single-hop min-transmit-interval** *value*	Optional By default, the minimum sending interval of non-single-hop BFD control packets is 1000ms.

Note:

- The actual sending interval of the local BFD packets = MAX (minimum sending interval of the local BFD control packets, the minimum receiving interval of the peer BFD control packets)
- After configuring the minimum receiving time interval of non-single hop BFD control packet, it will take effect for IPv4/IPv6 multi-hop session and MPLS LSP session. If the registration module specifies the minimum receiving time interval of non-single hop BFD control packet, it will take effect with the value specified by the module. If multiple registration modules specify the minimum receiving time interval of non-single hop BFD

control packet of the same session at the same time, it will take effect with the specified minimum value.

Configure Minimum Receiving Interval of Non Single-hop BFD Control Packets

Table 7-6 Configure the minimum receiving interval of the non-single-hop BFD control packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the minimum receiving interval of the non-single-hop BFD control packet	**bfd non-single-hop min-receive-interval** *value*	Optional By default, the minimum receiving interval of the non-single hop BFD control packets is 1000ms.

Note:

- The actual sending interval of the peer BFD control packets = MAX (minimum sending interval of the peer BFD control packets, the minimum receiving interval of the local BFD control packets)
- After configuring the minimum sending time interval of non-single hop BFD control packet, it will take effect for IPv4/IPv6 multi-hop session and MPLS LSP session. If the registration module specifies the minimum sending time interval of non-single hop BFD control packet, it will take effect with the value specified by the module. If multiple registration modules specify the minimum sending time interval of non-single hop BFD control packet of the same session at the same time, it will take effect with the specified minimum value.

Configure Detection Timeout Multiples of Non-Single-hop BFD Session

Table 7-7 Configure the detection timeout multiples of the non-single-hop BFD session

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the detection timeout multiples of the non-single-hop BFD session	**bfd non-single-hop multiplier** *value*	Optional By default, the detection timeout multiples of the non-single-hop BFD session is 5.

Note:

- To ensure the validity of the BFD session detection, be careful to configure the minimum of the BFD detection timeout multiples.

- Local BFD actual detection time = the detection timeout multiples of the peer BFD session × the actual sending interval of the peer BFD packet
- After configuring the detection timeout multiple of non-single hop BFD sessions, it will take effect for IPv4/IPv6 multi hop sessions and MPLS LSP sessions. If the registration module specifies the detection timeout multiple of non-single hop BFD session, the value specified by the registration module takes effect. If multiple registration modules specify the detection timeout multiple of non-single hop BFD sessions of the same session at the same time, the specified minimum value will take effect.

7.2.2. BFD Monitoring and Maintaining

Table 7-8 BFD monitoring and maintaining

Command	Description
show bfd capability	Display the BFD capability information
show bfd discriminator	Display the BFD local discriminator value information
show bfd session	Display the information of the BFD IPv4 session
show bfd session ipv6	Display the information of the BFD IPv6 session
show bfd session lag-micro	Display the information of the BFD LAG-Micro session
show bfd session mpls	Display the information of the BFD MPLS session
show bfd session summary	Display the summary information of the BFD session

7.3. BFD Typical Configuration Example

7.3.1. Configure BFD Basic Functions

Network Requirements

- All devices run the OSPF protocol; Device1 and Device3 configure the BFD detection function.
- Modify the BFD parameters. When the line between the switch and Device3 fails, the service data between Device1 and Device3 can realize the ms-level switching.

Network Topology

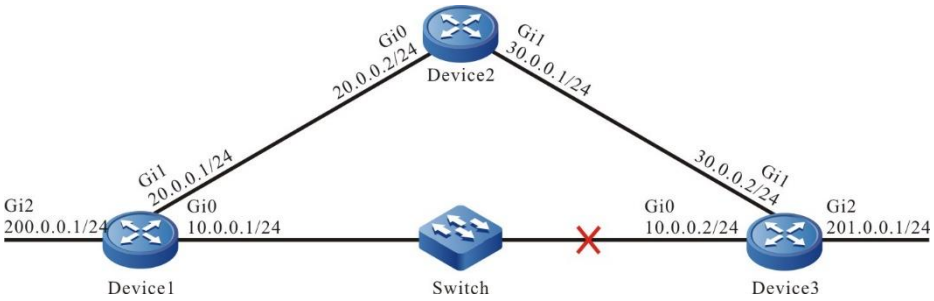

Figure 7-1 Networking of configuring the BFD basic functions

Configuration Steps

Step 1: Configure the interface IP address. (Omitted)

Step 2: Configure OSPF.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.255 area 0
Device1(config-ospf)#network 20.0.0.0 0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.255 area 0
Device2(config-ospf)#network 30.0.0.0 0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 10.0.0.0 0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.255 area 0
Device3(config-ospf)#exit
```

Step 3: Configure OSPF to link with BFD.

#Configure Device1.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip ospf bfd
Device1(config-if-gigabitethernet0)#exit
```

#Configure Device3.

```
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#ip ospf bfd
Device3(config-if-gigabitethernet0)#exit
```

#View the BFD session of Device1.

```
Device1#show bfd session 10.0.0.2 detail
OurAddr     NeighAddr        LD/RD          State      Holddown      interface
10.0.0.1    10.0.0.2         312/319        UP         5000          gigabitethernet0
Type:ipv4 direct
Local State:UP  Remote State:UP  Up for: 0h:10m:57s  Number of times UP:1
Send Interval:1000ms  Detection time:5000ms(1000ms*5)
Local Diag:0  Demand mode:0  Poll bit:0
MinTxInt:1000  MinRxInt:1000  Multiplier:5
Remote MinTxInt:1000  Remote MinRxInt:1000  Remote Multiplier:5
Registered modules:OSPF
```

We can see that OSPF links with BFD successfully, the session is set up normally and the detection timeout is 5s.

#View the route table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 00:20:01, gigabitethernet0
L   10.0.0.1/32 is directly connected, 00:20:01, gigabitethernet0
C   20.0.0.0/24 is directly connected, 00:25:22, gigabitethernet1
L   20.0.0.1/32 is directly connected, 00:25:22, gigabitethernet1
O   30.0.0.0/24 [110/2] via 20.0.0.2, 00:12:31, gigabitethernet1
                [110/2] via 10.0.0.2, 00:11:20, gigabitethernet0
C   127.0.0.0/8 is directly connected, 00:31:09, lo0
```

```
L   127.0.0.1/32 is directly connected, 00:31:09, lo0
C   200.0.0.0/24 is directly connected, 00:20:10, gigabitethernet2
L   200.0.0.1/32 is directly connected, 00:20:10, gigabitethernet2
O   201.0.0.0/24 [110/2] via 10.0.0.2, 00:11:30, gigabitethernet0
```

In the route table, we can see that the route 201.0.0.0/24 first selects the line between Device1 and Device3 to communicate.

Step 4: Configure the BFD parameters.

#Configure Device1. Modify the minimum sending interval and minimum receiving interval of the BFD control packets to 100ms. The detection timeout multiples is 3.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#bfd min-transmit-interval 100
Device1(config-if-gigabitethernet0)#bfd min-receive-interval 100
Device1(config-if-gigabitethernet0)#bfd multiplier 3
Device1(config-if-gigabitethernet0)#exit
```

#Configure Device3. Modify the minimum sending interval and minimum receiving interval of the BFD control packets to 100ms. The detection timeout multiples is 3.

```
Device3(config)#interface gigabitethernet0
Device3(config-if-gigabitethernet0)#bfd min-transmit-interval 100
Device3(config-if-gigabitethernet0)#bfd min-receive-interval 100
Device3(config-if-gigabitethernet0)#bfd multiplier 3
Device3(config-if-gigabitethernet0)#exit
```

Step 5: Check the result.

#View the BFD session of Device1.

```
Device1#show bfd session 10.0.0.2 detail
OurAddr    NeighAddr      LD/RD          State      Holddown      interface
10.0.0.1   10.0.0.2       312/319        UP         300           gigabitethernet0
Type:direct
Local State:UP  Remote State:UP  Up for: 0h:11m:27s  Number of times UP:1
Send Interval:100ms  Detection time:300ms(100ms*3)
Local Diag:0  Demand mode:0  Poll bit:0
MinTxInt:100  MinRxInt:100  Multiplier:3
Remote MinTxInt:100  Remote MinRxInt:100  Remote Multiplier:3
Registered modules:OSPF
```

After modifying the BFD parameters, the BFD detection timeout is negotiated from 5s to 300ms.

#When the line between Device1 and Device3 fails, BFD fast detects the fault and informs OSPF, and then OSPF switches the route to Device2 for communication. View the route table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   10.0.0.0/24 is directly connected, 00:25:00, gigabitethernet0
L   10.0.0.1/32 is directly connected, 00:25:00, gigabitethernet0
C   20.0.0.0/24 is directly connected, 00:30:33, gigabitethernet1
L   20.0.0.1/32 is directly connected, 00:30:33, gigabitethernet1
O   30.0.0.0/24 [110/2] via 20.0.0.2, 00:17:32, gigabitethernet1
C   127.0.0.0/8 is directly connected, 00:36:10, lo0
L   127.0.0.1/32 is directly connected, 00:36:10, lo0
C   200.0.0.0/24 is directly connected, 00:25:11, gigabitethernet2
L   200.0.0.1/32 is directly connected, 00:25:11, gigabitethernet2
O   201.0.0.0/24 [110/3] via 20.0.0.2, 00:00:10, gigabitethernet1
```

Compared with the route table in Step 3, we can see that the route 201.0.0.0/24 is already switched to Device2 for communication.

The BFD processing mode on Device3 is similar to Device1.

8. EEP

8.1. Overview

EEP: embedded event platform, which is an extensible and customizable event detection and processing mechanism directly provided in the device. EEP provides a method for users to monitor specific events, obtain information and set actions when events occur.

8.2. EEP Function Configuration

Table 8-1 EEP function configuration list

Configuration Task	
Configure EEP policy	Configure the EEP policy
Configure the EEP event	Configure EEP to bind none event
	Configure EEP to bind the timer event
	Configure EEP to bind TRACK event
Configure the EEP action	Configure the EEP action

8.2.1. Configure EEP Policy

Configuration Condition

None

Configure EEP Policy

The system can configure multiple EEP policies. Each EEP policy is independent of each other. Only one EEP event can be configured in an EEP policy, and up to 50 EEP actions can be configured.

EEP policy has three states: init, running and suspend:

- The EEP policy is created for the first time, and the status of the EEP policy is init.
- In the created EEP policy, configure EEP events and EEP actions. The status of EEP policy is changed to running. In this state, the EEP policy will execute the configured EEP actions successively after monitoring the configured EEP events.
- The user can suspend all configured EEP policies or a specified EEP policy through the command **event platform suspend** {**policy** *policy-name*}. The EEP policy status changes to suspend. In this state, the EEP policy will not execute the configured EEP action after monitoring the configured EEP event.

Table 8-2 Configure the EEP policy

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Create EEP policy	**event platform applet** *policy-name*	Mandatory
Suspend EEP policy	**event platform suspend** {**policy** *policy-name*}	Optional

8.2.2. Configure EEP Event

Configuration Conditions

Before configuring the EEP event, first complete the following task:

- Configure the EEP policy

Configure EEP to Bind None Event

Table 8-3 Configure EEP to bind none event

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the EEP policy configuration mode	**event platform applet** *policy-name*	-
Configure EEP to bind none event	**event none**	Mandatory

Note:

- The EEP binds null events, and the EEP policy has no events to monitor. Therefore, the user can only trigger the EEP policy of binding null events to execute EEP actions through the command **event platform run** *policy- name*.

Configure EEP to Bind Timer Event

The timer events bound to EEP can be divided to four kinds of timer events:

- Absolute timer: The timer event is triggered when the specified time configured by the user arrives.
- Calendar timer: The timer event is triggered when the periodic time configured by the user arrives.

- Countdown timer: When the countdown time configured by the user arrives, the timer event is triggered.
- Watchdog timer: When the watchdog time configured by the user arrives, the timer event is triggered.

Table 8-4 Configure EEP to bind the timer event

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the EEP policy configuration mode	**event platform applet** *policy-name*	-
Configure EEP to bind the Absolute timer event	**event timer absolute** *year month day hour:minute*[*:second*]	Optional
Configure EEP to bind the Calendar timer event	**event timer calendar** { **per-day** *hour:minute*[*:second*] **| per-hour** *minute* | **per-month** *day hour:minute*[*:second*] | **per-week** *week hour:minute*[*:second*] }	Optional The value range of *minute* is 0-59. The value range of *day* is 1-28. The value range of *week* is 0-6, 0 indicates Sunday.
Configure EEP to bind the Countdown timer event	**event timer countdown** *time-value*	Optional The value range of *time-value* is 1-107374182, and the unit is second.
Configure EEP to bind the Watchdog timer event	**event timer watchdog** *time-value*	Optional The value range of *time-value* is 1-107374182, and the unit is second.

Configure EEP to Bind TRACK Event

Table 8-5 Configure EEP to bind the TRACK event

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the EEP policy configuration mode	**event platform applet** *policy-name*	-
Configure EEP to bind the TRACK event	**event track** *track-id* {*up-to-down*| *down-to-up*}	Optional The value range of *track-id* is 1-500.

8.2.3. Configure EEP Actions

Table 8-6 Configure the EEP actions

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the EEP policy configuration mode	**event platform applet** *policy-name*	-
Configure EEP to execute the command line actions	**action** *action-number* {**cli-command** *cli-command-string* | **force-switchover | reload** [**master | slave**] **| syslog** [**msg** *message-text* | **priority** *priority-value* **msg** *message-text*]}	Optional The value range of *action-number* is 1-1000.

Note:

- When EEP policy executes command actions, execute the command line from small to large according to *action-number*.
- The command line ***cli-command-string*** is executed in configuration mode by default.

8.2.4. EEP Monitoring and Maintaining

Table 8-7 EEP monitoring and maintaining

Command	Description
show eep policy registered { *detail* **|** *INEXIST-EVENT* **|** *NONE-EVENT* **|** *TIMER-EVENT* **|** *TRACK-EVENT* }	View all EEP policy status information

8.3. EEP Typical Configuration Example

8.3.1. Configure EEP Policy to Associate PBR

Network Requirements

- OSPF protocol is running on all devices, and PBR is configured on Device1.
- By configuring PBR, PC can access server 2.2.2.2 through Device1 and Device2.
- By configuring EEP to associate PBR, when the interface between Device1 and Device2 goes down, EEP will quickly notify PBR to delete the next hop configuration, so that PC can access server 2.2.2.2 through Device1 and Device3; When the link between Device1 and Device2 returns to normal, EEP notifies PBR to add the next hop configuration to enable PC to access server 2.2.2.2 through Device1 and Device2.

Network Topology

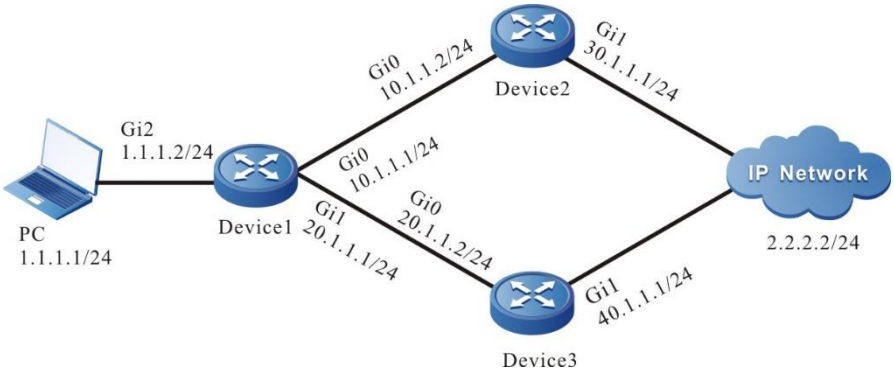

Figure 8-1 Networking of configuring EEP policy to associate with PBR

Configuration Steps

Step 1: Configure the IP address of the interface. (omitted)

Step 2: Enable the unicast routing protocol OSPF so that all devices in the network can communicate with each other.

#Configure Device1.

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 1.1.1.0 0.0.255 area 0
```

```
Device1(config-ospf)#network 11.1.0 0.0.255 area 0
Device1(config-ospf)#network 21.1.0 0.0.255 area 0
Device1(config-ospf)#exit
```

#Configure Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device1(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 11.1.0 0.0.255 area 0
Device2(config-ospf)#network 31.1.0 0.0.255 area 0
Device2(config-ospf)#exit
```

#Configure Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device1(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 21.1.0 0.0.255 area 0
Device3(config-ospf)#network 41.1.0 0.0.255 area 0
Device3(config-ospf)#exit
```

#Check the routing table of Device1. You can see that there are two next hops to the 2.2.2.0/24 network.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   1.1.1.0/24 is directly connected, 22:14:53, gigabitethernet2
L   1.1.1.1/32 is directly connected, 22:14:53, gigabitethernet2
O   2.2.2.0/24 [110/3] via 11.1.2, 00:00:09, gigabitethernet0
              [110/3] via 21.1.2, 00:00:09, gigabitethernet1
C   11.1.0/24 is directly connected, 21:41:21, gigabitethernet0
L   11.1.1/32 is directly connected, 21:41:21, gigabitethernet0
C   21.1.0/24 is directly connected, 15:19:15, gigabitethernet1
L   21.1.1/32 is directly connected, 15:19:15, gigabitethernet1
O   31.1.0/24 [110/2] via 11.1.2, 18:55:36, gigabitethernet0
O   41.1.0/24 [110/2] via 21.1.2, 00:22:08, gigabitethernet1
C   127.0.0.0/8 is directly connected, 87:42:47, lo0
L   127.0.1/32 is directly connected, 87:42:47, lo0
```

#Configure Device1 and modify the cost value of the interface gigabitethernet0 to 100, so that the route to the 2.2.2.0/24 network preferably selects the gigabitethernet1 interface.

```
Device1(config)#interface gigabitethernet0
Device1(config-if-gigabitethernet0)#ip ospf cost 100
Device1(config-if-gigabitethernet0)#exit
```

#View the route table of Device1.

```
Device1#show ip route
Codes: C - Connected, L - Local, S - static, R - RIP,  B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management, E - IRMP, EX - IRMP external

C   1.1.1.0/24 is directly connected, 23:27:34, gigabitethernet2
L   1.1.1.1/32 is directly connected, 23:27:34, gigabitethernet2
O   2.2.2.0/24 [110/3] via 21.1.2, 01:12:50, gigabitethernet1
C   11.1.0/24 is directly connected, 22:54:03, gigabitethernet0
L   11.1.1/32 is directly connected, 22:54:03, gigabitethernet0
C   21.1.0/24 is directly connected, 16:31:57, gigabitethernet1
L   21.1.1/32 is directly connected, 16:31:57, gigabitethernet1
O   31.1.0/24 [110/3] via 21.1.2, 00:31:42, gigabitethernet0
O   41.1.0/24 [110/2] via 21.1.2, 01:34:50, gigabitethernet1
C   127.0.0.0/8 is directly connected, 88:55:28, lo0
L   127.0.1/32 is directly connected, 88:55:28, lo0
```

#View the path to the server 2.2.2.2 through the **traceroute** command on the PC.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

 1    1 ms    1 ms    1 ms  1.1.1.2
 2   <1 ms   <1 ms   <1 ms  21.1.2

 n   <1 ms   <1 ms   <1 ms  2.2.2.2
Trace complete.
```

It can be seen that PC accesses server 2.2.2.2 through Device1 and Device3.

Step 3: On Device1, configure the policy routing.

#Configure ACL 1001, permitting PC to access the network 2.2.2.0/24.

```
Device1(config)#ip access-list extended 1001
```

```
Device1(config-ext-nacl)#permit ip any 2.2.2.0 0.0.255
Device1(config-ext-nacl)#exit
```

#Configure policy routing aaa, associate access control list 1001, and specify the next hop as 11.1.2.

```
Device1(config)#route-policy aaa permit 10
Device1(config-pbr)#match ip address acl 1001
Device1(config-pbr)#set ip next-hop 11.1.2
Device1(config-pbr)#exit
```

#View the information of the policy route aaa of Device1.

```
Device1#show route-policy aaa
route-policy aaa
  sequence 10 permit:
    match ip address acl 1001
    set ip next-hop 11.1.2
```

Step 4: Apply policy routing.

#On the interface gigabitethernet2 of Device1, apply the policy routing aaa.

```
Device1(config)#interface gigabitethernet2
Device1(config-if-gigabitethernet2)#ip policy aaa
Device1(config-if-gigabitethernet2)#exit
```

#On the PC, view the path to the server 2.2.2.2 via the command Traceroute.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

  1    1 ms    1 ms    1 ms  1.1.1.2
  2   <1 ms   <1 ms   <1 ms  11.1.2

  n   <1 ms   <1 ms   <1 ms  2.2.2.2
Trace complete.
```

You can see that after the policy routing is applied to the interface gigabitethernet2, the PC accesses the server 2.2.2.2 through Device1 and Device2.

Step 5: Configure EEP policy to associate PBR.

#Configue TRACK 1 to monitor the status of the interface gigabitethernet 0.

```
Device1(config)#track 1
Device1(config-track)#interface gigabitethernet0 line-protocol
```

```
Device1(config-track)#exit
```

#Configure EEP policy e1 on Device1, bind track group 1, monior the status of interface gigabitethernet0, and notify PBR to delete the corresponding next hop configuration when Device1 interface gigabitethernet0 is down.

```
Device1(config)#event platform applet e1
Device1(config-eep)#event track 1 up-to-down
Device1(config-eep)#action 1 cli-command route-policy aaa permit 10
Device1(config-eep)#action 2 cli-command no set ip next-hop 11.1.2
Device1(config-eep)#exit
```

#Configure EEP policy e2 on Device1, bind track group 1, monior the status of interface gigabitethernet0, and notify PBR to delete the corresponding next hop configuration when Device1 interface gigabitethernet0 is up.

```
Device1(config)#event platform applet e2
Device1(config-eep)#event track 1 down-to-up
Warning:
Configuring event track 1 down-to-up is risky, are you sure to configure?(Yes/No)yes
Device1(config-eep)#action 1 cli-command route-policy aaa permit 10
Device1(config-eep)#action 2 cli-command set ip next-hop 11.1.2
Device1(config-eep)#exit
```

Step 6: Check the result.

#When interface gigabitethernet0 of Device1 is down, EEP will quickly notify PBR to delete the next hop configuration, and PC will access server 2.2.2.2 through Device3.

```
Device1#show route-policy aaa
route-policy aaa
  sequence 10 permit:
    match ip address acl 1001
```

#View the path to the server 2.2.2.2 through the traceroute command on the PC.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

  1    1 ms    1 ms    1 ms  1.1.1.2
  2   <1 ms   <1 ms   <1 ms  21.1.2

  n   <1 ms   <1 ms   <1 ms  2.2.2.2
Trace complete.
```

You can see that after the interface gigabitethernet2 is down, the PC accesses the server 2.2.2.2 through Device1 and Device3.

#When the interface gigabitethernet0 of Device1 is up, EEP will notify PBR to add the next hop configuration, and PC will access server 2.2.2.2 through Device2.

```
Device1#show route-policy aaa
route-policy aaa
  sequence 10 permit:
    match ip address acl 1001
    set ip next-hop 11.1.2
```

#View the path to the server 2.2.2.2 through the traceroute command on the PC.

```
C:\Documents and Settings\Administrator>tracert 2.2.2.2

Tracing route to 2.2.2.2 over a maximum of 30 hops

  1    1 ms    1 ms    1 ms  1.1.1.2
  2   <1 ms   <1 ms   <1 ms  11.1.2

  n   <1 ms   <1 ms   <1 ms  2.2.2.2
Trace complete.
```

You can see that after the interface gigabitethernet2 is up, the PC accesses server 2.2.2.2 through Device1 and Device2.

9. ULFD

9.1. Overview

In the traditional Ethernet, we usually use the fiber and other physical medium to connect the devices. In the actual networking, the fiber crossover connection (Figure 9-1), or one fiber not connected or disconnected (Figure 9-2) may result in the uni-directional communication. This kind of faulty link is called uni-directional link. The uni-directional link causes a series of problems. For example, the spanning tree detection failure results in the topology calculation error.

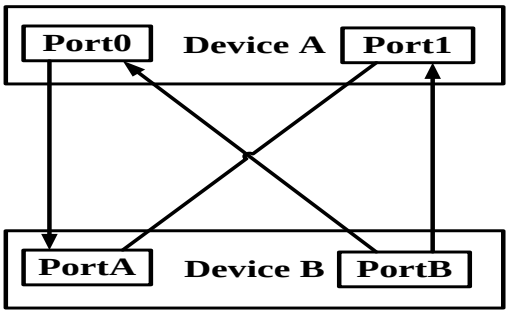

Figure 9-1 Fiber crossover connection

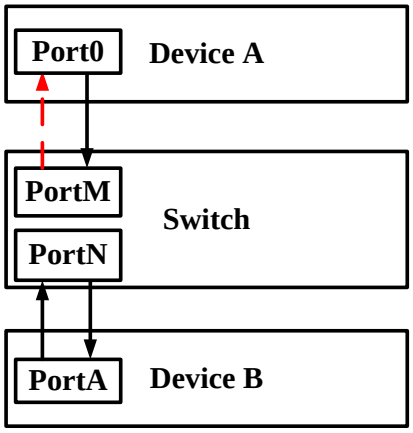

Figure 9-2 One fiber is not connection or disconnected

ULFD (Unidirectional Link Fault Detection) can monitor whether the fiber or twisted-pair has the uni-directional link. When ULFD detects the uni-directional link, it is responsible for closing the physical and logical uni-directional connection, sending the alarm information to the user and blocking the failure of other protocols.

9.2. ULFD Function Configuration

Table 9–1 ULFD function configuration list

Configuration Task	
Configure the ULFD basic functions	Enable global ULFD function
	Enable the ULFD function of the Ethernet interface
Configure the ULFD parameters	Configure the period of sending the ULFD detection packets
	Re-set the Ethernet interface disabled by ULFD

9.2.1. Configure ULFD Basic Functions

Configuration Condition

Before configuring the ULFD basic functions, first complete the following task:

- Ensure that the ULFD detection port is connected normally

Enable global ULFD function

ULFD has two work modes, that is, normal and aggressive. For the two modes, the basis of judging the uni-directional link is different. The normal mode is often used to check the uni-direction caused by the crossover connection. The aggressive mode is used to check the uni-directional connection caused by the crossover connection or disconnection.

Table 9–2 Enable global ULFD function

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enable global ULFD function	**ulfd router enable**	Mandatory By default, do not enable global ULFD function.

Enable ULFD Function of Ethernet Interface

ULFD detection needs to enable the global ULFD detection function and the ULFD detection function of the Ethernet interface. If the ULFD function is not enabled globally, but just enabled on the Ethernet interface, the ULFD function cannot take effect.

If the global enabled ULFD detection mode and Ethernet interface enabled ULFD detection mode are inconsistent, the Ethernet interface ULFD detection mode takes effect first.

Table 9–3 Enable the ULFD function of the Ethernet interface

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Enter the Ethernet interface configuration mode	**interface** *interface-name*	-
Enable the ULFD function of the Ethernet interface	**ulfd interface** [**aggressive | normal**]	Mandatory By default, do not enable the ULFD function of the Ethernet interface.

Note:

- To switch over the ULFD work mode on the Ethernet interface, first cancel the previous work mode and then configure the new mode.
- When enabling the ULFD function on the Ethernet interface, ensure that the neighbor Ethernet interface is also configured with the ULFD function and works in the same detection mode.

9.2.2. Configure ULFD Parameters

Configuration Condition

Before configuring the ULFD parameters, first complete the following task:

- Enable the ULFD function

Configure Sending Period of ULFD Detection Packet

ULFD periodically sends the detection packets to detect whether the network has the uni-directional link. We can modify the sending period of the detection packets according to the actuality of the network. The sending period of the detection packets is 7-120s. By default, it is 15s.

Table 9–4 Configure the sending period of the ULFD detection packet

Step	Command	Description
Enter the global configuration mode	**configure terminal**	-
Configure the sending period of the ULFD packet	**ulfd router message time** *time-value*	Optional By default, the sending period of the uni-directional detection packet is 15s.

Reset Ethernet Interface Disabled by ULFD

If ULFD detects the uni-direction and disables the Ethernet interface, to re-enable the ULFD detection function of the Ethernet interface, the user needs to perform the reset operation manually. The operation sets the Ethernet interface to UP and re-enables the ULFD detection.

Table 9–5 Reset the Ethernet interface disabled by ULFD

Step	Command	Description
Reset the Ethernet interface disabled by ULFD	**ulfd router reset** [**interface** *interface-name*]	Optional By default, do not execute the reset operation automatically after the Ethernet interface is disabled.

Caution:

- If ULFD has detected uni-directional link, do not switch over the ULFD work mode on the interface. If switching over the work mode, the **ULFD reset** command for resetting the disabled interface becomes invalid.

9.2.3. ULFD Monitoring and Maintaining

Table 9–6 ULFD monitoring and maintaining

Command	Description
show ulfd { **interface** [*interface-name*] **| router | statistic** }	Display the ULFD configuration information, status information, and statistics information

9.3. ULFD Typical Configuration Example

9.3.1. Configure ULFD Basic Function

Network Requirements

- Device1 and Device2 are connected via the fiber.
- Configure the ULFD normal mode to disable the port when detecting the uni-directional link.

Network Topology

Figure 9-3 Networking of configuring the ULFD basic function

Configuration Steps

Step 1: Configure the ULFD function

#Enable the ULFD function on Device1 and configure the ULFD work mode as the normal mode on port gigabitethernet0.

```
Device1#configure terminal
Device1(config)#ulfd router enable
Device1(config)#interface gigabitethernet 0
Device1(config-if-gigabitethernet0)#ulfd interface
Device1(config-if-gigabitethernet0)#exit
```

#Enable the ULFD function on Device2 and configure the ULFD work mode on port gigabitethernet0 as the normal mode.

```
Device2#configure terminal
Device2(config)#ulfd router enable
Device2(config)#interface gigabitethernet 0
Device2(config-if-gigabitethernet0)#ulfd interface
Device2(config-if-gigabitethernet0)#exit
```

#View the ULFD information of port gigabitethernet0 on Device1.

```
Device1#show ulfd route interface gigabitethernet 0
Interface name      : gigabitethernet0
ULFD config mode    : Normal
ULFD running mode   : Normal
Link status         : Link Up
Link direction      : Bidirectional
ULFD fsm status     : Advertisement

Neighbors number    : 1
----------
  Device ID         : 001fce787878
  Interface name    : gigabitethernet0
  Device Name       : Device2
  Message Interval  : 15
  Timeout Interval  : 5
  Link Direction    : Bidirectional
  Aging Time        : 40
  Time to Die       : 36
-------------------------------------
```

Note:

- The method of viewing the port ULFD information on Device2 is the same as that of Device1. (Omitted)

Step 2: Check the result.

#In the actual networking environment, when the fibers are cross-connected or one fiber is not connected, disconnected, it results in the uni-directional communication. After configuring the ULFD function, port gigabitethernet0 is disabled when detecting the uni-directional connection on Device1 and the following log information is output:

```
%ULFD-LOG-5:Interface gigabitethernet0 learnt a new neighbor: deviceId[001fce7c7179], deviceName[Device2], interfaceName[gigabitethernet0].

%ULFD-LOG-4:Interface gigabitethernet0 unidirectional link was detected.

%ULFD-LOG-4:Now shutdown interface gigabitethernet0, if you want to restore it, pleaseuse the command [ulfd router reset interface] on the mode of globalconfiguration.
```

#View the status of the port gigabitethernet0 and we can see that the port is disabled.

```
Device1#show interface gigabitethernet0
gigabitethernet0:
  line protocol is administratively down by ULFD
  Flags: (0x18062) BROADCAST MULTICAST ARP RUNNING
  Type: ETHERNET_CSMACD
  Internet address: 67.67.0.1/24
  Broadcast address: 67.67.0.255
  Metric: 0, MTU: 1500, BW: 1000000 Kbps, DLY: 10 usec, VRF: global
  Reliability 255/255, Txload 1/255, Rxload 1/255
  Ethernet address is 001f.cecf.6c59
  Last clearing of "show interface" counters is 0 hour 0 minute 0 second ago
  input rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
  output rate 0 bit/sec, 0 packet/sec, bandwidth utilization 0.00%
  0 packets received; 0 packets sent
  0 bytes received; 0 bytes sent
  0 multicast packets received
  0 multicast packets sent
  0 input errors; 0 output errors
  0 collisions; 0 dropped
  Unknown protocol 0
    line status down: speed auto, duplex auto, media-type auto
    rxframe:0, rxBroadcast:0, rxMulticast:0, rxOctets:0
    rxPause:0, rxCrcErr:0, rxOctErr:0, rxtxLenErr:0
    txframe:0, txBroadcast:0, txMulticast:0, txOctets:0
    txPause:0, jabbers:0, collisions:0, CarrierSenseErrors:0
    InDiscards:0, InErrors:0, OutDiscards:0, OutErrors:0
```

Note:

- When configuring the ULFD function, ensure that ULFD configured at the two sides of the link work in the same detection mode.
- When ULFD work mode is aggressive mode, refer to the configuration method.

10. ОБЩАЯ ИНФОРМАЦИЯ

10.1. Замечания и предложения

Мы всегда стремимся улучшить нашу документацию и помочь вам работать лучше, поэтому мы хотим услышать вас. Мы всегда рады обратной связи, в особенности:

- ошибки в содержании, непонятные или противоречащие места в тексте;
- идеи по улучшению документации, чтобы находить информацию быстрее;
- неработающие ссылки и замечания к навигации по документу.

Если вы хотите написать нам по поводу данного документа, то используйте, пожалуйста, форму обратной связи на qtech.ru.

10.2. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» −> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» −> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

10.3. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

Телефон Технической поддержки +7 (495) 797-33-11 доб. 0