Reliability Configuration

Оглавление

8. CONFIGURING RNS

QTECH
МИР ДОСТУПНЕЕ

1.1 Overview

The Rapid Ethernet Uplink Protection Protocol (REUP) provides a rapid uplink protection function.

In the dual uplink networking, REUP is used to ensure normal communication between links, block redundant links, avoid link loops, and implement fast backup.

The upstream interfaces of REUP are configured in pairs. If both interfaces are normal, an interface works in the backup state. The interface in the backup state does not forward data packets. When the interface in the forward state is faulty, the backup interface switches to the forward state immediately, and provides data transmission. In addition, REUP also sends address update packets to upstream devices so that the upstream devices can update their MAC addresses immediately. This function of REUP ensures that layer-2 data streams can be restored within 50 ms after a link is faulty.

REUP is mutually exclusive with the Spanning Tree Protocol (STP) based on interfaces. In this case, a device runs STP downward and runs REUP upward to implement backup and fault protection for the upstream link. REUP ensures that basic link redundancy is provided when STP is disabled and that millisecond-level fault recovery faster than STP is also provided.

Protocols and Standards

- REUP is a proprietary protocol of QTECH Network, and there is no standard and protocol for reference.
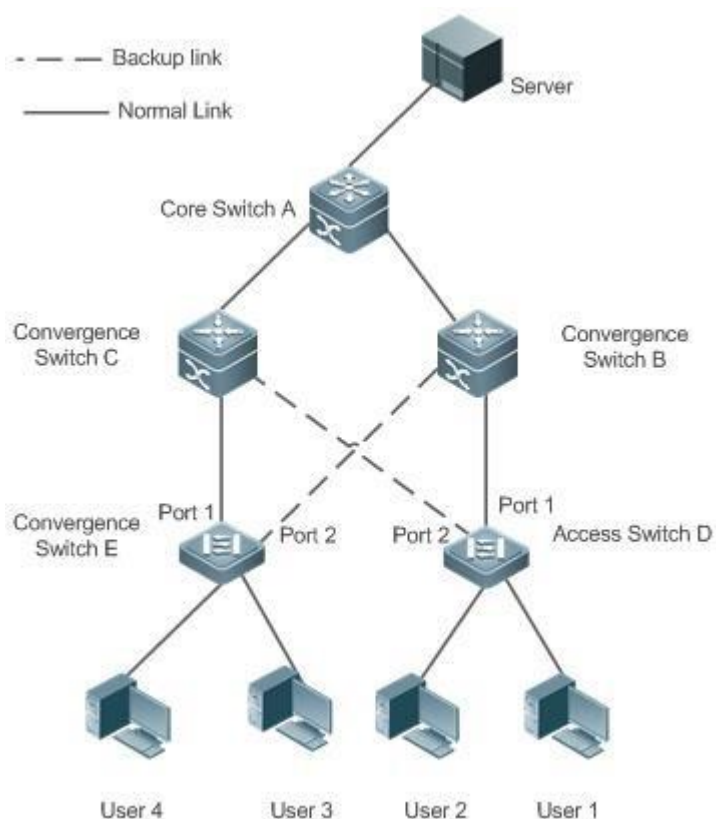
1.2 Applications

Application	Description
Communication in Dual Uplink Networking	Forward packets in the dual-uplink networking.

1.2.1 Communication in Dual Uplink Networking
Scenario

For communication in dual uplink networking, the access switch has two uplink paths, as shown in Figure 1-1.

Figure 1-1 Dual uplink networking

Deployment

- Enable REUP on interface1 and interface2 of the access switch D/E to implement fast switching when a link is faulty.

- Enable MAC address update message receiving of REUP on the interfaces connected to switches A/B/C to rapidly clear the MAC addresses on the interfaces when a link is faulty.

1.3   Features

Basic Concepts

❖   REUP Pair

Specify an interface as the backup interface of another interface to configure an REUP pair. One interface is the active interface and the other interface is the backup interface. When the two interfaces are normal, an interface is configured as the forward interface whereas the other interface is configured as the backup interface. You can determine the interface to be configured as the backup interface. See the related information in the section "Configuring the Preemption Mode and Delay Time of REUP".

❖   MAC Address Update Message

MAC address update messages refer to FLUSH packets sent by QTECH Network to uplink devices through private multicast. When an uplink device of QTECH Network enables the function for receiving MAC address update messages and receives MAC address update messages, the device updates the MAC addresses of corresponding interfaces.

❖ **MAC Address Update Group**

Multiple interfaces are added to a group. If one interface in the group receives a MAC address update message, the MAC addresses of other interfaces in the group will be updated. In this case, the group is called MAC address update group.

❖ **MAC Address Update Packet**

Packets sent to update MAC addresses in order to support uplink devices are called MAC address update packets.

❖ **Link Tracking Group**

The uplink and downstream interfaces of a device are added to a group. If all upstream interfaces in the group are down, all downstream interfaces in this group are forced down. In this case, this group is called a link tracing group.

Overview

| Feature	Description
Dual Link Backup of REUP	When a link is faulty, the other link can rapidly switch to the forward state.
Preemption Mode and Delay Time of REUP	When both links are normal, the preemption mode can be used to determine the link that is used for forwarding data and the delay time that is used to determine the waiting time before switching.
MAC Address Update	During link switching, the MAC address of an interface is updated to make packet convergence faster.
VLAN Load Balance	When the two links are normal, the utilization of link bandwidth can be maximized.
Link State Tracking	When the upstream link is faulty, the downstream link is switched.

1.3.1 Dual Link Backup of REUP

When an active link is faulty, the link in the backup state will rapidly switch to the forward state and start forwarding data, minimizing the service interruption caused by link failure.

Working Principle

Specify an interface as the backup interface of another interface to configure an REUP pair. When the two interfaces are normal, a link is in the forward state (forwarding data packets) and the other link is in the backup state (not forwarding data). When the active link is faulty, the link in the backup state rapidly switches to the forward state and starts forwarding data.

When the faulty link is recovered, the link enters the backup state and does not forward data packets. Of course, you can configure the preemption mode to specify whether a link recovered from failure preempts the link that is in the forward state currently.

Figure 1-2 A topology with two normal links
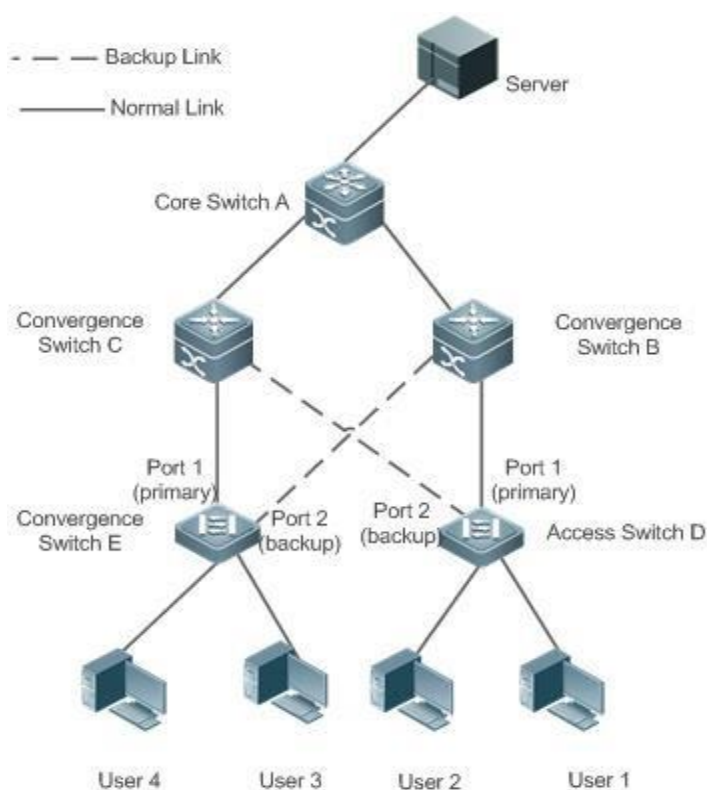
As shown in Figure 1-2, connect interfaces 1 and 2 of switch D (E) to the uplink switches B and C (C and B) and configure REUP on interfaces 1 and 2. When the links are normal, interface 1 is in the forward state and forwards data packets and interface 2 is in the backup state and does not forward data packets.

Figure 1-3 A topology with interface 1 of switch D (E) faulty
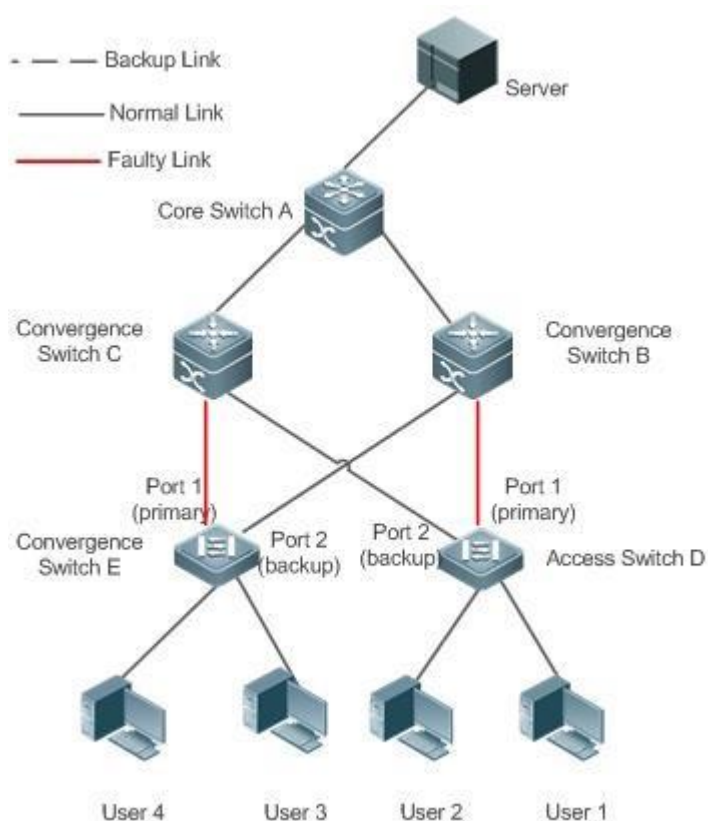
Once interface 1 is faulty, interface 2 immediately starts forwarding data packets and recovers the uplink transmission of the switch. In the non-preemption mode, when the link of interface 1 is recovered, interface 1 is in the backup state and does not forward data packets whereas interface 2 continues forwarding data packets.

Related Configuration

❖ **Enabling Dual Link Backup on an interface**

By default, dual link backup on an interface is disabled.

You can run the **switchport backup interface** command to configure a layer-2 physical interface (or layer-2 AP interface) as a backup interface and enable the dual link ackup function of REUP.

You must enable the dual link backup function of REUP on an interface. The function involves the link switching of REUP only when an interface is faulty.

REUP, ERPS, and RERP do not share interfaces.

Devices enabled with REUP must disable the storm control function of all layer-2 interfaces.

1.3.2   Preemption Mode and Delay Time of REUP
Working Principle

You can determine which link should be used first by configuring the preemption

mode of REUP. If the preemption mode is set to bandwidth first, REUP selects a link with a high bandwidth first. You can also set the preemption mode to forced to select a stable and reliable link first forcibly.

To avoid frequent active/backup link switching caused by abnormal faults, REUP provides a preemption delay function. When the two links are recovered, link switching is performed when the faulty link becomes stable after a delay (35s by default).

Related Configuration

❖ **Configuring the Preemption Mode and Delay Time of REUP**

By default, the preemption mode is disabled and the delay time is 35s.

You can run the **switchport backup interface preemption mode** command to configure the preemption mode. You can run the **switchport backup interface preemption delay** command to configure the delay time.

A smaller delay means more frequent preemption switching after the faulty link is recovered.

REUP uses the value of the Bandwidth attribute for an AP interface as the actual bandwidth of the AP interface, which is equal to the value of the Speed attribute (the number of link up member interfaces x the number of member interfaces).

When an uplink enables STP, the preemption delay time of REUP is greater than 35s.

1.3.3 MAC Address Update

During link switching, the MAC address of an interface is updated to make packet convergence faster.

Working Principle

As shown in Figure 1-2, interface 1 and interface 2 of switch D (E) are enabled with dual link backup of REUP. Interface 1 works as the active interface. During normal communication, switch A learns the MAC addresses of users 1 and 2 (users 3 and 4) from the interfaces connecting to switch B (C).

When interface 1 of switch D (E) is faulty, interface 2 rapidly switches to the forward state and starts forwarding data packets. In this case, switch A does not learn the MAC addresses of users 1 and 2 (users 3 and 4) on the interfaces connecting to switch B (C). The data packets sent by the server to users 1 and 2 (users 3 and 4) are forwarded to switch C (B) by switch A, causing that the packets from the server to users 1 and 2 (users 3 and 4) are lost.

To avoid the preceding problems, you can enable the MAC address update function on switch D (E). When interface 2 starts forwarding packets, switch D (E) sends a MAC address update message to interface 2. After receiving the MAC address update message, switch A updates the MAC address on the interface of switch A. In this way, switch A forwards the packets sent by the server to the users to the interfaces of switch

B (C) to make packet convergence faster. In addition, import the setting of a MAC address update group, that is, classify multiple interfaces into the same group. When an interface in this group receives a MAC address update message, the MAC addresses on other interfaces in the group are updated to reduce the side effect of flooding caused by MAC address update.

To be compatible with upstream devices not supporting MAC address update messages, switch D (E) will send MAC address update packets for users 1 and 2 (users 3 and 4) upward when interface 2 switches to the forward state. In this way, switch A can update the MAC addresses of users 1 and 2 (users 3 and 4) to the corresponding interfaces and recover the downlink data transmission of switch A.

Related Configuration

❖ **Enabling Sending of MAC Address Update Messages on an interface**

By default, sending of MAC address update messages is disabled on an interface.

You can run the **mac-address-table move update transit** command to enable sending of MAC address updates on all interfaces of a device.

If sending of MAC address update messages is not enabled, MAC address update messages will not be sent when dual link backup switching of REUP is performed.

❖ **Enabling Receiving of MAC Address Update Messages on an interface**

By default, receiving of MAC address update messages is disabled on an interface.

You can run the **mac-address-table move update receive** command to enable receiving of MAC address updates on all interfaces of a device.

If receiving of MAC address update messages is not enabled, a device cannot receive MAC address update messages from downlink devices during dual link backup switching of REUP and will not update the MAC addresses.

❖ **Configuring a VLAN for Sending MAC Address Update Messages**

By default, a VLAN for sending MAC address update messages is the default VLAN to which an interface belongs.

You can run the **mac-address-table move update transit vlan** command to configure the VLAN in which interfaces send MAC address update messages.

If the VLAN in which interfaces send MAC address update messages is configured, the messages are sent in the configured VLAN; otherwise, the messages are sent in the default VLAN to which the interface belongs.

❖ **Configuring a VLAN for Receiving MAC Address Update Messages**

By default, MAC address update messages are received in all VLANs.

You can run the **no mac-address-table move update receive vlan** command to configure a VLAN in which interfaces do not receive MAC address update messages. MAC address update messages are received in remaining VLANs.

If no VLAN in which interfaces receive MAC address update messages is configured, MAC address update messages are received in all the configured VLANs; otherwise, MAC address update messages are received in the remaining VLANs.

❖ **Configuring a MAC Address Update Group**

By default, there is no MAC address update group.

You can run the **mac-address-table update group** command to add an interface to the MAC address update group. The interface is added to the first update group by default.

If no MAC address update group is configured, MAC address update will not be performed when MAC address update packets are received.

❖ **Configuring the Maximum Number of MAC Address Update Packets Sent Per Second**

By default, the maximum number of MAC address update packets sent per second is 150.

You can run the **mac-address-table move updatemax-update-rate** command to configure the maximum number of MAC address update packets sent per second.

The larger the number of packets, the more CPU time used for sending the packets, and the fewer downlink packets are lost.

1.3.4   VLAN Load Balance
Working Principle

The VLAN load balance function allows REUP to forward data packets of mutually exclusive VLANs for two interfaces to make full use of the link bandwidth.

As shown in Figure 1-4, configure dual link backup of REUP and enable VLAN load balance of REUP on interface 1 and interface 2 of switch D, and map VLAN 1 to instance 1 and VLAN 2 to instance 2. Data of VLAN 1 (instance 1) is transmitted through interface 1 and all the other data of VLAN 2 (instance 2) is transmitted through interface 2. Perform the same processing on switch E.

When an interface is faulty, the other interface takes over the transmission of all VALNs. When the faulty interface is recovered and does not become faulty within the preemption delay, the transmission of VLANs is switched back to the recovered interface.

Figure 1-4 A topology with two normal links of load balance
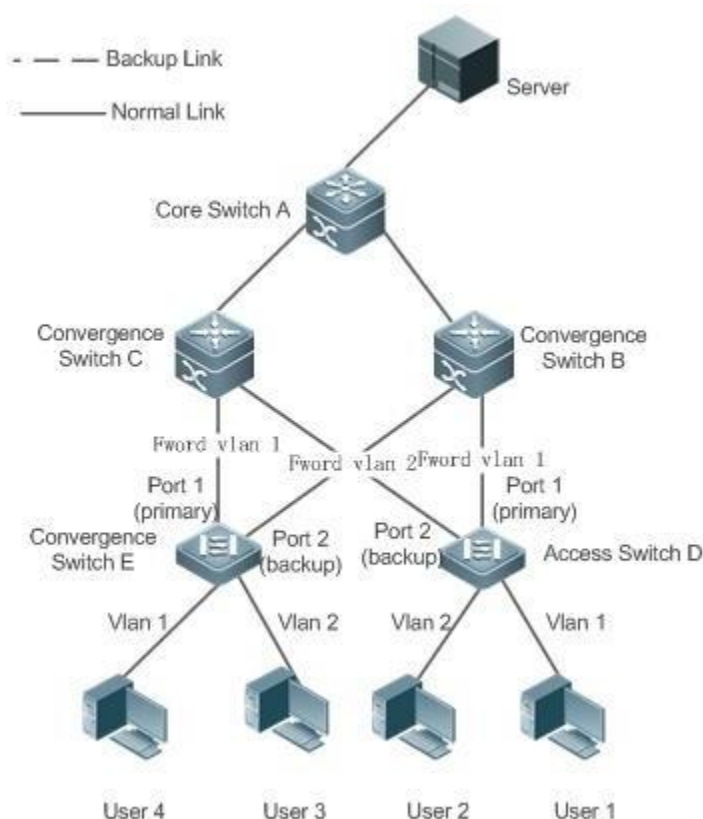
Related Configuration

❖ **Enabling VLAN Load Balance on an interface**

By default, the VLAN load balance function on an interface is disabled.

You can run the **switchport backup interface prefer instance** command to enable the VLAN load balance function.

If this function is not enabled, the link bandwidth cannot be fully used when packets are forwarded when the two links are normal. You must enable the VLAN load balance function on a port so that the interface can be involved in VLAN load balance.

The instance mapping of REUP VLAN load balance is controlled by the MSTP module in a unified manner. For details about how to configure the instances, see the description in the *Configuring MSTP*.

The VLAN load balance function can be configured only on trunk, uplink or hybrid interfaces.

1.3.5 Link State Tracking

Link tracking means that when the upstream link is faulty, services are switched

www.qtech.ru

to the downstream link so that the backup interface can continue forwarding packets.

Working Principle

Link state tracking provides the function of notifying downlink devices for link switching when the upstream link is faulty. You can configure the uplink and downstream interfaces of a link state tracking group and bind the link status of multiple downstream interfaces to the interfaces of multiple upstream links to implement link status synchronization. When all upstream links in a tracking group are faulty, the interfaces of the downstream links are shut down forcibly to ensure that the transmission of the downstream links is switched from the active link to the backup link.

As shown in Figure 1-5, when the upstream link of switch B is faulty, link state tracking rapidly shuts down the downstream interface of switch B so that the uplink transmission of switch D is switched to switch C.

Figure 1-5 A topology where the upstream link of the active link is faulty
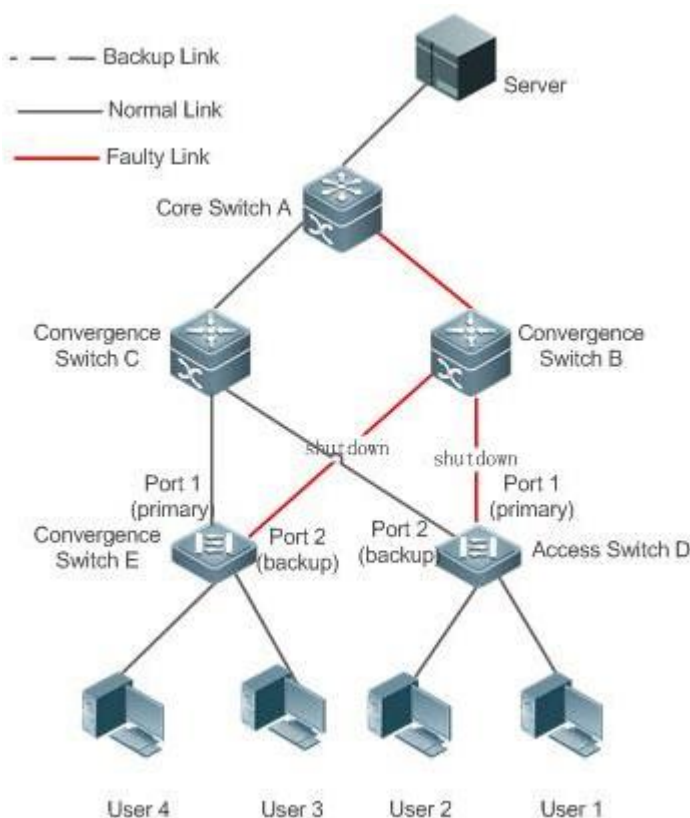
Related Configuration

❖ **Enabling Link Tracking**

Link tracking is disabled by default.

You can run the **link state track** [*number*] command to enable a link tracking group.

The value of **number** ranges from 1 to 2. The first link tracking group is enabled by default (the default value of **number** is 1).

If link tracking is not enabled, the status of a corresponding upstream interface cannot be detected and packet forwarding switching cannot be implemented in time.

❖ Enabling the Downlink Delay Up Function for a Link Tracking Group

By default, the downlink delay for link tracking is 0s.

You can run the **link state track** *number* **up-delay** *timer* command to enable a link tracking group. The value of **number** ranges from 1 to 2. The first link tracking group is enabled by default (the default value of **number** is 1). The value of **timer** ranges from 0 to 300s, which is 0s by default.

By enabling the downlink delay up function, you can avoid frequent downlink switching caused by uplink flapping in a link tracking group. That is, when the upstream link becomes up, the downstream link becomes up after a delay.

❖ **Adding an interface to a Link Tracking Group**

By default, an interface is not added to a link tracking group.

You can run the **link state group** [*number*] {**upstream** | **downstream**} command to set upstream interfaces and downstream interfaces of the link tracking group. The value of **number** ranges from 1 to 2. An interface is added to the first link tracking group by default (the default value of number is **1**).

If an interface is not added to a tracking group, the status of a corresponding upstream interface cannot be detected and packet forwarding switching cannot be implemented in time.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of REUP	(Mandatory) It is used to enable dual link backup of REUP.	
	switchport backup interface	Enables dual link backup of REUP.
Configuring the Preemption Mode and Delay Function of REUP	(Optional) It is used to determine the preemption mode and delay time. The default values are used if they are not configured.	
	switchport backup interface preemption mode	Sets the preemption mode.

	switchport backup interface preemption delay	Sets the delay time for preemption.
[Configuring MAC Address Update](#)	(Optional) It is used to enable rapid update of MAC addresses.	
Configuration	**Description and Command**	
	mac-address-table move update transit	Enables sending of MAC address update messages.
	mac-address-table move update transit vlan	Enables sending of the VLAN ID of MAC address update messages.
	mac-address-table move update	Configures the maximum number of MAC address update packets sent per second. The value ranges from 0 to 32000. The default value is 150.
	mac-address-table move update receive	Enables receiving of MAC address update messages.
	mac-address-table move update receive vlan	Configures the VLAN range for processing MAC address update messages.
[Configuring VLAN Load Balance](#)	(Optional) It is used to enable VLAN load balance.	
	switchport backup interface prefer instance	Configures the link VLAN load balance of REUP.
[Configuring Link Tracking](#)	(Optional) It is used to enable link tracking.	
	link state track up-delay	Enables the downlink delay up for a link state tracking group.
	link state track	Enables a link state tracking

		group.
	link state group	Add an interface as an upstream interface or a downstream interface of a specified link state tracking group.

1.4.1   Configuring Basic Functions of REUP

Configuration Effect

- When a link is faulty, the other normal link is switched to the forward state immediately for forwarding packets.

Notes

- An interface belongs to only one REUP pair. Each active link has only one backup link. A backup link can be used as the backup link of only one active link. The active and backup links must use different interfaces.

- REUP supports layer-2 physical interfaces and AP interfaces, but does not support AP member interfaces.

- The active and backup interfaces may be of different types and have different rates. For example, an AP interface can be used as the active interface whereas a physical interface is configured as the backup interface.

- Interfaces configured with REUP are not involved in STP calculation.

- Each device can be configured with a maximum of 16 REUP pairs.

- Interfaces successfully configured with REUP cannot change interfaces to layer-3 interfaces or be added to an AP.

Configuration Steps

❖ **Enabling Dual Link Backup of REUP**

- Mandatory.

- If there is no special requirement, dual link backup of REUP should be enabled on an interface of the receiving switch.

Verification

Run the **show interfaces switchport backup [detail]** command to check whether dual link backup of REUP is configured.

Related Commands

www.qtech.ru

❖ **Enabling Dual Link Backup of REUP**

Command	switchport backup interface *interface-id*
Parameter Description	*interface-id*: Indicates the backup interface ID.
Command Mode	Interface configuration mode
Usage Guide	If the interface where the mode resides is the active interface, the interface corresponding to the **interface-id** parameter is the backup interface. When the active link is faulty, rapidly recover the transmission of the backup link.

Configuration Example

❖ Enabling Dual Link Backup of REUP

Scenario	**As shown in Figure 1-6, there are two upstream links from switch D to switch A, which are switch D > switch**
Figure 1-6	B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A,
Dual uplink networking	which are switch E > switch B > switch A and switch E > switch C > switch A.
Configuration Steps	Configure dual link backup (the interface Gi0/1 is the active interface and Gi0/2 is the backup interface) of REUP on the access switch D (E).

D	`SwitchD> enable`
	
	`SwitchD# configure terminal`
	
	`SwitchD(config)# interface GigabitEthernet 0/1 SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk`
	`SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface GigabitEthernet 0/2 SwitchD(config-if-GigabitEthernet 0/1)# exit`

E	`SwitchE> enable`
	`SwitchE# configure terminal`
	`SwitchE(config)# interface GigabitEthernet 0/1 SwitchE(config-if-GigabitEthernet 0/1)# switchport mode trunk`
	`SwitchE(config-if-GigabitEthernet 0/1)#switchport backup interface GigabitEthernet 0/2 SwitchD(config-if-GigabitEthernet 0/1)# exit`

Verification	Check the dual link backup information configured for switch D (E).
D	`SwitchD#show interfaces switchport backup detail` `Switch Backup Interface Pairs:`

	`Active Interface     Backup Interface     State`
	
	`Gi0/1                Gi0/2                Active Up/Backup Standby`
	
	`Interface Pair : Gi0/1, Gi0/2 Preemption Mode : off Preemption Delay : 35 seconds`
	`Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)`

E	`SwitchE#show interfaces switchport backup detail Switch Backup Interface Pairs:`
	`Active Interface     Backup Interface     State`
	
	`Gi0/1                Gi0/2                Active Up/Backup Standby`
	`Interface Pair : Gi0/1, Gi0/2 Preemption Mode : off Preemption Delay : 35 seconds`
	`Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)`

Common Errors

- Other REUP pairs are configured on a configured interface.
- A configured interface is not a layer-2 physical interface or AP interface.

1.4.2 Configuring the Preemption Mode and Delay Function of REUP
Configuration Effect

- Restrict the preemption mode and preemption delay time for REUP link switching.

Notes

- Dual link backup of REUP must be configured.

www.qtech.ru

Configuration Steps

▪ Optional.

If the active link needs to always forward packets or the link bandwidth needs to be used to determine the link for forwarding packets, the corresponding preemption mode and delay time must be configured.

Verification

Run the **show interfaces switchport backup [detail]** command to check whether the preemption mode and delay time are consistent with the configurations.

Related Commands

❖ **Configuring the Preemption Mode of REUP**

Command	switchport backup interface *interface-id* preemption mode {forced|bandwidth|off}
Parameter Description	*interface-id*: Indicates the backup interface ID. **mode**: Sets the preemption mode: **forced**: Indicates the forced mode. **bandwidth**: Indicates the bandwidth mode. **off**: Indicates that the preemption mode is off.
Command Mode	Interface configuration mode
Usage Guide	The preemption modes include forced, bandwidth and off. In the bandwidth mode, an interface with a high bandwidth is selected first to transmit data; in the forced mode, the active interface is selected first to transmit data; in the off mode, no preemption is performed. The default mode is off.

❖ Configuring the Delay Time of REUP

Command	switchport backup interface *interface-id*preemption delay *delay-time*
Parameter Description	*interface-id*: Indicates the backup interface ID. *delay-time*: Indicates the delay time.
Command Mode	Interface configuration mode

Usage Guide	Preemption delay indicates the delay time after a faulty link is recovered to the time when link switching is performed again.

Configuration Example

❖ Configuring the Preemption Mode and Delay Time of REUP

Scenario	**As shown in Figure 1-6, there are two upstream links from switch D to switch A, which are switch D > switch B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A, which are switch E > switch B > switch A and switch E > switch C > switch A.**
Configuration Steps	Configure the preemption mode to bandwidth on the access switch D (E) and the delay time to 40s.
D	```SwitchD> enable```

	```SwitchD# configure terminal```
	```SwitchD(config)# interface GigabitEthernet 0/1```
	```SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preemption mode bandwidth SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preemption delay 40 SwitchD(config-if-GigabitEthernet 0/1)# exit```

E	```SwitchE> enable```
	```SwitchE# configure terminal```
	```SwitchD(config)# interface GigabitEthernet 0/1```
	```SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preemption mode bandwidth SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi 0/2 preemption delay 40 SwitchD(config-if-GigabitEthernet 0/1)# exit```

Verification	Check the dual link backup information configured for switch D (E).

D	```SwitchD#show interfaces switchport backup detail Switch Backup Interface Pairs:```
	``` Active Interface Backup Interface State```
	``` Gi0/1 Gi0/2 Active Up/Backup Standby```
	
	```Interface Pair : Gi0/1, Gi0/2 Preemption Mode : bandwidth Preemption Delay : 40 seconds```
	```Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)```

E	```SwitchE#show interfaces switchport backup detail Switch Backup Interface Pairs:```
	``` Active Interface Backup Interface State```
	
	``` Gi0/1 Gi0/2 Active Up/Backup Standby```

```
Interface Pair : Gi0/1, Gi0/2 Preemption Mode : bandwidth Preemption
Delay : 40 seconds
Bandwidth : Gi0/1(100000 Mbits), Gi0/2(100000 Mbits)
```

Common Errors

- A configured interface is not a layer-2 physical interface or AP interface.

1.4.3   Configuring MAC Address Update
Configuration Effect

- Rapidly delete and update MAC addresses of an interface during link switching to make packet convergence faster.

Notes

- Dual link backup of REUP must be configured.

- Each device can be configured with a maximum of 8 address update groups. Each address update group can have a maximum of 8 member interfaces and an interface can belong to multiple address update groups.

Configuration Steps

- Mandatory.

- If there is no special requirement, the MAC address update function should be configured.

Verification

Run the **show mac-address-table update group** [**detail**] command to view the update group configuration.

Related Commands

❖ **Configuring the MAC Address Update Group ID of a Switch**

Command	mac-address-table update group [*group-num*]
Parameter Description	*group-num*: Indicates the MAC address update group ID.
Command Mode	Interface configuration mode

| Usage Guide | In order to reduce large flooding caused by MAC address update which may affect normal data transmission of the switch, we add a setting of a MAC address update group. Only after all interfaces on a switching path are added to the same MAC address update group, transmission of downlink data can be rapidly recovered. |

❖ Enabling Sending of MAC Address Update Messages

Command	mac-address-table move update transit
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	To reduce link switching and loss of downlink data streams, you need to enable sending of MAC address update messages on a switch that performs switching.

❖ Enabling Sending of the VLAN ID of MAC Address Update Messages

Command	mac-address-table move update transit vlan*vid*
Parameter Description	*vid*: Indicates the VLAN ID for sending MAC address update messages.
Command Mode	Interface configuration mode
Usage Guide	After sending of MAC address update messages is enabled, MAC address update messages can be sent to uplink devices during link switching.

Configure the maximum number of MAC address update packets sent per second.

❖ **Configuring the Maximum Number of MAC Address Update Packets Sent Per Second**

Command	mac-address-table move update max-update-rate*pkts-per-second*
Parameter Description	*pkts-per-second*: Indicates the maximum number of MAC address update packets sent per second. The value ranges from 0 to 32000. The default value is 150.

Command Mode	Global configuration mode
Usage Guide	During link switching, REUP sends MAC address update packets of a specified quantity to uplink devices per second to recover the downlink data transmission of the uplink device.

❖   Enabling Receiving of MAC Address Update Messages

Command	mac-address-table move update receive
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	During switching of dual link backup, downlink data streams may be lost since the MAC address table of the uplink switch is not updated in real time. In order to reduce loss of layer-2 data streams, you need to update the MAC address table of the uplink switch. In this case, you need to enable receiving of MAC address update messages on the uplink switch.

❖   Configuring the VLAN Range for Processing MAC Address Update Messages

Command	mac-address-table move update receive vlan*vlan-range*
Parameter Description	*vlan-range*: Indicates the VLAN range for processing MAC address update messages.
Command Mode	Global configuration mode
Usage Guide	This command is used to disable the function for processing MAC address update messages on certain VLANs. For a VLAN disabled with the function for processing MAC address update messages, MAC address update packets can be used to recover the downlink transmission of uplink devices; however, the convergence performance for link faults will be decreased.

Configuration Example

❖   Configuring MAC Address Update

Scenario	**As shown in Figure 1-6, there are two upstream links from switch D to switch A, which are switch D > switch B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A, which are switch E > switch B > switch A and switch E > switch C > switch A.**
Configuration Steps	▪ Enable sending of MAC address update messages on the access switch D (E). ▪ Enable receiving of MAC address update packets on switch B (C). ▪ Add all interfaces on the REUP switching path to the same MAC address update group. ▪ In the environment, Gi0/1 and Gi0/3 of switch B are the interfaces on the switching path of switch D's uplink, and Gi0/3 and Gi0/2 are the interfaces on the switching path of switch E's uplink. You can add interfaces Gi0/1, Gi0/2 and Gi0/3 to the same address update group. Similarly, you can obtain the configuration of switch C. ▪ Enable receiving of MAC address update packets on switch A. ▪ Add all interfaces on the REUP switching path of switch A to the same MAC address update group.
| D | ```
SwitchD> enable
SwitchD# configure terminal
SwitchD(config)# mac-address-table move update transit SwitchD(config)# exit
``` |
| **E** | ```
SwitchE> enable
SwitchE# configure terminal
SwitchE((config)# mac-address-table move update transit SwitchE(config)# exit
``` |
| B | ```
SwitchB# configure terminal

SwitchB(config)# mac-address-table move update receive SwitchB(config)# interface range gigabitEthernet 0/1 -3 SwitchB(config-if-range)#switchport mode trunk SwitchB(config-if-range)# mac-address-table update group 1 SwitchB(config-if-range)# end
``` |
| C | ```
SwitchB# configure terminal
SwitchB(config)# mac-address-table move update receive SwitchB(config)# interface range gigabitEthernet 0/1 -3 SwitchB(config-if-range)#switchport mode trunk SwitchB(config-if-range)# mac-address-table update group 1 SwitchB(config-if-range)# end
``` |

| A | ```
SwitchA# configure terminal

SwitchA(config)# mac-address-table move update receive SwitchA(config)#
interface range gigabitEthernet 0/1 -2 SwitchA(config-if-range)#
switchport mode trunk SwitchA(config-if-range)# mac-address-table update
group 1 SwitchA(config-if-range)# end
``` |
|---|---|
| **Verification** | Check the information about the address update groups on switches D, E, C, B and A. |
| D | ```
SwitchD# show run | incl mac-ad

mac-address-table move update transit
``` |
| **E** | ```
SwitchE# show run | incl mac-ad

mac-address-table move update transit
``` |
| B | SwitchB# show mac-address-table update group detail |
| | show mac-address-table update group detailMac-address-table Update Group:1 Received mac-address-table update message count:0 |

Group	member	Receive	Count	Last Receive Switch-ID	Receive Time
Gi0/1		0		0000.0000.0000	
Gi0/2		0		0000.0000.0000	
Gi0/3		0		0000.0000.0000	

| C | ```
SwitchC# show mac-address-table update group detail

Mac-address-table Update Group:1

Received mac-address-table update message count:0
``` |
|---|---|

Group	member	Receive	Count	Last Receive Switch-ID	Receive Time
Gi0/1		0		0000.0000.0000	
Gi0/2		0		0000.0000.0000	
Gi0/3		0		0000.0000.0000	

```
SwitchA# show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0

 Group member      Receive Count Last Receive Switch-ID
                                                    Receive Time

Gi0/1  0      0000.0000.0000

Gi0/2  0      0000.0000.0000
```

Common Errors

- A configured interface is not a layer-2 physical interface or AP interface.

1.4.4 Configuring VLAN Load Balance

Configuration Effect

- Maximize the utilization of link bandwidth.

Notes

- Dual link backup of REUP must be configured.
- The Access interface cannot be shared by VLAN load balance and STP.
- For interfaces successfully configured with VLAN load balance, you cannot modify the attributes of the interfaces but can modify the VLAN attributes of the interfaces.

Configuration Steps

- If maximizing bandwidth utilization is not required, this configuration is optional.
- If there is a requirement for VLAN load balance, corresponding configuration must be performed.

Verification

Run the **show interfaces switchport backup [detail]** command to check whether VLAN load balance is configured.

Related Commands

❖ **Configuring VLAN Load Balance**

Command	switchport backup interface *interface-id* prefer instance *instance-range*
Parameter Description	*interface-id*: Indicates the backup interface ID. *instance-range*: Indicates the load instance range of the backup

www.qtech.ru

	interface.
Command Mode	Interface configuration mode
Usage Guide	You can modify the mapping between instances and VLANs by using the instance mapping function of MSTP.

Configuration Example

❖ Configuring VLAN Load Balance

Scenario	**As shown in Figure 1-6, there are two upstream links from switch D to switch A, which are switch D > switch B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A, which are switch E > switch B > switch A and switch E > switch C > switch A.**
Configuration Steps	▪ Configure instance mappings on switch D (E) to map VLAN 1 to instance 1, VLAN 2 to instance 2, VLAN 3 to instance 3, and VLAN 4 to instance 4. For details, see the *MSTP Configuration Guide*. ▪ Configure the VLAN load balance function on switch D (E).

D	```SwitchD> enable```
	```SwitchD# configure terminal```
	```SwitchD(config)# interface GigabitEthernet 0/1 SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk```
	```SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi0/2 prefer instance 2 SwitchD(config-if-GigabitEthernet 0/1)# exit```

E	```SwitchE> enable```

	```SwitchE# configure terminal```
	
	```SwitchE(config)# interface GigabitEthernet 0/1 SwitchE(config-if-GigabitEthernet 0/1)# switchport mode trunk```
	```SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface gi0/2 prefer instance 4 SwitchD(config-if-GigabitEthernet 0/1)# exit```

Verification	Check the dual link backup information configured for switch D (E).

D	`SwitchD#show interfaces switchport backup detail Switch Backup Interface Pairs:`
	
	` Active Interface      Backup Interface      State`
	
	`Gi0/1  Gi0/2  Active Up/Backup Up`
	
	`Instances Preferred on Active Interface: Instance 0-1,3-64 Mapping VLAN 1,3-4094`
	
	`Instances Preferred on Backup Interface: Instance 2 Mapping VLAN 2`
	
	`Interface Pair : Gi0/1, Gi0/2 Preemption Mode : balance Preemption Delay : 35 seconds`
	
	`Bandwidth : Gi0/1(800 kbits), Gi0/2(100000 kbits)`

E	`SwitchE#show interfaces switchport backup detail Switch Backup Interface Pairs:`
	
	` Active Interface      Backup Interface      State`
	
	` Gi0/1               Gi0/2                Active Up/Backup Up`

	`Instances Preferred on Active Interface: Instance 0-3,5-64 Mapping VLAN 1-3,5-4094`
	
	`Instances Preferred on Backup Interface: Instance 4 Mapping VLAN 4`
	
	`Interface Pair : Gi0/1, Gi0/2 Preemption Mode : balance Preemption Delay : 35 seconds`
	
	`Bandwidth : Gi0/1(800 kbits), Gi0/2(100000 kbits)`

Common Errors

- The mappings between VLAN IDs and instances are not configured.

1.4.5 Configuring Link Tracking
Configuration Effect

- After detecting that the upstream link is disconnected, forcibly disconnect the downstream link so that link switching can be performed.

Notes

- Dual link backup of REUP must be configured.

- For the link state tracking function, each interface belongs to only one link state tracking group and each device can be configured with up to 2 link state tracking groups. Each link state tracking group can have 8 upstream interfaces and 256 downstream interfaces.

Configuration Steps

- Mandatory.

- If there is no special requirement, the uplink tracking function should be configured.

Verification

Run the **show link state group** command to view the configured link tracking information.

Related Commands

❖ **Enabling a Link State Tracking Group**

Command	link state track **[*num*]**
Parameter Description	*num*: Indicates the ID of a link state tracking group.
Command Mode	Global configuration mode
Usage Guide	You can create a link tracking group and then add an interface to the specified tracking group.

❖ Enabling the Downlink Delay Up for a Link State Tracking Group

Command	link state track *num* up-delay *timer*
Parameter Description	*num*: Indicates the ID of a link state tracking group. *timer*: Indicates the downlink delay up time, which is 0s by default.
Command Mode	Global configuration mode
Usage Guide	You must enable the delay function so that the downstream link can be up after the delay.

❖ Adding an interface to a Link Tracking Group

Command	ink stategroup *num* **{**upstream	downstream**}**
Parameter Description	*num*: Indicates the ID of a link state tracking group. **upstream**: Adds the interface as an upstream interface of the tracking group. **downstream**: Adds the interface as a downstream interface of the tracking group.
Command Mode	Interface configuration mode
Usage Guide	You can create a link tracking group and then add an interface to the specified tracking group.

Configuration Example

❖ Configuring a Link Tracking Group

Scenario	**As shown in Figure 1-6, there are two upstream links from switch D to switch A, which are switch D > switch B > switch A and switch D > switch C > switch A. There are two upstream links from switch E to switch A,** **which are switch E > switch B > switch A and switch E > switch C > switch A.**
Configuration Steps	▪ Create link tracking group 1 on switch B (C). ▪ On switch B (C), add the interfaces Gi0/1 and Gi0/2 as downstream interfaces of the link tracking group and add the interface Gi0/3 as an upstream interface of the link tracking group.

B	```SwitchB> enable```
	
	 ```SwitchB# configure terminal SwitchB(config)# link state track 1```
	 ```SwitchB(config)# interface GigabitEthernet 0/1```
	
	 ```SwitchB(config-if-GigabitEthernet 0/1)#link state group 1 downstreamSwitchB(config-if-GigabitEthernet 0/1)#exit```
	 ```SwitchB(config)# interface GigabitEthernet 0/2```
	
	 ```SwitchB(config-if-GigabitEthernet 0/2)# link state group 1 downstream SwitchB(config-if-GigabitEthernet 0/2)#exit```
	 ```SwitchB(config)# interface GigabitEthernet 0/3```
	
	 ```SwitchB(config-if-GigabitEthernet 0/3)#link state group 1 upstream SwitchB(config-if-GigabitEthernet 0/3)#exit```

C	```SwitchC> enable```
	
	 ```SwitchC# configure terminal SwitchC(config)# link state track 1```
	 ```SwitchC(config)# interface GigabitEthernet 0/1```
	
	 ```SwitchC(config-if-GigabitEthernet 0/1)#link state group 1 downstreamSwitchC(config-if-GigabitEthernet 0/1)#exit```
	 ```SwitchC(config)# interface GigabitEthernet 0/2```
	
	 ```SwitchC(config-if-GigabitEthernet 0/2)# link state group 1 downstream SwitchC(config-if-GigabitEthernet 0/2)#exit```
	 ```SwitchC(config)# interface GigabitEthernet 0/3```
	
	 ```SwitchC(config-if-GigabitEthernet 0/3)#link state group 1 upstream SwitchC(config-if-GigabitEthernet 0/3)#exit```

Verification	Check the link tracking group information configured for switch B (C).

B	`SwitchB#show link state group`
	`Link State Group:1 Status: enabled, Down Upstream Interfaces`
	`:Gi0/3(Down)`

	`Downstream Interfaces : Gi0/2(Down)`

Common Errors

- Interfaces are added to a link tracking group when the link tracking group is not enabled.

1.5 Monitoring

Displaying

Description	Command
Displays the dual link backup information of REUP.	**show interfaces**[*interface-id*]**switchport backup** [**detail**]
Displays the configurations of an MAC address update group.	**show mac-address-table update group** [**detail**]
Displays the REUP statistics about sent MAC address update messages.	**show mac-address-table move update**
Displays the information about a link state tracking group.	**show link state group**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables all REUP debugging.	**debug reup all**
Debugs the normal running process of REUP.	**debug reup process**
Debugs MAC address update messages of REUP.	**debug reup packet**

Debugs MAC address update packets of REUP.	**debug reup macupdt**
Debugs hot backup.	**debug reup ha**
Debugs errors occurring in REUP running.	**debug reup error**
Debugs received events.	**debug reup evnet**
Debugs statistics when **show** operations are performed.	**debug reup status**

2.1   Overview

The Rapid Link Detection Protocol (RLDP) achieves rapid detection of unidirectional link failures, directional forwarding failures and downlink loop failures of an Ethernet. When a failure is found, relevant ports will be closed automatically according to failure treatment configuration or the user will be notified to manually close the ports to avoid wrong flow forwarding or an Ethernet layer-2 loop.
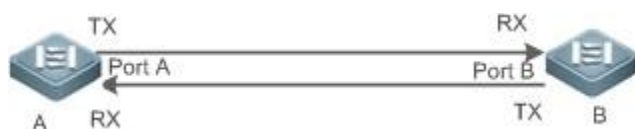
2.2   Applications

Application	Description
Unidirectional Link Detection	Detect a unidirectional link failure.
Bidirectional Forwarding Detection	Detect a bidirectional link failure.
Downlink Loop Detection	Detect a link loop.

2.2.1   Unidirectional Link Detection

Scenario

As shown in the following figure, A is connected to B via optical fiber. The two lines are the Tx and Rx lines of optical fiber. Unidirectional link detection is enabled on A and B. If any of the Tx of Port A, Rx of Port B, Tx of Port B and Rx of Port A fails, a unidirectional failure will be detected and treated under the RLDP. If the failure is eliminated, the administrator may manually restore the RLDP on A and B and resume detection.

Figure 2-1

Remarks	**A and B are layer-2 or layer-3 switches.**
	The Tx of Port A of A is connected to the Rx of Port B of B. The

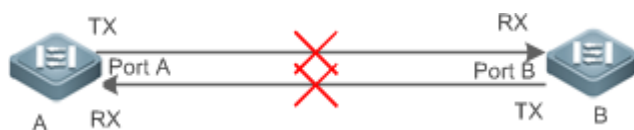|	Rx of Port A of A is connected to the Tx of Port B of B.

Deployment

- Global RLDP is enabled.

- Configure unidirectional link detection under Port A and Port B and define a method for failure treatment.

2.2.2   Bidirectional Forwarding Detection

Scenario

As shown in the following figure, A is connected to B via optical fiber, and the two lines are Tx and Rx lines of optical fiber. Unidirectional link detection is enabled on A and B. If the Tx of Port A, Rx of Port B, Rx of Port A and Tx of Port B all fail, a bidirectional failure will be detected and treated under the RLDP. If the failure is eliminated, the administrator may manually restore the RLDP on A and B and resume detection.

Figure 2-2

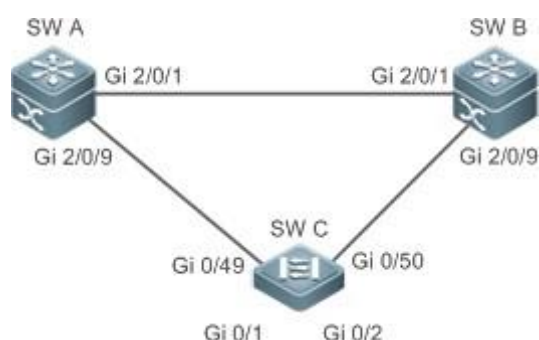| Remarks	A and B are layer-2 or layer-3 switches. The Tx of Port A of A is connected to the Rx of Port B of B. The Rx of Port A of A is connected to the Tx of Port B of B.

Deployment

- Global RLDP is enabled.
- Configure BFD under Port A and Port B and define a method for failure treatment.

2.2.3   Downlink Loop Detection

Scenario

As shown in the following figure, A, B and C are connect into a loop. Downlink loop detection is enabled on A, and a loop is detected and treated.

Figure 2-3

Remarks	A, B and C are layer-2 or layer-3 switches.
	A, B and C are interconnected via exchange ports

Deployment

- Global RLDP is enabled on A.

- Configure downlink loop detection on the Gi 2/0/1 and Gi 2/0/9 ports of A, and define a method for failure treatment.

2.3 Features

Most Ethernet link detection mechanisms detect link connectivity through automatic physical-layer negotiation. However, in some cases devices are connected on the physical layer and operate normally but layer-2 link communication is disabled or abnormal. The RLDP recognizes a neighbor device and detects a link failure through exchanging Prob packets, Echo packets or Loop packets with the device.

Basic Concepts

❖ **Unidirectional Link Failure**

A unidirectional link failure occurs in case of a cross-connected optical fiber, a disconnected optical fiber, an open-circuit optical fiber, one open-circuit line in a twisted-pair cable, or unidirectional open circuit of an intermediate device between two devices. In such cases, one end of a link is connected and the other disconnected so that flow is forwarded wrongly or a loop guard protocol (for example, the STP) fails.

❖ **Bidirectional Link Failure**

A bidirectional link failure occurs in case of two optical fibers, two open-circuit lines in a twisted-pair cable, or bidirectional open circuit of an intermediate device between two devices. In such cases, the both ends of a link are disconnected so that flow is forwarded wrongly.

❖ **Loop Failure**

A downlink device is wrongly connected to form a loop, resulting in a broadcast storm.

❖ **RLDP Packet**

The RLDP defines three types of packets: Prob packets, Echo packets and Loop packets.

- Prob packets are layer-2 multicast packets for neighbor negotiation, and unidirectional or bidirectional link detection. The default encapsulation format is SNAP, which changes automatically to EthernetII if a neighbor sends EthernetII packets.

- Echo packets are layer-2 unicast packets as response to Prob packets and used for unidirectional or bidirectional link detection. The default encapsulation format is SNAP, which changes automatically to EthernetII if a neighbor sends EthernetII packets.

- Loop packets are layer-2 multicast packets for downlink loop detection. They can only be received. The default encapsulation format is SNAP.

❖ **RLDP Detection Interval and Maximum Detection Times**

A detection interval and the maximum detection times can be configured for the RLDP. A detection interval determines the period of sending Prob packets and Loop packets. When a device receives a Prob packet, it replies with an Echo packet immediately. A detection interval and the maximum detection times determine the maximum detection time (equal to a detection interval × the maximum detection times + 1) for unidirectional or bidirectional link detection. If neither Prob nor Echo packet from a neighbor can be received within the maximum detection time, the treatment of unidirectional or bidirectional failure will be triggered.

❖ **RLDP Neighbor Negotiation**

When configured with unidirectional or bidirectional link detection, a port can learn a peer-end device as its neighbor. One port may learn one neighbor, which is variable. If negotiation is enabled, unidirectional or bidirectional link detection starts after a port finds a neighbor through negotiation, which succeeds when a port receives a Prob packet from the neighbor. However, if the RLDP is enabled under a failure, the port cannot learn a neighbor so that detection cannot start. In this case, recover the link state before enabling the RLDP.

❖ **Treatment for Failed Port under RLDP**

- Warning: Only print Syslog to indicate a failed port and a failure type.

- Shutdown SVI: Print Syslog, and then inquire an SVI according to the Access VLAN or Native VLAN of a port and shut down the SVI if the port is a

physical exchange port or layer-2 AP member port.

- Port violation: Print Syslog, and configure a failed port as in violation state, and the port will enter Linkdown state physically.

- Block: Print Syslog, and configure the forward state of a port as Block, and the port will not forward packets.

❖ **Recovery of Failed Port under RLDP**

- Manual reset: Manually reset all failed ports to initialized state and restart link detection.

- Manual or automatic errdisable recovery: Recover all failed ports to initialized state manually or regularly (30s by default and configurable) and restart link detection.

- Automatic recovery: Under unidirectional or bidirectional link detection, if the treatment for failed ports is not specified as port violation, recover ports to initialized state based on Prob packets and restart link detection.

❖ **Port State under RLDP**

- normal: Indicates the state of a port after link detection is enabled.

- error: Indicates the state of a port after a unidirectional or bidirectional link failure or a loop failure is detected.

❖ **Overview**

Feature	Description
Deploying RLDP Detection	Enable unidirectional or bidirectional link detection or downlink loop detection for failures and implement treatment.

2.3.1 Deploying RLDP Detection

The RLDP provides unidirectional link detection, bidirectional forwarding detection and downlink loop detection.

Working Principle

❖ **Unidirectional Link Detection**

When this function is enabled, a port sends Prob packets and receives Echo packets from a neighbor regularly as well as receiving Prob packets from a neighbor and replying with Echo packets. Within the maximum detection time, if the port receives Prob packets but no Echo packets, or none of them, treatment for a unidirectional failure will be triggered and detection will stop.

❖ **Bidirectional Forwarding Detection**

When this function is enabled, a port sends Prob packets and receives Echo packets from a neighbor regularly as well as receiving Prob packets from a neighbor and replying with Echo packets. Within the maximum detection time, if the port receives neither Prob packets nor Echo packets from a neighbor, treatment for a bidirectional failure will be triggered and detection will stop.

❖ **Downlink Loop Detection**

When this function is enabled, a port sends Loop packets regularly. In the following cases, a loop failure will be triggered after the same port or a different port receives the packets: in one case, the egress and ingress ports are the same routed port or layer-3 AP member port; in another case, the egress and ingress ports are exchange ports or layer-2 AP member ports in a same default VLAN and in Forward state. Treatment for the failure will be implemented and detection will stop.

Related Configuration

▪ Configuring RLDP Detection

By default, RLDP detection is disabled.

You may run the global command **rldp enable** or the interface command **rldp port** to enable RLDP detection and specify a detection type and treatment.

You may run the **rldp neighbor-negotiation** command to neighbor negotiation, the **rldp detect-interval** to specify a detection interval, the **rldp detect-max** to specify detection times, or the **rldp reset** to recover a failed port.

2.4   Configuration

Configuration	Description and Command	
Configuring Basic RLDP	(Mandatory) It is used to enable RLDP detection under global configuration mode.	
Functions	**rldp enable**	Enables global RLDP detection on all ports.
	(Mandatory)It is used to specify under interface configuration mode a detection type and failure treatment for an interface.	
	rldp port	Enables RLDP detection on a port and specifies a detection type

		and failure treatment.
	(Optional)It is used to configure a detection interval, detection times and neighbor negotiation under global configuration mode.	
	rldp detect-interval	Modifies global RLDP parameters on all ports, such as the detection interval, maximum detection times and neighbor negotiation.
	rldp detect-max	
	rldp neighbor-negotiation	
	(Optional) It is used under privileged mode.	
	rldp reset	Recovers all ports.

2.4.1   Configuring Basic RLDP Functions

Configuration Effect

- Enable RLDP unidirectional link detection, bidirectional forwarding detection, or downlink loop detection to discover loop failures.

Notes

- Loop detection is effective to all member ports of an AP when configured on one of the ports. Unidirectional link detection and bidirectional forwarding detection are effective only on an AP member port.

- The loop detection on a physical port added to an AP shall be configured the same as that of the other member ports. There are three cases. First, if loop detection is not configured on a newly-added port but on the existing member ports, the new port adopts the configuration and detection results of the existing ports. Second, if a newly-added port and the existing member ports have different loop detection configuration, the new port adopts the configuration and detection results of the existing ports.

- When configuring the RLDP on an AP port, you may configure failure treatment only as "shutdown-port", to which other configurations will be modified.

- When "shutdown-port" is configured on a port, RLDP detection cannot be restored in case of a failure. After troubleshooting, you may run the **rldp reset** or **errdisable recovery** command to restore the port and resume detection. For configuration of the **errdisable recovery** command, please refer to the

Configuring Interface.

Configuration Steps

❖ **Enabling RLDP**

▪ Mandatory.

▪ Enable RLDP detection on all ports under global configuration mode.

❖ **Enabling Neighbor Negotiation**

▪ Optional.

▪ Enable the function under global configuration mode, and port detection will be started under successful neighbor negotiation.

❖ **Configuring Detection Interval**

▪ Optional.

▪ Configure a detection interval under global configuration mode.

❖ **Configuring Maximum Detection Times**

▪ Optional.

▪ Specify the maximum detection times under global configuration mode.

❖ **Configuring Detection under Port**

▪ Mandatory.

▪ Configure unidirectional RLDP detection, bidirectional RLDP detection or downlink loop detection under interface configuration mode, and specify failure treatment.

❖ **Restoring All Failed Ports**

▪ Optional.

▪ Enable this function under privileged mode to restore all failed ports and resume detection.

Verification

▪ Display the information of global RLDP, port and neighbor.

Related Commands

❖ **Enabling Global RLDP Detection**

www.qtech.ru

Command	rldp enable
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable global RLDP detection.

❖ Enabling RLDP Detection on Interface

Command	rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port | block }
Parameter Description	**unidirection-detect**: Indicates unidirectional link detection. **bidirection-detect**: Indicates bidirectional forwarding detection. **loop-detect**: Indicates downlink loop detection. **warning**: Indicate the failure treatment is warning. **shutdown-svi**: Indicate the failure treatment is closing the SVI that the interface is on. **shutdown-port**: Indicates the failure treatment is port violation. **block**: Indicates the failure treatment is disabling learning and forwarding of a port.
Command Mode	Interface configuration mode
Usage Guide	The interfaces include layer-2 switch ports, layer-3 routed ports, layer-2 AP member ports, and layer-3 AP member ports.

❖ Modifying Global RLDP Detection Parameters

Command	rldp {detect-interval *interval* | detect-max *num* | neighbor-negotiation }
Parameter Description	**detect-interval** *interval*: Indicates a detection interval. **detect-max** *num*: Indicates detection times. **neighbor-negotiation**: Indicates neighbor negotiation.
Command	Global configuration mode

Mode	
Usage Guide	Modify all RLDP parameters on all ports when necessary.

❖ Recovering Failed Port

Command	rldp reset
Parameter Description	N/A
Command Mode	Privileged mode
Usage Guide	Recover all failed ports to initialized state and resume detection.

❖ Displaying RLDP State Information

Command	show rldp **[** interface *interface-name* **]**
Parameter Description	*interface-name*: Indicates the interface to display information of.
Command Mode	Privileged mode, global configuration mode, or interface configuration mode
Usage Guide	Display RLDP state information.

Configuration Example

❖ Enabling RLDP Detection in Ring Topology

Scenario Figure 2-4	**As shown in the following figure, the aggregation and access sections are in a ring topology. The STP is enabled on all devices to prevent loop and provide redundancy protection. To avoid a unidirectional or bidirectional link failure resulting in STP failure, RLDP unidirectional and bidirectional link detection is enabled between aggregation devices as well as between an aggregation device and the access device. To avoid loop due to wrong downlink connection of the aggregation devices, enable RLDP downlink loop detection on the downlink ports of the aggregation devices and of the access device. To avoid loop due to wrong downlink connection of the access device, enable RLDP downlink loop detection on the downlink ports of the access device.** ![SW A Gi 2/0/1 — SW B Gi 2/0/1, SW A Gi 2/0/9 and SW B Gi 2/0/9 connected to SW C Gi 0/49 and Gi 0/50, with SW C Gi 0/1 and Gi 0/2]
Configuration Steps	▪ sw A and sw B are aggregation devices, and sw C is an access device. Users connected to sw C. sw A, sw B and sw C are structured in a ring topology, and the STP is enabled on each of them. For STP configuration, refer to relevant configuration guide. ▪ Enable the RLDP on sw A, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port. ▪ Enable the RLDP on sw B, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port. ▪ Enable the RLDP on sw C, enable unidirectional and bidirectional link detection on the two uplink ports, and enable loop detection on the two downlink ports.
A	``` A#configure terminal A(config)#rld p enable A(config)#interface GigabitEthernet 2/0/1 A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port ```

| | ```
A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect
shutdown-port A(config-if-GigabitEthernet 2/0/1)# exit
A(config)#interface GigabitEthernet 2/0/9

A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect
shutdown-port A(config-if-GigabitEthernet 2/0/1)#rldp port
bidirection-detect shutdown-port A(config-if-GigabitEthernet
2/0/1)#rldp port loop-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#exit
``` |
| **B** | Apply the configuration on SW A. |
| **C** | ```
C#configure
terminal
C(config)#rld
p enable
C(config)#interface GigabitEthernet 0/49

C(config-if-GigabitEthernet 0/49)#rldp port unidirection-detect
shutdown-port C(config-if-GigabitEthernet 0/49)#rldp port
bidirection-detect shutdown-port C(config-if-GigabitEthernet 0/49)#
exit
C(config)#interface GigabitEthernet 0/50

C(config-if-GigabitEthernet 0/50)#rldp port unidirection-detect
shutdown-port C(config-if-GigabitEthernet 0/50)#rldp port
bidirection-detect shutdown-port C(config-if-GigabitEthernet
0/50)#exit
C(config)#interface GigabitEthernet 0/1

C(config-if-GigabitEthernet 0/1)# rldp port loop-detect
shutdown-port C(config-if-GigabitEthernet 0/1)#exit
C(config)#interface GigabitEthernet 0/2
C(config-if-GigabitEthernet 0/2)# rldp port loop-detect
shutdown-port C(config-if-GigabitEthernet 0/2)#exit
``` |
| **Verification** | Check the RLDP information on sw A, sw B and sw C. Take sw A for example. |
| **A** | ```
A#show rldp

rldp state      : enable rldp hello interval: 3 rldp max hello       :
rldp local bridge : 00d0.f822.33aa
``` |
| | ```
Interface
GigabitEthernet 2/0/1
port state    :
normal
neighbor bridge :
00d0.f800.51b1 neighbor port
                :
GigabitEthernet 2/0/1
unidirection detect
information:
    action:
    shutdown-port
    state :
``` |

```
                      normal
                  bidirection detect
                      information:
                      action: shutdown-
                      port state :
                      normal


                  Interface
                  GigabitEthernet 2/0/9
                  port state     :
                  normal
                  neighbor bridge :
                  00d0.f800.41b0 neighbor port
                                  :
                  GigabitEthernet 0/49
                  unidirection detect
                  information:
                      action:
                      shutdown-port
                      state :
                      normal
                  bidirection detect
                      information:
                      action: shutdown-
                      port state :
                      normal
                  loop detect
                      information:
                      action:
                      shutdown-port
                      state : normal
```
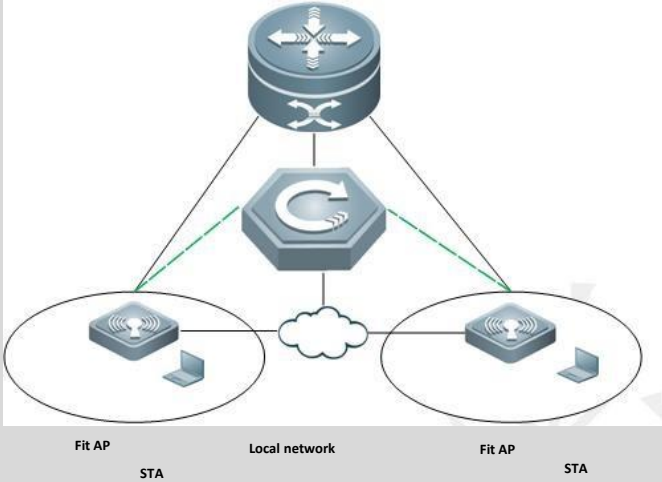
Common Errors

- RLDP functions and private multicast address authentication or TPP are enabled at the same time.

- Neighbor negotiation is not enabled when configuring unidirectional or bidirectional link detection. The RLDP should be enabled on a neighbor device, or otherwise a unidirectional or bidirectional failure will be detected.

- If RLDP detection is configured to be implemented after neighbor negotiation while configuring unidirectional or bidirectional link detection, detection cannot be implemented as no neighbor can be learned due to a link failure. In this situation, you are suggested to recover the link state first.

- You are suggested not to specify the failure treatment as Shutdown SVI under a routed port.

- You are suggested not to specify the failure treatment as Block for a port, on which a loop protection protocol is enabled, for example, the STP.

❖ **Configuring RLDP Loop Detection on Wireless APs**

Scenario Figure 2-5	**As shown in the following figure, a large number of APs exist in the wireless AP scenario. If the RLDP loop detection function is configured and modified on APs one by one, the workload is heavy. The RLDP loop detection configurations can be pushed from the AC device to all online APs (or an independent AP).**
	Fit AP Local network Fit AP STA STA
Configuration Steps	▪ Log in to the AC device and enter the AP configuration mode. ▪ Enable the RLDP loop detection function on the wired ports of the corresponding AP. ▪ Enable the RLDP function on corresponding APs in global configuration mode. ▪ On corresponding APs, configure the recovery time for the RLDP violated port.

A	`A#configure terminal`
	`A(config)#ap-config all`
	`A(config-ap)#exec-cmd mode "int gi 0/1" cmd "rldp port loop-detect shutdown-port" A(config-ap)#exec-cmd mode configure cmd "rldp enable"`
	`A(config-ap)#exec-cmd mode configure cmd "errdisable recovery interval 600"`

Verification	On the AC device, check the RLDP loop detection configurations.

A	`A# show run`
	`!`
	`ap-config all`
	` exec-cmd mode "int gi 0/1" cmd "rldp port loop-detect shutdown-port" exec-cmd mode configure cmd "rldp enable"`
	` exec-cmd mode configure cmd "errdisable recovery interval 600"`
	`!`

Common Errors

▪ When the **exec-cmd** command is executed for interface configuration, the

input of the corresponding AP wired port is incorrect.

- When the RLDP loop detection configurations are modified, the **no exec-cmd** command is not executed to delete the original configurations or the **exec-cmd** command is not re-executed to cancel the configurations.

2.5 Monitoring

Displaying

Description	Command
Displays RLDP state.	**show rldp** [**interface** *interface-name*]

3.1   Overview

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant routing protocol.

VRRP adopts the master-backup design to ensure migration of functions from a Master router to a Backup one when the Master failed, without influencing internal and external data communication or modifying Local Area Network (LAN) configuration. A VRRP group maps multiple routers into a virtual router. VRRP ensures only one router at a moment on behalf of a virtual router transfers packets, which is the elected Master. If the Master fails, one of the Backup routers will replace it. Under VRRP, it seems that a host in a LAN uses only one router and the routing remains functional even when the first-hop router fails.

- VRRP is applicable to LAN scenarios which require the redundancy of routing egresses.

Protocols and Standards

- RFC2338: Virtual Router Redundancy Protocol

- RFC3768: Virtual Router Redundancy Protocol (VRRP)

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

3.2   Applications

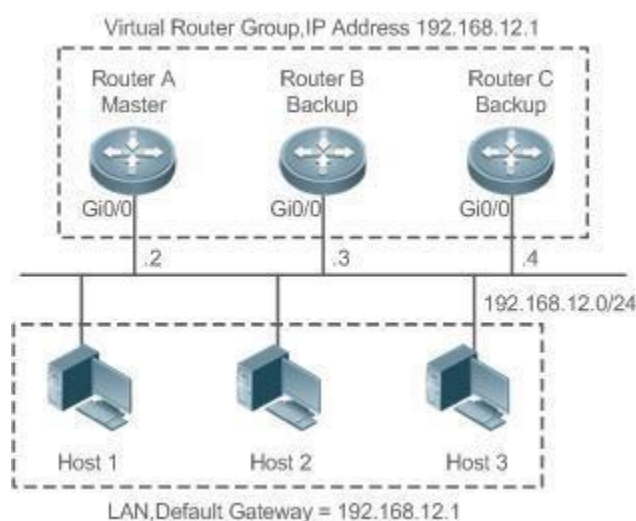| Application	Description
Routing Redundancy	Configure routers in a LAN as one VRRP group to achieve simple routing redundancy.
Load Balancing	Configure routers in a LAN as multiple VRRP groups to achieve traffic load balancing.

3.2.1   Routing Redundancy
Scenario

Configure routers in a LAN as one VRRP group, where hosts take the virtual IP address of this group as the default gateway address.

- Packets from Host 1, Host 2 and Host 3 to other networks are forwarded by the elected Master router (Router A in Figure 3-1).

- If Router A fails, the Master will be re-elected between Router B and

QTECH | www.qtech.ru
МИР ДОСТУПНЕЕ

Router C to forward packets, achieving simple routing redundancy.
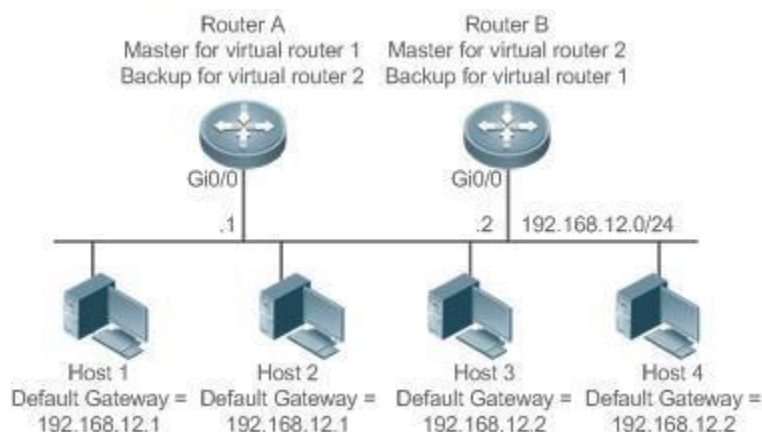
Figure 3-1

Deployment

- Router A, Router B and Router C are connected to the LAN via Ethernet interfaces.

- On Router A, Router B and Router C, VRRP is configured on the Ethernet interfaces connected to the LAN.

- These Ethernet interfaces are in the same VRRP group whose virtual IP address is 192.168.12.1.

- The gateway address for Host 1, Host 2 and Host 3 is the IP address of the VRRP group, namely 192.168.12.1.

3.2.2 Load Balancing
Scenario

Configure routers in a LAN as multiple VRRP groups. Hosts in the LAN take virtual IP addresses of the groups as their gateways, and each router backs up for other routers in different group.

- Packets from Host 1 and Host 2 to other networks with the default gateway address as the virtual IP address of virtual router 1 are forwarded by the Master of virtual router 1 (Router A in Figure 3-2).

- Packets from Host 3 and Host 4 to other networks with the default gateway address as the virtual IP address of virtual router 2 are forwarded by the Master of virtual router 2 (Router B in Figure 3-2).

- Routing redundancy is achieved on Router A and Router B, and the LAN traffic is shared to achieve load balancing. Figure 3-2

Deployment

- Router A and Router B are connected to the LAN via Ethernet interfaces.

- On Router A and Router B, two virtual routers are configured on the Ethernet interfaces connected to the LAN.

- Router A takes the IP address 192.168.12.1 of Ethernet interface Gi0/0 as the IP address of virtual router 1. Thus for virtual router 1, Router A becomes the Master and Router B becomes the Backup.

- Router B takes the IP address 192.168.12.2 of Ethernet interface Gi0/0 as the IP address of virtual router 2. Thus for virtual router 2, Router B becomes the Master and Router A becomes the Backup.

- In the LAN, Host 1 and Host 2 take the IP address 192.168.12.1 of virtual router 1 as the default gateway address, while Host 3 and Host 4 take the IP address 192.168.12.2 of virtual router 2 as the default gateway address.

3.3   Features

Basic Concepts

❖ Virtual Router

A virtual router, also called a VRRP group, is regarded as a default gateway for hosts in a LAN. A VRRP group contains a Virtual Router Identifier (VRID) and a set of virtual IP addresses.

❖ Virtual IP Address

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

❖ IP Address Owner

If a VRRP group has the virtual IP address as that of an Ethernet interface on one real router, the router is regarded as the virtual IP address owner. In such case, the router priority is 255. If the owned Ethernet interface is available, the VRRP group will be in Master state automatically. The IP address owner receives and processes the packets with the destination IP address as that of the virtual router.

❖ **Virtual MAC Address**

The virtual MAC address of a VRRP group is an IEEE 802 MAC address, formatted as **00-00-5E-00-01-{VRID}** with the first five octets assigned and the last two as a group VRID. A VRRP group responds to an Address Resolution Protocol (ARP) request with its virtual MAC address instead of a real MAC address.

❖ **Master Router**

In a VRRP group, only the Master router answers ARP requests and forwards IP packets. If a real router is the IP Address Owner, it becomes the Master router.

❖ **Backup Router**

In a VRRP group, Backup routers only monitor the state of the Master but do not respond to ARP requests or forward IP packets. When the Master fails, Backup routers will take the chance to compete for the position.

❖ **Preemption Mode**

If a VRRP group runs in Preemption mode, a higher priority Backup router will replace the lower priority Master router.
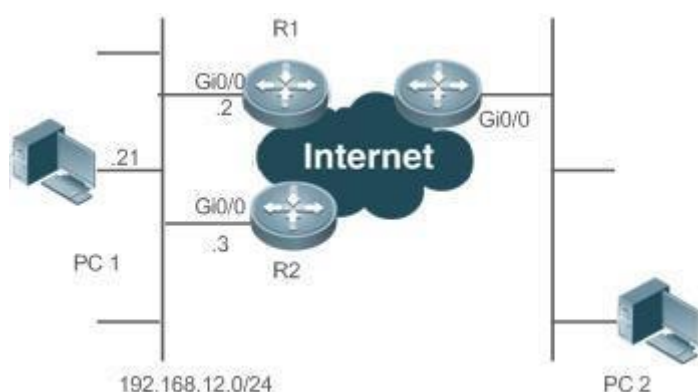
Overview

Feature	Description
VRRP	VRRP achieves redundancy for the default gateways of terminals on a multi-access media (for example, Ethernet). It enables a Backup router to forward packets when the Master router is down, providing transparent routing switch and promoting network service quality.

3.3.1 VRRP

In case that the Master router is faulty, VRRP achieves migration of functions from the Master router to a Backup one without influencing internal and external data communication or modifying LAN configuration.

Working Principle

Figure 3-3 Working Principle of VRRP

❖ **Working Mode of VRRP**

The RFC2338, RFC3768 and RFC5798 protocols define the format and operating mechanism of VRRP packets. Multicast VRRP packets are sent periodically with specified destination addresses by the Master router to advertise normal operation

or for Master election. VRRP allows a router in a LAN to automatically replace the Master who forwards IP packets when the latter fails. This helps achieve hot backup and fault tolerance of IP-based routing as well as ensure communication continuity and reliability for hosts in the LAN. A VRRP group achieves redundancy through multiple real routers. However, only one router acts as the Master to forward packets while the others are Backup routers. Router switching in a VRRP group is completely transparent to hosts in a LAN.

❖ **Master Election Process**

The RFC standards stipulate the master election process as follows:

▪ VRRP provides a simple mechanism for Master election. First, compare the VRRP priorities configured on the interfaces of the routers in a VRRP group. The router with the highest priority is elected as the Master. If these priorities are equal, compare the primary IP addresses of these routers. The router with the biggest IP address is elected as the Master.

▪ After the Master router is elected, the other routers become Backup routers (and enter the **Backup** state) and monitor the state of the master router through the VRRP packets the master router sends. If the master router is operational, it regularly sends VRRP multicast packets known as Advertisement packets to notify the Backup routers of its status. If the Backup routers do not receive such packets within a set period, all of them will enter the Master state. In such case, the previous step of Master election is repeated. In this way, a router with the highest priority will be elected as a new master, achieving VRRP backup.

Once the Master router of a VRRP group is elected, it is responsible to forward packets for hosts in a LAN.

❖ **Communication Process**

The VRRP communication process can be explained by Figure 3-3. The routers R1 and R2 are connected to the LAN segment 192.168.12.0/24 via the VRRP-enabled Ethernet interfaces Gi0/0. Hosts in the LAN take the virtual IP address of the VRRP group as the default gateway address. Only the virtual router is recognized by the hosts. The Master router in the group, however, is unknown. For example, when PC 1 plan to communicate with PC 2, PC 1 sends packets to the default gateway with the virtual IP address; The Master router in the group receives the packets and forwards them to PC 2. In this process, PC 1 only senses the virtual router instead of R1 or R2. The Master router in the group is elected between R1 and R2. When the Master fails, it will be replaced automatically by the other router.

Related Configuration

❖ **Enabling VRRP**

By default, VRRP is disabled on an interface.

In the interface configuration mode, run the **vrrp** *group* **ip** *ipaddress* [**secondary**] or **vrrp** *group* **ipv6** *ipv6-address*

command to set the VRID and virtual
IP address to enable VRRP. VRRP
must be enabled on an interface.

❖ **Configuring the IPv4 VRRP Authentication String**

By default, VRRP is in non-authentication mode.

Run the **vrrp group authentication** *string* command to set an authentication string in MD5 authentication mode or a plain text password in plain text mode for an IPv4 VRRP group. In the plain text authentication mode, a password contains 8 bytes at most.

Members of a VRRP group can communicate with each other only when they are in the same authentication mode. In the plain text authentication mode, all routers in a VRRP group should have the same authentication password. The plain text authentication password cannot guarantee security but only prevents/prompts wrong VRRP configurations.

❖ **Configuring the VRRP Advertisement Interval**

By default, the advertisement interval of the Master router is 1 second.

Run the **vrrp** [**ipv6**] *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* } command to change the interval and timeout times.

When VRRP learning timer is not configured, the same advertisement interval should be set for a VRRP group, otherwise routers in Backup state will discard received VRRP packets.

❖ **Configuring the VRRP Preemption Mode**

By default, a VRRP group operates in the Preemption mode.

To enable the Preemption mode for a VRRP group, run the **vrrp** [**ipv6**] *group* **preempt** [**delay** *seconds*] command. The optional parameter **delay** *seconds* is 0 by default.

If a VRRP group operates in the Preemption mode, a router will become the Mater of the group when it finds that its priority is higher than that of the current Master. If a VRRP group operates in Non-preemption mode, a router will not become the Master even when it finds that its priority is higher than that of the current Master. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group. The optional parameter Delay *Seconds* defines the delay before a backup VRRP router declares its Master identity.

❖ **Enabling the IPv6 VRRP Accept Mode**

By default, the Accept mode is disabled for an IPv6 VRRP group.

To enable the Accept mode, run the **vrrp ipv6** *group* **accept_mode** command.

After the Accept mode is enabled, an IPv6 VRRP virtual router in Master state receives and processes packets with the virtual router IP address as the destination; when the Accept mode is disabled, the virtual router discards such packets except Neighbor Advertisement (NA) packets and Neighbor Solicitation (NS) packets. Besides, an IPv6 VRRP master virtual router in Owner state receives and processes packets with the virtual router IP address as the destination by default no matter whether the Accept mode is configured or not.

❖ **Configuring the VRRP Router Priority**

By default, the router priorities in a VRRP group are all 100.

To adjust the priority, run the **vrrp** [**ipv6**] *group* **priority** *level* command.

If a router in the Preemption mode owns the group's virtual IP address and the highest priority, it becomes the group Master, while the other routers with lower priorities in the group become Backup (or monitoring) routers.

❖ **Configuring the VRRP Tracked Interface**

By default, no interface is tracked by a VRRP group.

To configure such an interface, run the **vrrp** *group* **track** { *interface-type interface-number* | **bfd** *interface-type*

interface-number ipv4-addess } [*priority*] or **vrrp ipv6** group **track** *interface-type interface-number* [*priority*] command.

After an interface is configured for a VRRP group to monitor, the router priority will be adjusted dynamically based on the interface state. Once the interface becomes unavailable, the priority of the router in the group will be reduced by a set value, and another functional and higher priority router in this group will

become the Master.

❖ **Configuring the VRRP Tracked IP Address**

By default, no IP address is tracked by a VRRP group.

To configure such an address, run the **vrrp** *group* **track** *ip-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry**

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

After an IP address is configured for a VRRP group to monitor, the router priority will be adjusted dynamically based on the address accessibility. Once the address is inaccessible (the ping command fails), the priority of the router in the group will be reduced by a set value, and another higher priority router in this group will become the Master.

❖ **Configuring the VRRP Learning Timer**

By default, the learning timer is disabled for a VRRP group.

To enable it, run the **vrrp** [**ipv6**] *group* **timers learn** command.

After the learning timer is configured, a VRRP Backup router learns the advertisement interval of NA packets from the Master. Based on this instead of a locally set interval, the Backup router calculates the interval for determining a failure of the Master. This command achieves the synchronization of advertisement intervals between Backup routers and the Master.

❖ **Configuring the VRRP Group Description**

By default, no description is configured for a VRRP group.

To configure such a string, run the **vrrp** [**ipv6**] *group* **description** *text* command.

A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

❖ **Configuring the VRRP Delay**

By default, no delay is configured for a VRRP group.

To enable it, run the **vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* } command. The two types of delay range from 0 to 60 seconds.

The command configures the delay of starting a VRRP group on an interface. There are two types of VRRP delay: the delay after system startup and the delay after an interface resumes. You may configure them respectively or simultaneously. After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup

or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.

❖ **Configuring the IPv4 VRRP Version**

By default, IPv4 adopts the VRRPv2 standard.

To specify the version for IPv4 VRRP, run the **vrrp** *group* **version** { **2 | 3** } command.

When the parameter value is set to 2, VRRPv2 is adopted; when the parameter value is set to 3, VRRPv3 is adopted.

❖ **Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets**

By default, IPv4 VRRP packets are sent to the first Up Sub VLAN interface of a Super VLAN.

To specify the first Sub VLAN in Up state of a Super VLAN to receive IPv4 VRRP packets, run the vrrp detection-vlan

first-subvlan command; to specify a Sub VLAN, run the vrrp detection-vlan *subvlan-id* command. If VRRP and VRRP Plus are enabled simultaneously on a Super VLAN interface, VRRP packets are sent to all Up interfaces of the Sub VLANs under the Super VLAN.

Both the above configurations reduce VRRP packets and avoid influencing router performance and occupying network bandwidth. Yet the routers constituting an IPv4 VRRP group should be interconnected within the first UP Sub VLAN interface or a specified Sub VLAN of the Super VLAN.

❖ **Configuring the BFD Support for IPv4 VRRP on an Interface**

By default, the Bidirectional Forwarding Detection (BFD) protocol support for VRRP is not enabled on an interface. To enable it, run the vrrp *group* bfd *ip-address* command.
For a Backup router, run this command to correlate an IPv4 VRRP group with BFD without caring the configured IP address. For the Master, as the primary IP address of a Backup router is not known, the router IP address can only be specified by the administrator.

To enable the BFD support, make sure that IP and BFD session parameters are configured on the target interface.

After the BFD support is enabled for a specified IPv4 VRRP group, when the Master fails, a Backup router may detect it within one second.

❖ **Configuring Global IPv4 VRRP BFD**

By default, the VRRP does not adopt the global IPv4 VRRP BFD mode in detecting the state of the Master. To enable global IPv4 VRRP BFD, run the **vrrp bfd** *interface-type interface-number ip-address* command.

After global IPv4 VRRP BFD is enabled, multiple IPv4 VRRP groups may share BFD sessions, achieving fast detection and master-backup failover.

To enable the BFD support, make sure that IP and BFD session parameters are configured on the target interface.

3.4 Configuration

Configuration	Description and Command	
Configuring IPv4 VRRP	(Mandatory) It is used to enable IPv4 VRRP.	
	vrrp *group* **ip** *ipaddress* [**secondary**]	Enables IPv4 VRRP.
	(Optional) It is used to configure IPv4 VRRP parameters.	
	vrrp *group* **authentication** *string*	Configures the IPv4 VRRP authentication string.
	vrrp *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }	Configures the IPv4 VRRP advertisement interval and timeout times.
	vrrp *group* **preempt** [**delay** *seconds*]	Configures the IPv4 VRRP Preemption mode.
	vrrp *group* **priority** *level*	Configures the IPv4 VRRP router priority.
	vrrp *group* **track** { *interface-type interface-number* | **bfd** *interface-type interface-number ipv4-addess* } [*priority*]	Configures the IPv4 VRRP tracked interface.
	vrrp *group* **track** *ip-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]	Configures the IPv4 VRRP tracked IP address.
	vrrp *group* **timers learn**	Configures the IPv4 VRRP learning timer.

	vrrp *group* **description** *text*	Configures the IPv4 VRRP group description.
	vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }	Configures the IPv4 VRRP delay.
	vrrp *group* **version** { **2** | **3** }	Configures the IPv4 VRRP version.
	vrrp detection-vlan {first-subvlan | *subvlan-id*}	Specifies a sub VLAN of a super VLAN to receive the IPv4 VRRP packets.
	vrrp *group* **bfd** *ip-address*	Configures the BFD support for IPv4 VRRP on an Interface.
	vrrp bfd *interface-type interface-number ip-address*	Configures global IPv4 VRRP BFD.
[Configuring IPv6 VRRP](#)	(Mandatory) It is used to enable IPv6 VRRP.	
	vrrp *group* **ipv6** *ipv6-address*	Enables IPv6 VRRP in interface configuration mode.
	(Optional) It is used to configure IPv6 VRRP parameters.	
	vrrp ipv6 *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }	Configures the IPv6 advertisement interval and timeout times.
	vrrp ipv6 *group* **preempt** [**delay** *seconds*]	Configures the IPv6 VRRP Preemption mode.
	vrrp ipv6 *group* **accept_mode**	Enables the Accept mode for an IPv6 VRRP group.
	vrrp ipv6 *group* **priority** *level*	Configures the IPv6 VRRP router priority.

	vrrp ipv6 *group* **track** *interface-type* *interface-number* [*interface–priority*]	Configures the IPv6 VRRP tracked interface.
	vrrp ipv6 *group* **track** { *ipv6-global-address* | { *ipv6-linklocal-address interface-type interface-number* } } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]	Configures the IPv6 VRRP tracked IP address.
	vrrp ipv6 *group* **timers learn**	Configures the IPv6 VRRP learning timer.
	vrrp ipv6 *group* **description** *text*	Configures the IPv6 VRRP group description.
	vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }	Configures the IPv6 VRRP delay.
[Configuring VRRP-MSTP](#)	The configuration is the same as IPv4 VRRP configuration.	

3.4.1 Configuring IPv4 VRRP

Configuration Effect

- Configure a VRRP group on an interface of a specific LAN segment by setting the VRID and virtual IP address.

- Configure multiple VRRP groups on an interface to achieve load balancing and offer more stable and reliable network services.

- Configure the VRRP tracked interfaces to monitor real-time failures, change interface priorities and realize master-backup failover dynamically.

Notes

- To achieve VRRP, the routers in a VRRP group should be configured with the same virtual IPv4 address.

- To achieve mutual backup between multiple IPv4 VRRP groups, configure multiple IPv4 VRRP groups with identical VRRP configuration on different interface and configure different priorities for them so that they act as the master and backup groups mutually.

- Enable VRRP on Layer-3 interfaces.

Configuration Steps

❖ **Enabling IPv4 VRRP**

- By default, IPv4 VRRP is disabled on an interface. You can enable it based on your demand.

❖ **Configuring the IPv4 VRRP Authentication String**

- By default, VRRP is in non-authentication mode. You can enable plain text authentication mode based on your demand.

❖ **Configuring the IPv4 VRRP Advertisement Interval**

- By default, the Master router sends advertisement packets every one second. You can modify the interval based on your demand.

❖ **Configuring the IPv4 VRRP Preemption Mode**

- By default, a VRRP group operates in Preemption mode with a zero-second delay.

❖ **Configuring the IPv4 VRRP Router Priority**

- The default router priority for a VRRP group is 100. You can modify the priority based on your demand.

❖ **Configuring the IPv4 VRRP Tracked Interface**

- By default, an IPv4 VRRP group monitors no interface and the value of priority change is 10. To achieve fault monitoring through interface monitoring, please configure this item.

❖ **Configuring the IPv4 VRRP Learning Timer**

- By default, the learning timer is disabled for a VRRP group. Enable this function if the Backup routers need to learn the Master's advertisement interval.

❖ **Configuring the IPv4 VRRP Group Description**

- By default, no description is configured for a VRRP group. To distinguish VRRP groups clearly, configure descriptions.

❖ **Configuring the IPv4 VRRP Delay**

- By default, the IPv6 VRRP delay is not configured. To guarantee an effective non-preemption mode, configure the delay.

❖ **Configuring the IPv4 VRRP Version**

- By default, IPv4 adopts the VRRPv2 standard. To change it, use the corresponding command.

QTECH
МИР ДОСТУПНЕЕ   www.qtech.ru

❖ **Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets**

▪ By default, IPv4 VRRP packets are only sent to the first **UP** Sub VLAN interface of a Super VLAN, but you may configure a specific Sub VLAN.

❖ **Configuring the BFD Support for IPv4 VRRP on an Interface**

▪ By default, the BFD support is not configured on an interface. To configure it, use the corresponding command.

❖ **Configuring Global IPv4 VRRP BFD**

▪ By default, global IPv4 VRRP BFD is not enabled. To implement it, use the corresponding command.

Verification

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

Related Commands

❖ **Enabling IPv4 VRRP**

Command	vrrp *group* ip *ipaddress* [secondary]
Parameter Description	*group*: Indicates the VRID of a VRRP group, the range of which varies with product models. *ipaddress*: Indicates the IP address of a VRRP group. **secondary**: Indicates the secondary IP address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	If no virtual IP address is specified, routers cannot join a VRRP group. If no secondary IP address is applied, the configured IP address will be the primary IP address of a VRRP group.

❖ Configuring the IPv4 VRRP Authentication String

Command	vrrp *group* authentication *string*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *string*: Indicates the authentication string of a VRRP group (a plain text password consists of 8 bytes at most).
Command Mode	Interface configuration mode

| Usage Guide | In a VRRP group, the same authentication password should be configured for routers. The plain text authentication password cannot guarantee security but only prevents/prompts wrong VRRP configurations. This command is only applicable to VRRPv2 instead of VRRPv3. Authentication is abolished for VRRPv3 (IPv4 VRRP and IPv6 VRRP) packets. If VRRPv2 is chosen for an IPv4 VRRP group, the command is effective; if VRRPv3 is chosen, the command is ineffective. |

❖ Configuring the IPv4 VRRP Advertisement Interval

Command	vrrp *group* timers advertise **{ *advertise-interval* |** csec *centisecond-interval* **}**
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group (unit: second). **csec** *centisecond-interval:* An interval for a master router in a backup group to send VRRP packets. It is an integer from 50 to 99. The unit is centisecond. No default value is provided. The command is only effective for VRRPv3 packets. If it is configured for VRRPv2 packets, the default interval is one second.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the Master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority and other information. According to the RFC standards, if an IPv4 VRRP group adopts VRRPv3 for sending multicast packets, the maximum advertisement interval is 40 seconds. Therefore, if the interval is set longer than 40 seconds, this maximum interval will be applied, though the configuration is effective.

❖ Configuring the IPv4 VRRP Preemption Mode

Command	vrrp *group* preempt **[** delay *seconds* **]**
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.
Command Mode	Interface configuration mode

Usage Guide	If a VRRP group runs in Preemption mode, a higher priority router will take the place of the lower priority Master. If a VRRP group runs in Non-preemption mode, a router with the priority higher than that of the Master remains Backup. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group.

❖ Configuring the IPv4 VRRP Router Priority

Command	vrrp *group* priority *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of an interface in a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the VRRP router priority.

❖ Configuring the IPv4 VRRP Tracked Interface

Command	vrrp *group* track { *interface-type interface-number*	bfd *interface-type interface-number ipv4-addess* } [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. **bfd** *interface-type interface-number ipv4-address*: A specified adjacent IP address tracked through BFD. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	A tracked interface must be a routable Layer-3 logic interface (for example, a Routed port, an SVI interface,
	a Loopback interface, or a Tunnel interface). The priority of the router owns the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

❖ Configuring the IPv4 VRRP Tracked IP Address

Command	vrrp *group* track *ipv4-address* [interval *interval-value*] [timeout *timeout-value*] [retry *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv4-addres*: Indicates the IPv4 address to be tracked. ***interval*** *interval-value*: Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. ***timeout*** *timeout-value*: Indicates the probe timeout of waiting for responses. If no response is received when the timeout is up, it is regarded that the destination is inaccessible. The unit is second. Unless configured manually, the value is 1 second by default. **retry** *retry-value*: Indicates the probe retries. If the probe packet is sent continually for retry-value times but no response is received, it is regarded that the destination is inaccessible. The unit is times. Unless configured, the value is 3 times by default. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv4 address for an IPv4 VRRP group. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

❖ Configuring the IPv4 VRRP Learning Timer

Command	vrrp *group* timers learn
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	Once the learning timer is enabled on a VRRP router, a Backup router learns the advertisement interval of the Master during the timer. Based on this, the Backup router calculates the interval for determining the Master router as failed instead of using the locally configured advertisement interval. This command achieves synchronization with the learning timer between the Master and

	Backup routers.

❖   Configuring the IPv4 VRRP Group Description

Command	vrrp *group* description *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

❖   Configuring the IPv4 VRRP Delay

Command	vrrp delay **{ minimum *min-seconds*	reload *reload-seconds* }**
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. The two types of delay share a value range of 0 to 60 seconds. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.

❖   Configuring the IPv4 VRRP Version

Command	vrrp *group* version **{ 2	3 }**
Parameter Description	**2**: Indicates VRRPv2. **3**: Indicates VRRPv3.
Command Mode	Interface configuration mode

Usage Guide	Considering the compatibility between VRRPv2 and VRRPv3, specify a standard for IPv4 VRRP based on the actual network condition. VRRPv2 is developed in RFC3768, while VRRPv3 is described in RFC5798. This command is only applicable to IPv4 VRRP.

❖ Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets

Command	vrrp detection-vlan {first-subvlan	*subvlan-id*}
Parameter Description	**first-subvlan**: Sends IPv4 VRRP packets only to the first UP Sub VLAN interface in a Super VLAN. *subvlan-id*: Sends IPv4 VRRP packets to a specified Sub VLAN.
Command Mode	Interface configuration mode
Usage Guide	This command is used to specify a Sub VLAN of a Super VLAN to receive the IPv4 VRRP packets. IPv4 VRRP packets are sent in a Super VLAN using the following three methods. Packets are sent to the first UP Sub VLAN interface in a Super VLAN, or to a specified Sub VLAN interface in a Super VLAN, or to all the Sub VLAN interfaces in a Super VLAN. If VRRP and VRRP Plus are enabled simultaneously on a Super VLAN interface, VRRP packets are sent to all Up interfaces of the Sub VLANs under the Super VLAN. This command is configured on a VLAN interface and effective only to Super VLAN interfaces.

❖ Configuring the BFD Support for IPv4 VRRP on an Interface

Command	vrrp *group* bfd *ip-address*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ip-address*: Indicates the interface IP address.
Command Mode	Interface configuration mode
Usage Guide	For a Backup router, run this command to correlate an IPv4 VRRP group with BFD without caring the configured IP address. For the Master, as the primary IP address of a Backup router is not known, the router IP address can only be specified by the administrator. If global IPv4 VRRP BFD is configured, this configuration cannot be performed. To enable the BFD support, make sure that IP and BFD session parameters are configured on the target interface.

❖ Configuring Global IPv4 VRRP BFD

Command	vrrp bfd *interface-type interface-number ip-address*
Parameter Description	*interface-type interface-number*: Indicates interface type and ID. *ip-address*: Indicates the interface IP address.
Command Mode	Global configuration mode
Usage Guide	If global IPv4 VRRP BFD is configured, the configured BFD support will be deleted. To enable the BFD support, make sure that IP and BFD session parameters are configured on the target interface. A global IPv4 VRRP BFD session is only applicable to an IPv4 VRRP group consisting of two routers.

Configuration Example

❖ Configuring an IPv4 VRRP Group and Tracked Interface

Scenario Figure 3-4	
Configuration Steps	▪ The cluster of Work Station A and Work Station B (192.168.201.0/24) uses the virtual IP address 192.168.201.1 of the VRRP group constituted by the routers R1 and R2 as the gateway address to communicate with Work Station B (192.168.12.0 /24). ▪ GigabitEthernet 2/1 on R1 is configured as the tracked interface.

	· No VRRP but an ordinary routing function is configured on R3.

R3	R3#configure terminal R3(config)#interface GigabitEthernet 0/0
	
	// The command "no switchport" is only required for
	a switch. R3(config-if-GigabitEthernet 0/0)#no
	switchport
	R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217
	255.255.255.0 R3(config-if-GigabitEthernet 0/0)#exit
	
	R3(config)#interface GigabitEthernet 1/1
	
	// The command "no switchport" is only required for
	a switch. R3(config-if-GigabitEthernet 1/1)#no
	switchport
	R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0
	R3(config-if-GigabitEthernet 1/1)#exit
	
	R3(config)#interface GigabitEthernet 2/1
	
	// The command "no switchport" is only required for a switch.
	R3(config-if-GigabitEthernet 2/1)#no switchport
	
	R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61
	255.255.255.0 R3(config-if-GigabitEthernet 2/1)#exit
	R3(config)#router ospf
	
	R3(config-router)#network 202.101.90.0 0.0.0.255 area 10
	
	R3(config-router)#network 192.168.12.0 0.0.0.255 area 10
	
	R3(config-router)#network 60.154.101.0 0.0.0.255 area 10

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

R2	R2#configure terminal R2(config)#interface GigabitEthernet 0/0
	R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0
	R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
	R2(config-if-GigabitEthernet 0/0)#vrrp 1 version 3
	R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3 R2(config-if-GigabitEthernet 0/0)#exit R2(config)#interface GigabitEthernet 1/1 // The command "no switchport" is only required for a switch.
	R2(config-if-GigabitEthernet 1/1)#no switchport
	R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0 R2(config-if-GigabitEthernet 1/1)#exit
	R2(config)#router ospf
	R2(config-router)#network 60.154.101.0 0.0.0.255 area 10
	R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
Verification	Run the **show vrrp** command to verify the configuration.
	▪ Check whether R1, which acts as the Master, reduces its VRRP priority from 120 to 90 when GigabitEthernet2/1 connected to the Wide Area Network (WAN) is unavailable. If yes, R2 becomes the Master.
	▪ Check whether R1 resumes its VRRP priority from 30 to 120 when GigabitEthernet 2/1 connected to
	the WAN recovers. If yes, R1 is re-elected as the Master.
R1	R1#show vrrp
	GigabitEthernet 0/0 - Group 1 State is Master
	Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101
	Advertisement interval is 3 sec Preemption is enabled
	min delay is 0 sec Priority is 120
	Master Router is 192.168.201.217 (local), priority is 120 Master Down interval is 10.59 sec
	Tracking state of 1 interface, 1 up:
	Up GigabitEthernet 2/1 priority decrement=30
R2	R2#show vrrp
	GigabitEthernet 0/0 - Group 1 State is Backup
	Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec
	Preemption is enabled
	min delay is 0 sec Priority is 100
	Master Router is 192.168.201.217 , priority is 120 Master Advertisement interval is 3 sec
	Master Down interval is 10.82 sec

Common Errors

- Different virtual IP addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.

- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.

- Different VRRP versions are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.

- For VRRPv2, the Ethernet interfaces of the routers in a VRRP group are all in plain text authentication mode but inconsistent in authentication strings, resulting in multiple Master routers in the group.

Configuration Example

❖ **Configuring Multiple IPv4 VRRP Groups**

Scenario Figure 3-5	
Configuration Steps	▪ The user workstation cluster (192.168.201.0/24) uses the backup group constituted by the routers R1 and R2. The gateway for partial workstations (A for example) points to the virtual IP address 192.168.201.1 of the backup group 1, while that for other partial workstations (C for example) points to the virtual IP address 192.168.201.2 of the backup group 2. IPv4 multicast routing is enabled on all the routers. ▪ R1 acts as the master router in the group 2 and as a backup router in the group 1. ▪ R2 acts as a backup router in the group 2 and as a master router in the group 1.

R3	R3#configure terminal R3(config)#interface GigabitEthernet 0/0
	// The command "no switchport" is only required for a switch. R3(config-if-GigabitEthernet 0/0)#no switchport
	R3(config-if-GigabitEthernet 0/0)#ip address 192.168.12.217 255.255.255.0 R3(config-if-GigabitEthernet 0/0)#exit
	R3(config)#interface GigabitEthernet 1/1
	// The command "no switchport" is only required for a switch. R3(config-if-GigabitEthernet 1/1)#no switchport
	R3(config-if-GigabitEthernet 1/1)#ip address 60.154.101.5 255.255.255.0 R3(config-if-GigabitEthernet 1/1)#exit
	R3(config)#interface GigabitEthernet 2/1
	// The command "no switchport" is only required for a switch. R3(config-if-GigabitEthernet 2/1)#no switchport
	R3(config-if-GigabitEthernet 2/1)#ip address 202.101.90.61 255.255.255.0 R3(config-if-GigabitEthernet 2/1)#exit
	R3(config)#router ospf
	R3(config-router)#network 202.101.90.0 0.0.0.255 area 10
	R3(config-router)#network 192.168.12.0 0.0.0.255 area 10
	R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
R1	R1#configure terminal R1(config)#interface GigabitEthernet 0/0
	R1(config-if-GigabitEthernet 0/0)#ip address 192.168.201.217 255.255.255.0
	R1(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
	R1(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
	R1(config-if-GigabitEthernet 0/0)#vrrp 2 priority 120
	R1(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3
	R1(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2
	R1(config-if-GigabitEthernet 0/0)#vrrp 2 track GigabitEthernet 2/1 30 R1(config-if-GigabitEthernet 0/0)#exit
	R1(config)#interface GigabitEthernet 2/1
	R1(config-if-GigabitEthernet 2/1)#ip address 202.101.90.63 255.255.255.0 R1(config-if-GigabitEthernet 2/1)#exit
	R1(config)#router ospf
	R1(config-router)#network 202.101.90.0 0.0.0.255 area 10
	R1(config-router)#network 192.168.201.0 0.0.0.255 area 10

R2	R2#configure terminal R2(config)#interface GigabitEthernet 0/0
	R2(config-if-GigabitEthernet 0/0)#ip address 192.168.201.213 255.255.255.0
	R2(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.201.1
	R2(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 3
	R2(config-if-GigabitEthernet 0/0)#vrrp 1 priority 120
	R2(config-if-GigabitEthernet 0/0)#vrrp 2 ip 192.168.201.2
	R2(config-if-GigabitEthernet 0/0)#vrrp 2 timers advertise 3 R2(config-if- GigabitEthernet 0/0)#exit R2(config)#interface GigabitEthernet 1/1
	R2(config-if-GigabitEthernet 1/1)#ip address 60.154.101.3 255.255.255.0 R2(config-if-GigabitEthernet 1/1)#exit
	R2(config)#router ospf
	R2(config-router)#network 60.154.101.0 0.0.0.255 area 10
	R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
Verification	Run the **show vrrp** command to verify the configuration. ▪ Check whether R1, which acts as a master router in the group 2, reduces its VRRP group priority from 30 to 90 when it finds that the interface GigabitEthernet 2/1 connected to a WAN is unavailable. If yes, R2 in the group 2 becomes a master router. ▪ Check whether R1 increases its VRRP group priority from 30 to 120 when it finds the interface GigabitEthernet 2/1 connected to a WAN becomes available again. If yes, R1 becomes a master router again in the group 2.
R1	R1#show vrrp
	GigabitEthernet 0/0 - Group 1 State is Backup
	Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec
	Preemption is enabled min delay is 0 sec
	Priority is 100
	Master Router is 192.168.201.213 , priority is 120 Master Advertisement interval is 3 sec
	Master Down interval is 10.82 sec GigabitEthernet 0/0 - Group 2
	State is Master
	Virtual IP address is 192.168.201.2 configured Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec
	Preemption is enabled min delay is 0 sec
	Priority is 120
	Master Router is 192.168.201.217 (local), priority is 120 Master Advertisement interval is 3 sec
	Master Down interval is 10.59 sec Tracking state of 1 interface, 1 up:
	up GigabitEthernet 2/1 priority decrement=30

R2	R2#show vrrp GigabitEthernet 0/0 - Group 1 State is Master Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101
	Advertisement interval is 3 sec Preemption is enabled **min delay is 0 sec Priority is 120** **Master Router is 192.168.201.213 (local), priority is 120 Master Advertisement interval is 3 sec** **Master Down interval is 10.59 sec GigabitEthernet 0/0 - Group 2** **State is Backup** **Virtual IP address is 192.168.201.2 configured Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec** **Preemption is enabled min delay is 0 sec** **Priority is 100** **Master Router is 192.168.201.217 , priority is 120 Master Advertisement interval is 3 sec** **Master Down interval is 10.82 sec**

Common Errors

- Different virtual IP addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.

- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.

- Different VRRP versions are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.

- For VRRPv2, the Ethernet interfaces of the routers in a VRRP group are all in plain text authentication mode but inconsistent in authentication strings, resulting in multiple Master routers in the group.

3.4.2   Configuring IPv6 VRRP
Configuration Effect

- Configure an IPv6 VRRP group on an interface of a specific LAN segment by setting the VRID and virtual IPv6 address.

- Configure multiple IPv6 VRRP groups on an interface to achieve load balance and achieve more stable and reliable network services.

- Configure the VRRP tracked interfaces to monitor real-time failures, change interface priorities and realize master-backup failover

dynamically.

Notes

- To achieve VRRP, the routers in a VRRP group should be configured with the same virtual IPv6 address.

- To achieve mutual backup for multiple IPv6 VRRP backup groups, you need to configure multiple IPv6 VRRP groups with identical VRRP configuration on an interface and configure different priorities for them to make routers master and backup mutually.

- VRRP must be enabled on Layer-3 interfaces.

Configuration Steps

❖ **Enabling IPv6 VRRP in Interface Configuration Mode**

- By default, IPv6 VRRP is not enabled on an interface. You can enable it based on your demand.

❖ **Configuring the IPv6 VRRP Advertisement Interval**

- By default, the Master router sends advertisement packets every one second. You can modify the interval based on your demand.

❖ **Configuring the IPv6 VRRP Preemption Mode**

- By default, a VRRP group operates in Preemption mode with a zero-second delay.

❖ **Enabling the Accept Mode for an IPv6 VRRP Group**

- By default, the Accept mode is disabled for an IPv6 VRRP group. To require an IPv6 VRRP VRRP group in Master state to receive and process packets with the destination IP address as that of the virtual router, enable Accept mode.

❖ **Configuring the IPv6 VRRP Router Priority**

- The default router priority for a VRRP group is 100. You can modify the priority based on your demand.

❖ **Configuring the IPv6 VRRP Tracked Interface**

- By default, no tracked interface is configured. You can modify the interval based on your demand.

❖ **Configuring the IPv6 VRRP Tracked IP Address**

- By default, no tracked IPv6 address is configured and the value of priority change is 10. You can configure this function based on your demand.

- By default, the learning timer is disabled for a VRRP group. Enable this function if the Backup routers need to learn the Master's advertisement interval.

❖ **Configuring the IPv6 VRRP Group Description**

- By default, no description is configured for a VRRP group. To distinguish VRRP groups clearly, configure descriptions.

❖ **Configuring the IPv4 VRRP Delay**

- By default, the IPv6 VRRP delay is not configured. To guarantee an effective non-preemption mode, configure the delay.

Verification

- Run the **show ipv6 vrrp** command to verify the configuration.

Related Commands

❖ **Enabling IPv6 VRRP**

Command	vrrp *group* ipv6 *ipv6-address*
Parameter Description	*group*: Indicates the VRID of a VRRP group, the range of which varies with product models. *ipv6-address*: Indicates the IPv6 address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	IPv6 VRRP groups and IPv4 VRRP groups share a VRID range from 1 to 255. One VRID is applicable to an IPv4 VRRP group and an IPv6 VRRP group at the same time. The first configured address should be a link-local address, which can be deleted only after other virtual addresses.

❖ Configuring the IPv6 VRRP Advertisement Interval

Command	vrrp ipv6 *group* timers advertise **{ *advertise-interval* | csec *centisecond-interval* }**
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group (unit: second). *csec centisecond-interval:* An interval for a master router in a backup group to send VRRP packets. It is an integer from 50 to 99. The unit is centisecond. No default value is provided. The command is only effective for VRRPv3 packets. If it is configured for VRRPv2 packets, the default interval is one second.
Command Mode	Interface configuration mode

Usage Guide	If a router is elected as the Master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority and other information.
	According to the RFC standards, if an IPv6 VRRP group adopts VRRPv3 for sending multicast packets, the maximum advertisement interval is 40 seconds. Therefore, if the interval is set longer than 40 seconds, this maximum interval will be applied, though the configuration is effective.
Command	**vrrp ipv6** *group* **preempt** [**delay** *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.
Command Mode	Interface configuration mode
Usage Guide	If a VRRP group runs in Preemption mode, a higher priority router will take the place of the lower priority Master. If a VRRP group runs in Non-preemption mode, a router with the priority higher than that of the Master remains Backup. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group.

❖ Enabling the Accept Mode for an IPv6 VRRP Group

Command	vrrp ipv6 *group* accept_mode
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	By default, an IPv6 VRRP group in **Master** state is not permitted to receive packets with the destination IPv6 address as that of the VRRP group. However, it receives NA and NS packets no matter whether Accept mode is configured. Besides, the IP Address Owner in Master state receives and processes the packets with the destination IPv6 address as that of the VRRP group no matter whether Accept mode is configured or not.

❖ Configuring the IPv6 VRRP Router Priority

Command	vrrp ipv6 *group* priority *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of a VRRP router.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the VRRP router priority.

❖ Configuring the IPv6 VRRP Tracked Interface

Command	vrrp ipv6 *group* track *interface-type interface-number* [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	A tracked interface must be a routable Layer-3 logic interface (for example, a Routed port, an SVI interface, a Loopback interface, or a Tunnel interface). The priority of the router owns the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

❖ Configuring the IPv6 VRRP Tracked IP Address

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

Parameter Description	*group*: Indicates the VRID of a VRRP group.
	ipv6-global-addres: Indicates the IPv6 global unicast address.
	ipv6-linklocal-address: Indicates the IPv6 link-local address.
	interface-type interface-number: Indicates the interface to be tracked.
	interval *interval-value*: Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. **timeout** *timeout-value*: Indicates the probe timeout of waiting for responses. If no response is received when the timeout is up, it is regarded that the destination is inaccessible. The unit is second. Unless configured manually, the value is 1 second by default. **retry** *retry-value*: Indicates the probe retries. If the probe packet is sent continually for *retry-value* times but no response is received, it is regarded that the destination is inaccessible. The unit is times. Unless configured, the value is 3 times by default. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv6 address for an IPv6 VRRP group. If the host IP address being tracked is a link-local address, specify a network interface. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

❖ Configures the IPv6 VRRP Learning Timer

Command	vrrp ipv6 *group* timers learn
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	Once the learning timer is enabled on a VRRP router, a Backup router learns the advertisement interval of the Master during the timer. Based on this, the Backup router calculates the interval for determining the Master router as failed instead of using the locally configured advertisement interval. This command achieves synchronization with the learning timer between the Master and

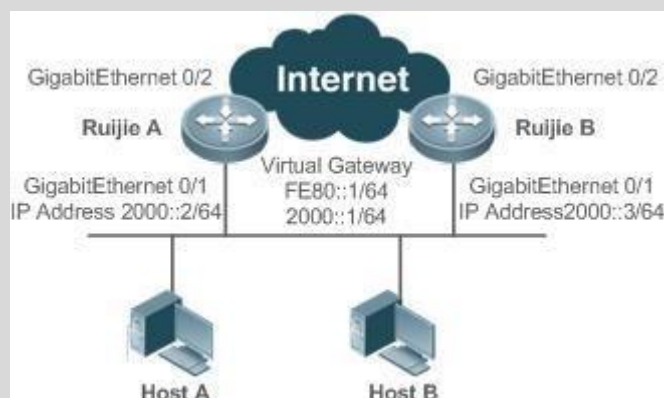|	Backup routers.

❖ Configuring the IPv6 VRRP Group Description

Command	vrrp ipv6 *group* description *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

❖ Configuring the IPv4 VRRP Delay

Command	vrrp delay **{** minimum *min-seconds* **|** reload *reload-seconds* **}**
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. The two types of delay share a value range of 0 to 60 seconds. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.

Configuration Example

❖ Configuring an IPv6 VRRP Group and Tracked Interface

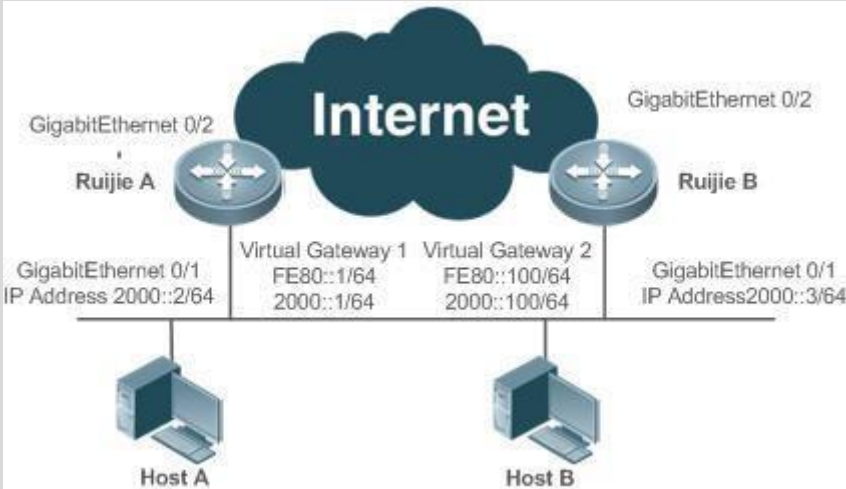| Scenario Figure 3-6	
Configuration Steps	▪ Host A and Host B access the Internet resources through the default gateway 2000::1/64. ▪ QTECH A and QTECH B belong to the IPv6 VRRP group 1, and their virtual addresses are 2000::1/64 and FE80::1 respectively. ▪ QTECH A tracks the interface GigabitEthernet 0/2 connected to the Internet. When GigabitEthernet 0/2 is unavailable, QTECH A reduces its priority and QTECH B acts as a gateway.
QTECHA	`QTECHA#configure terminal`

	`QTECHA(config)#interface  GigabitEthernet  0/1  QTECHA(config-if-GigabitEthernet 0/1)#no switchport`
	
	`QTECHA(config-if-GigabitEthernet  0/1)#ipv6  address  2000::2/64 QTECHA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 QTECHA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1`
	
	`QTECHA(config-if-GigabitEthernet  0/1)#vrrp  ipv6  1  priority  120 QTECHA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3`
	
	`QTECHA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 track GigabitEthernet 0/2 50`
	
	`QTECHA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode`

QTECHB	`QTECHB#configure terminal QTECHB(config)#interface GigabitEthernet 0/1`
	
	`QTECHB(config-if-GigabitEthernet  0/1)#no  switchport  QTECHB(config-if-GigabitEthernet  0/1)#ipv6  address  2000::3/64  QTECHB(config-if-GigabitEthernet  0/1)#vrrp  1  ipv6  FE80::1  QTECHB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1`
	
	`QTECHB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100`
	
	`QTECHB(config-if-GigabitEthernet  0/1)#vrrp  ipv6  1  timers  advertise  3 QTECHB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode`

Verification	Run the **show vrrp** command to verify the configuration.
	▪ Check whether QTECH A, which acts as the Master router, reduces its VRRP group priority from 120 to 70 when it finds that the interface GigabitEthernet 0/2 connected to WAN is unavailable. If yes, QTECH B becomes the Master.
	▪ Check whether QTECH A increases its VRRP group priority from 50 to 120 when it finds the interface GigabitEthernet 0/2 connected to WAN becomes available again. If yes, QTECH A becomes the Master again.
| QTECHA | ```
QTECHA#show ipv6 vrrp 1 GigabitEthernet 0/1 - Group 1
State is Master
Virtual IPv6 address is as follows: FE80::1
2000::1
Virtual MAC address is 0000.5e00.0201
``` |
| | ```
Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled
min delay is 0 sec Priority is 120
Master Router is FE80::1234 (local), priority is 120 Master Advertisement interval is 3 sec
Master Down interval is 10.59 sec Tracking state of 1 interface, 1 up:
up GigabitEthernet 0/2 priority decrement=50
``` |
| QTECHB | ```
QTECHB#show ipv6 vrrp 1 GigabitEthernet 0/1 - Group 1
State is Backup
Virtual IPv6 address is as follow: FE80::1
2000::1
Virtual MAC address is 0000.5e00.0201 Advertisement interval is 3 sec Accept_Mode is enabled
Preemption is enabled min delay is 0 sec
Priority is 100
   Master Router is FE80::1234,
   priority is 120 Master
   Advertisement interval is 3
   sec Master Down interval is
   10.82 sec
``` |

Common Errors

- Different virtual IPv6 addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.

- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.

Configuration Example

❖ **Multiple VRRP Backup Groups (under IPv6)**

Scenario Figure 3-7	
Configuration Steps	▪ Host A and Host B access the Internet resources through the gateways 2000::1/64 and 2000::100/64 respectively. ▪ QTECH A and QTECH B belong to the IPv6 VRRP group 1, and their virtual addresses are 2000::1/64 and FE80::1 respectively. ▪ QTECH A and QTECH B belong to the backup group 2 of a virtual IPv6 router, and their virtual addresses are 2000::100/64 and FE80::100 respectively. ▪ QTECH A and QTECH B act as gateways and forward flows, being a backup router to each other.
QTECHA	QTECHA#configure terminal QTECHA(config)#interface GigabitEthernet 0/1 QTECHA(config-if-GigabitEthernet 0/1)#no switchport QTECHA(config-if-GigabitEthernet 0/1)#ipv6 address 2000::2/64 QTECHA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 QTECHA(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1 QTECHA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 120 QTECHA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3 QTECHA(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode QTECHA(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100 QTECHA(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100 QTECHA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 100 QTECHA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3 QTECHA(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode

QTECHB	`QTECHB#configure terminal QTECHB(config)#interface GigabitEthernet 0/1` `QTECHB(config-if-GigabitEthernet 0/1)#no switchport QTECHB(config-if-GigabitEthernet 0/1)#ipv6 address 2000::3/64 QTECHB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 QTECHB(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1` `QTECHB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100 QTECHB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3 QTECHB(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode QTECHB(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100 QTECHB(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100`  `QTECHB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 120`  `QTECHB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3 QTECHB(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode`
Verification	Run the **show vrrp** command to verify the configuration.

QTECHA	`QTECHA#show ipv6 vrrp GigabitEthernet 0/1 - Group 1`
	
	`State is Master`
	
	`Virtual IPv6 address is as follows:`
	
	`FE80::1 2000::1`
	
	`Virtual MAC address is 0000.5e00.0201 Advertisement interval is 3 sec Accept_Mode is enabled`
	
	`Preemption is enabled min delay is 0 sec`
	
	`Priority is 120`
	
	`Master Router is FE80::1234 (local), priority is 120 Master Advertisement interval is 3 sec`
	
	`Master Down interval is 10.59 sec`

	`GigabitEthernet 0/1 - Group 2 State is Backup`
	
	`Virtual IPv6 address is as follows: FE80::100`
	
	`2000::100`
	
	`Virtual MAC address is 0000.5e00.0202 Advertisement interval is 3 sec Accept_Mode is enabled`
	
	`Preemption is enabled min delay is 0 sec`
	
	`Priority is 100`
	
	`Master Router is FE80::5678, priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec`

| QTECHB | QTECHB#show ipv6 vrrp GigabitEthernet 0/1 - Group 1
State is Backup

Virtual IPv6 address is as follow: FE80::1
2000::1

Virtual MAC address is 0000.5e00.0201 Advertisement interval is 3 sec Accept_Mode is enabled
Preemption is enabled min delay is 0 sec
Priority is 100

   Master Router is FE80::1234,
   priority is 120 Master
   Advertisement interval is 3
   sec Master Down interval is
   10.82 sec
GigabitEthernet 0/1 - Group 2

State is Master
Virtual IPv6 address is as follows: FE80::100
2000::100

Virtual MAC address is 0000.5e00.0202 Advertisement interval is 3 sec Accept_Mode is enabled
Preemption is enabled min delay is 0 sec
Priority is 120

Master Router is FE80::5678(local), priority is 120 Master Advertisement interval is 3 sec
Master Down interval is 10.59 sec |

Common Errors

- Different virtual IPv6 addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.
- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.

3.4.3 Configuring VRRP-MSTP
Configuration Effect

- Link-level and gateway-level backup are achieved and network robustness is improved greatly when MTSP and VRRP are applied simultaneously.

Notes

- configure the routers in a VRRP backup group with the same virtual IPv4 address.
- Enabled VRRP on a Layer 3 interface.

www.qtech.ru

Configuration Steps

❖ **Enabling IPv4 VRRP**

▪ By default, IPv4 VRRP is not enabled on an interface. To enable IPv4 VRRP, please configure this item.

❖ **Configuring the IPv4 VRRP Authentication String**

▪ By default, VRRP is in a non-authentication mode. To enable plain text password authentication for VRRP, please configure this item.

❖ **Configuring the IPv4 VRRP Advertisement Interval**

▪ By default, a master router sends VRRP GWADV packets at an interface of one second. To manually set a value, please configure this item.

❖ **Configuring the IPv4 VRRP Preemption Mode**

▪ By default, VRRP groups work in the preemption mode with zero-second delay.

❖ **Configuring the IPv4 VRRP Router Priority**

▪ The default router priority for a VRRP group is 100. You can modify the priority based on your demand.

❖ **Configuring the IPv4 VRRP Tracked Interface**

▪ By default, an IPv4 VRRP group monitors no interface. To achieve fault monitoring through monitoring an interface, please configure this item.

❖ **Configuring the IPv4 VRRP Learning Timer**

▪ By default, timed learning is not enabled for a VRRP backup group. To enable backup routers to learn the VRRP GWADV packets from a master router, please configure this item.

❖ **Configuring the IPv4 VRRP Group Description**

▪ By default, no description is configured for a VRRP group. To distinguish VRRP groups conveniently, please configure this item.

❖ **Configuring the IPv4 VRRP Delay**

▪ By default, the VRRP delay for a VRRP group is not configured. Configure the delay to guarantee a stable transition from Non-preemption mode to Preemption mode.

❖ **Configuring the IPv4 VRRP Version**

▪ By default, the VRRPv2 standard is adopted for IPv4 VRRP packets. To modify it manually, please configure this item.

❖ **Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets**

- By default, IPv4 VRRP packets are only sent to the first UP Sub VLAN interface in a Super VLAN, but you may configure a specific Sub VLAN interface to send such packets.

❖ **Configuring the BFD Support for IPv4 VRRP on an Interface**

- By default, the linkage between an IPv4 VRRP and BFD is not configured on an interface. To enable such linkage, please configure this item.

❖ **Configuring Global IPv4 VRRP BFD**

- By default, global IPv4 VRRP BFD is not used to detect whether a master router is active. To enable this, please configure this item.

Verification

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

Related Commands

❖ **Enabling IPv4 VRRP**

Command	vrrp *group* ip *ipaddress* [secondary]
Parameter Description	*group*: Indicates the VRID of a VRRP group, the range of which varies with product models. *Ipaddress*: The IP address of a VRRP group. **secondary**: Indicates the secondary IP address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	If no virtual IP address is specified, routers cannot join a VRRP group. If no secondary IP address is applied, the configured IP address will be the primary IP address of a VRRP group.

❖ Configuring the IPv4 VRRP Authentication String

Command	vrrp *group* authentication *string*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *string*: Indicates the authentication string of a VRRP group (a plain text password consists of 8 bytes at most).
Command Mode	Interface configuration mode

| Usage Guide | In a VRRP group, the same authentication password should be configured for routers. The plain text authentication password cannot guarantee security but only prevents/prompts wrong VRRP configurations. This command is only applicable to VRRPv2 instead of VRRPv3.
Authentication is abolished for VRRPv3 packets. If VRRPv2 is chosen for an IPv4 VRRP group, the command is effective; if VRRPv3 is chosen, the command is ineffective. |

❖ Configuring the IPv4 VRRP Advertisement Interval

Command	vrrp *group* timers advertise { *advertise-interval*	csec *centisecond-interval* }
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group (unit: second). **csec** *centisecond-interval:* An interval for a master router in a backup group to send VRRP packets. It is an integer from 50 to 99. The unit is centisecond. No default value is provided. The command is only effective for VRRPv3 packets. If it is configured for VRRPv2 packets, the default interval is one second.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the Master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority and other information. According to the RFC standards, if an IPv4 VRRP group adopts VRRPv3 for sending multicast packets, the maximum advertisement interval is 40 seconds. Therefore, if the interval is set longer than 40 seconds, this maximum interval will be applied, though the configuration is effective.

❖ Configuring the IPv4 VRRP Preemption Mode

Command	vrrp *group* preempt [delay *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.
Command Mode	Interface configuration mode

| Usage Guide | If a VRRP group runs in Preemption mode, a higher priority router will take the place of the lower priority Master. If a VRRP group runs in Non-preemption mode, a router with the priority higher than that of the Master remains Backup. It makes little sense to configure the Preemption mode when the VRRP group uses the IP address of an Ethernet interface, in which case the group has the highest priority and automatically becomes the Master in the group. |

❖ Configuring the IPv4 VRRP Router Priority

Command	vrrp *group* priority *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of an interface in a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the priority of a VRRP group.

❖ Configuring the IPv4 VRRP Tracked Interface

Command	vrrp *group* track { *interface-type interface-number*	bfd *interface-type interface-number ipv4-addess* } [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. **bfd** *interface-type interface-number ipv4-address*: A specified adjacent IP address tracked through BFD. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	A tracked interface must be a routable Layer-3 logic interface (for example, a Routed port, an SVI interface, a Loopback interface, or a Tunnel interface). The priority of the router owns the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

❖ Configuring the IPv4 VRRP Tracked IP Address

Command	vrrp *group* track *ipv4-address* [interval *interval-value*] [timeout *timeout-value*] [retry *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv4-addres*: Indicates the IPv4 address to be tracked. *interval* *interval-value*: Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. *timeout* *timeout-value*: Indicates the probe timeout of waiting for responses. If no response is received when the timeout is up, it is regarded that the destination is inaccessible. The unit is second. Unless configured manually, the value is 1 second by default. **retry** *retry-value*: Indicates the probe retries. If the probe packet is sent continually for retry-value times but no response is received, it is regarded that the destination is inaccessible. The unit is times. Unless configured, the value is 3 times by default. *priority*: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv4 address for an IPv4 VRRP group. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

❖   Configuring the IPv4 VRRP Learning Timer

Command	vrrp *group* timers learn
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	Once the learning timer is enabled on a VRRP router, a Backup router learns the advertisement interval of the Master during the timer. Based on this, the Backup router calculates the interval for determining the Master router as failed instead of using the locally configured advertisement interval. This command achieves synchronization with the learning timer between the Master and

Backup routers.

❖ Configuring the IPv4 VRRP Group Description

Command	vrrp *group* description *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups. A description has 80 bytes at most, otherwise wrong configuration is prompted.

❖ Configuring the IPv4 VRRP Delay

Command	vrrp delay { minimum *min-seconds* | reload *reload-seconds* }
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. The two types of delay share a value range of 0 to 60 seconds. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.

❖ Configuring the IPv4 VRRP Version

Command	vrrp *group* version { 2 | 3 }
Parameter Description	**2**: Indicates VRRPv2. **3**: Indicates VRRPv3.

Command Mode	Interface configuration mode
Usage Guide	Considering the compatibility between VRRPv2 and VRRPv3, specify a standard for IPv4 VRRP based on the actual network condition. VRRPv2 is developed in RFC3768, while VRRPv3 is described in RFC5798. This command is only applicable to IPv4 VRRP.

❖ Specifying a Sub VLAN of a Super VLAN to Receive the IPv4 VRRP Packets

Command	vrrp detection-vlan {first-subvlan	*subvlan-id*}
Parameter Description	**first-subvlan**: Sends IPv4 VRRP packets only to the first UP Sub VLAN interface in a Super VLAN. *subvlan-id*: Sends IPv4 VRRP packets to a specified Sub VLAN.
Command Mode	Interface configuration mode
Usage Guide	This command is used to specify a Sub VLAN of a Super VLAN to receive the IPv4 VRRP packets. IPv4 VRRP packets are sent in a Super VLAN using the following three methods. Packets are sent to the first UP Sub VLAN interface in a Super VLAN, or to a specified Sub VLAN interface in a Super VLAN, or to all the Sub VLAN interfaces in a Super VLAN. If both VRRP and VRRP PLUS are enabled on a Super VLAN interface, VRRP packets are sent to all the UP Sub VLAN interfaces of the Super VLAN interface. This command is configured on a VLAN interface and effective only to Super VLAN interfaces.

❖ Configuring the BFD Support for IPv4 VRRP on an Interface

Command	vrrp *group* bfd *ip-address*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ip-address*: Indicates the interface IP address.
Command Mode	Interface configuration mode

3. Configuring VRRP

Usage Guide	For a Backup router, run this command to correlate an IPv4 VRRP group with BFD without caring the configured IP address. For the Master, as the primary IP address of a Backup router is not known, the router IP address can only be specified by the administrator. If global IPv4 VRRP BFD is configured, this configuration cannot be performed. To enable the BFD support, make sure that IP and BFD session parameters are configured on the target interface.

❖ Configuring Global IPv4 VRRP BFD

Command	vrrp bfd *interface-type interface-number ip-address*
Parameter Description	*interface-type interface-number*: Indicates interface type and ID. *ip-address*: Indicates the interface IP address.
Command Mode	Global configuration mode
Usage Guide	If global IPv4 VRRP BFD is configured, the configured BFD support will be deleted. To enable the BFD support, make sure that IP and BFD session parameters are configured on the target interface. A global IPv4 VRRP BFD session is only applicable to an IPv4 VRRP group consisting of two routers.

Configuration Example

❖ Configuring VRRP+MSTP

Scenario Figure 3-8	

Configuration Steps	▪ Enable MSTP on routers (switches A, B, C, D, E and F in this example). Configure VLAN-Instance mapping (mapping VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0), and configure gateways (Switch A and Switch B in this example) as the root bridges of corresponding instances. ▪ Add the SVIs of all VLANs to corresponding VRRP backup groups, and configure gateways as the

master and backup routers for corresponding backup groups See configuration details in the following table.

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

▪ Configure the uplink port (port Gi 0/1 of Switch A and Switch B) of master routers as a monitored interface of master router.

▪ Step 1: Create VLAN. Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 respectively on Switch A and

Switch B.

▪ Step 2: Configure MST regions. Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0.

▪ Step 3: Configure Switch A as the root bridge for MST 0 and MST 1, and Switch B as the root bridge for MST 2.

▪ Step 4: Enable MSTP.

▪ Step 5: Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups. See configuration in the above table.

▪ Step 6: Configure master routers and backup routers for all the groups.

▪ Step 7: Configure the uplink ports of master routers as monitored ports of VRRP groups. Caution: Monitored ports should be Layer 3 ports.

Step 8: Configure the Internet interfaces of the core routers as AP interfaces.

SwitchA	//Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 on Switch A.
	SwitchA#configure terminal
	Enter configuration commands, one per line. End with CNTL/Z.
	SwitchA(config)#vlan range 10,20,30,40
	SwitchA(config-vlan-range)#exit
	
	//Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0.
	SwitchA(config)#spanning-tree mst configuration
	SwitchA(config-mst)#instance 1 vlan 10,20
	%Warning:you must create vlans before configuring instance-vlan relationship
	SwitchA(config-mst)#instance 2 vlan 30,40
	%Warning:you must create vlans before configuring instance-vlan relationship
	SwitchA(config-mst)#exit
	
	//On Switch A, configure the priority of MST 0 and MST 1 as 4096, and that of MST 2 as 8192.
	SwitchA(config)#spanning-tree mst 0 priority 4096
	SwitchA(config)#spanning-tree mst 1 priority 4096
	SwitchA(config)#spanning-tree mst 2 priority 8192
	
	//Enabling MSTP
	SwitchA(config)#spanning-tree
	Enable spanning-tree.
	
	//Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups.
	SwitchA(config)#interface vlan 10
	SwitchA(config-if-VLAN 10)#ip address 192.168.10.2 255.255.255.0
	SwitchA(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
	SwitchA(config-if-VLAN 10)#exit
	SwitchA(config)#interface vlan 20
	SwitchA(config-if-VLAN 20)#ip address 192.168.20.2 255.255.255.0
	SwitchA(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
	SwitchA(config-if-VLAN 20)#exit
	SwitchA(config)#interface vlan 30
	SwitchA(config-if-VLAN 30)#ip address 192.168.30.2 255.255.255.0
	SwitchA(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
	SwitchA(config-if-VLAN 30)#exit
	SwitchA(config)#interface vlan 40
	SwitchA(config-if-VLAN 40)#ip address 192.168.40.2 255.255.255.0
	SwitchA(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1

	SwitchA(config-if-VLAN 40)#exit //Increase the priority of the VRRP 10 and VRRP 20 of Switch A to 120. SwitchA(config)#interface vlan 10

	SwitchA(config-if-VLAN 10)#vrrp 10 priority 120 SwitchA(config-if-VLAN 10)#exit SwitchA(config)#interface vlan 20
	
	SwitchA(config-if-VLAN 20)#vrrp 20 priority 120 SwitchA(config-if-VLAN 20)#exit
	
	//Configure the Gi 0/1 port of Switch A as Route Port and its IP address as10.10.1.1/24. SwitchA(config)#interface gigabitEthernet 0/1
	
	SwitchA(config-if-GigabitEthernet 0/1)#no switchport
	
	SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.10.1.1 255.255.255.0 SwitchA(config-if-GigabitEthernet 0/1)#exit
	
	//Configure the Gi 0/1 port of Switch A as a monitored port for VRRP 10 and VRRP 20, and a *Priority*
	
	decrement of 30.
	
	SwitchA(config)#interface vlan 10
	
	SwitchA(config-if-VLAN 10)#vrrp 10 track gigabitEthernet 0/1 30 SwitchA(config-if-VLAN 10)#exit
	
	SwitchA(config)#interface vlan 20
	
	SwitchA(config-if-VLAN 20)#vrrp 20 track gigabitEthernet 0/1 30 SwitchA(config-if-VLAN 20)#exit
	
	//Configure ports Gi 0/2 and Gi 0/3 as AP ports, which are Trunk ports. SwitchA#configure terminal
	
	Enter configuration commands, one per line. End with CNTL/Z. SwitchA(config)#interface range gigabitEthernet 0/2-3 SwitchA(config-if-range)#port-group 1
	
	SwitchA(config)#interface aggregateport 1
	
	SwitchA(config-if-AggregatePort 1)#switchport mode trunk

SwitchB	//Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 on Switch B. SwitchB#configure terminal
	
	Enter configuration commands, one per line. End with CNTL/Z. SwitchB(config)#vlan range 10,20,30,40
	
	SwitchB(config-vlan-range)#exit
	
	//Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0.
	
	SwitchB(config)#spanning-tree mst configuration
	
	SwitchB(config-mst)#instance 1 vlan 10,20
	
	%Warning:you must create vlans before configuring instance-vlan relationship

```
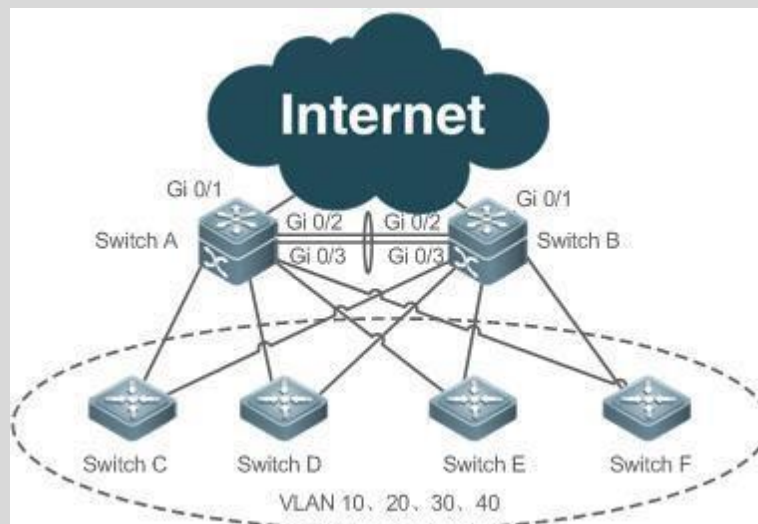SwitchB(config-mst)#instance 2 vlan 30,40

%Warning:you must create vlans before configuring instance-vlan relationship

SwitchB(config-mst)#exit


//On Switch B, configure the priority of MST 2 as 4096, and that of MST 0 and MST 1 as 8192.

SwitchB(config)#spanning-tree mst 2 priority 4096

SwitchB(config)#spanning-tree mst 0 priority 8192

SwitchB(config)#spanning-tree mst 1 priority 8192


//Enabling MSTP

SwitchB(config)#spanning-tree

Enable spanning-tree.


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

SwitchB(config)#interface vlan 10

SwitchB(config-if-VLAN 10)#ip address 192.168.10.3 255.255.255.0

SwitchB(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1

SwitchB(config-if-VLAN 10)#exit

SwitchB(config)#interface vlan 20

SwitchB(config-if-VLAN 20)#ip address 192.168.20.3 255.255.255.0

SwitchB(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1

SwitchB(config-if-VLAN 20)#exit

SwitchB(config)#interface vlan 30

SwitchB(config-if-VLAN 30)#ip address 192.168.30.3 255.255.255.0

SwitchB(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1

SwitchB(config-if-VLAN 30)#exit

SwitchB(config)#interface vlan 40

SwitchB(config-if-VLAN 40)#ip address 192.168.40.3 255.255.255.0

SwitchB(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1

SwitchB(config-if-VLAN 40)#exit


//Increase the priority of VRRP 30 and VRRP 40 of Switch B to 120.
```

	``
SwitchB(config)#interface vlan 30

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

//Configure the Gi 0/1 port of Switch B as Route Port and its IP address
as 10.10.1.1/24. SwitchB(config)#interface gigabitEthernet 0/1

SwitchB(config-if-GigabitEthernet 0/1)#no switchport

SwitchB(config-if-GigabitEthernet 0/1)#ip address 10.10.2.1 255.255.255.0
SwitchB(config-if-GigabitEthernet 0/1)#exit

//Configure the Gi 0/1 port of Switch B as a monitored port for VRRP 30
and VRRP 40, and the
``` *Interface-Priority* ```as 30.
SwitchB(config)#interface vlan 30

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

SwitchB(config)#interface vlan 40

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

//Configure ports Gi 0/2 and Gi 0/3 as AP ports, which are Trunk ports.
SwitchB #configure terminal

Enter configuration commands, one per line.
End with CNTL/Z. SwitchB (config)#interface
range gigabitEthernet 0/2-3 SwitchB
(config-if-range)#port-group 1
SwitchB (config)#interface aggregateport 1

SwitchB (config-if-AggregatePort 1)#switchport mode trunk
``` |
| **Verification** | |
| **Switch A** | ```
Check the configuration. SwitchA#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
``` |

```
spanning-tree mst configuration

instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094

instance 1 vlan 10, 20

instance 2 vlan 30, 40

spanning-tree mst 0 priority 4096

spanning-tree mst 1 priority 4096

spanning-tree mst 2 priority 8192

interface GigabitEthernet 0/1

no switchport

no ip proxy-arp

ip address 10.10.1.1 255.255.255.0

!

interface GigabitEthernet 0/2

port-group 1

!

interface GigabitEthernet 0/3

port-group 1

!

interface AggregatePort 1

switchport mode trunk

!

interface VLAN 10

no ip proxy-arp

ip address 192.168.10.2 255.255.255.0

vrrp 10 priority 120

vrrp 10 ip 192.168.10.1

vrrp 10 track GigabitEthernet 0/1 30

!

interface VLAN 20 no ip proxy-arp

ip address 192.168.20.2 255.255.255.0

vrrp 20 priority 120

vrrp 20 ip 192.168.20.1

vrrp 20 track GigabitEthernet 0/1 30

!

interface VLAN 30 no ip proxy-arp

ip address 192.168.30.2 255.255.255.0

vrrp 30 ip 192.168.30.1

!

interface VLAN 40 no ip proxy-arp

ip address 192.168.40.2 255.255.255.0
```

	vrrp 40 ip 192.168.40.1 //Check VRRP status. SwitchA#show vrrp brief

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

//Disconnect the uplink of Switch A, and check VRRP status. SwitchA#show vrrp brief

Interface	Grp	Pri	timer	Own	Pre	State	Master addr	Group addr
VLAN 10	10	90	3	–	P	Backup	192.168.10.3	192.168.10.1
VLAN 20	20	90	3	–	P	Backup	192.168.20.3	192.168.20.1
VLAN 30	30	100	3	–	P	Backup	192.168.30.3	192.168.30.1
VLAN 40	40	100	3	–	P	Backup	192.168.40.3	192.168.40.1

Switch B	//Check the configuration. SwitchB#show running-config ! vlan 10 ! vlan 20 ! vlan 30 !

```
vlan 40

!

spanning-tree

spanning-tree mst configuration

instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094

instance 1 vlan 10, 20

instance 2 vlan 30, 40

spanning-tree mst 0 priority 8192

spanning-tree mst 1 priority 8192

spanning-tree mst 2 priority 4096 interface GigabitEthernet 0/1
no switchport no ip proxy-arp
ip address 10.10.2.1 255.255.255.0

!
interface GigabitEthernet 0/2 port-group 1
interface GigabitEthernet 0/3

port-group 1

!

interface AggregatePort 1

switchport mode trunk

!

interface VLAN 10

no ip proxy-arp

ip address 192.168.10.3 255.255.255.0
```

```
vrrp 10 ip 192.168.10.1

!

interface VLAN 20

no ip proxy-arp

ip address 192.168.20.3 255.255.255.0

vrrp 20 ip 192.168.20.1

!

interface VLAN 30

no ip proxy-arp

ip address 192.168.30.3 255.255.255.0

vrrp 30 priority 120

vrrp 30 ip 192.168.30.1

vrrp 30 track GigabitEthernet 0/1 30

!

interface VLAN 40

no ip proxy-arp

ip address 192.168.40.3 255.255.255.0

vrrp 40 priority 120

vrrp 40 ip 192.168.40.1

vrrp 40 track GigabitEthernet 0/1 30
```

<table>
<tr><td></td><td>

//Check VRRP status.

SwitchB#show vrrp brief

!

</td></tr>
<tr><td></td><td>

```
Interface  Grp  Pri  timer  Own  Pre  State    Master addr   Group
addr VLAN 10    10          100  3    -        P             Backup
192.168.10.2  192.168.10.1
VLAN 20    20   100  3      -    P    Backup   192.168.20.2  192.168.20.1

VLAN 30    30   120  3      -    P    Master   192.168.30.3  192.168.30.1

VLAN 40    40   120  3      -    P    Master   192.168.40.3  192.168.40.1

//Disconnect the uplink of Switch B, and check VRRP
status. SwitchB#show vrrp brief
Interface  Grp  Pri  timer  Own  Pre  State    Master addr   Group
addr VLAN 10    10          100  3    -        P             Master
192.168.10.3  192.168.10.1
VLAN 20    20   100  3      -    P    Master   192.168.20.3  192.168.20.1

VLAN 30    30   120  3      -    P    Master   192.168.30.3  192.168.30.1

VLAN 40    40   120  3      -    P    Master   192.168.40.3  192.168.40.1
```

</td></tr>
</table>

Common Errors

- Different virtual IP addresses are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.

- Different VRRP advertisement intervals are configured on the routers in a VRRP group and the learning timer is not configured, resulting in multiple Master routers in the group.

- Different VRRP versions are configured on the routers in a VRRP group, resulting in multiple Master routers in the group.

- For VRRPv2, the Ethernet interfaces of the routers in a VRRP group are all in plain text authentication mode but inconsistent in authentication strings, resulting in multiple Master routers in the group.

3.5 Monitoring

Displaying

Description	Command
Displays the brief or detailed	**show** [**ipv6**] **vrrp** [**brief**	*group*]

information of IPv4/IPv6 VRRP.	
Displays the information of an IPv4/IPv6 VRRP group on a specified interface.	**show** [**ipv6**] **vrrp interface** *type number* [**brief**]
Displays the statistics of VRRP packets.	**show vrrp packet statistics** [*interface-type interface-number*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs VRRP errors, events, packets and status.	**debug** [**ipv6**] **vrrp**
Debugs VRRP errors.	**debug** [**ipv6**] **vrrp errors**
Debugs VRRP events.	**debug** [**ipv6**] **vrrp events**
Debugs VRRP packets.	**debug vrrp packets** [**acl** *acl-id*	[**icmp**	**protocol**] **interface** *type number* [*group*]] **debug ipv6 vrrp packets** [**acl** *acl-name*	[**icmp**	**protocol**] **interface** *type number* [*group*]]
Debugs VRRP status.	**debug** [**ipv6**] **vrrp state**

4.1 Overview

Virtual Router Redundancy Protocol Plus (VRRP Plus) is an extension of VRRP. It uses VRRP to implement gateway backup and load balancing in the IEEE 802.3 local area network (LAN).

A disadvantage of VRRP is that the router in backup state cannot forward packets. To use VRRP to implement load balancing, you need to manually configure multiple VRRP groups and set the gateway addresses of hosts in the LAN to virtual IP addresses of different VRRP groups. This increases the workload of the network administrator. VRRP Plus is designed to address this issue.

With VRRP Plus, load balancing is automatically implemented. That is, traffic of different hosts is automatically distributed to members of the VRRP Plus group, and it is unnecessary to configure multiple VRRP groups or set the gateway addresses of hosts in the LAN to virtual IP addresses of different VRRP groups. This greatly reduces the workload of the network administrator.

4.2 Applications

Application	Description
Enabling Load Balancing Within a VRRP Group	Implement load balancing within a VRRP group without configuring multiple groups or configuring different default gateways for hosts.

4.2.1 Enabling Load Balancing Within a VRRP Group
Scenario

Enable load balancing within a VRRP group without configuring without configuring multiple VRRP groups or configuring different default gateways for hosts.

As shown in Figure 4-1, configure data as follows:

- Configure a VRRP group that consists of Router A and Router B, and enable the VRRP Plus function.

- Configure the default gateway of each host as the master virtual IP address of the VRRP group. Figure 4-1 Application topology of IPv4 VRRP Plus

Virtual Router Group,IP address 192.168.12.1

Remarks	1. **Two layer-3 (L3) devices, Router A and Router B, form a VRRP Plus group, and the virtual IP address of the group is 192.168.12.1. Router A is the master device of VRRP and functions as a balancing virtual gateway (BVG). Router B is the backup device of VRRP and functions as a balancing virtual forwarder (BVF).**
	2. **Host 1 to Host 4 are hosts in the LAN with the network segment 192.168.12.0/24. Their default gateway addresses are set to the virtual IP address 192.168.12.1 of the VRRP Plus group.**
	3. **The load balancing policy is configured on the device to respond to the ARP requests sent from different hosts. For example, when Host 1 and Host 2 request the gateway ARP, the MAC address 0000.5e00.0101 is returned to Host 1 and Host 2. When Host 3 and Host 4 request the gateway ARP, the MAC address 001A.A916.0201 is returned to Host 3 and Host 4. In this way, packets exchanged between Host 1/Host 2 and the external network are sent to Router A, and packets exchanged between Host 3/Host 4 and the external network are sent to Router B, thereby implementing load balancing.**

Deployment

▪ Deploy VRRP Plus on Router A and Router B to implement load balancing on the local host.

4.3 Features

Basic Concepts

❖ BVG

The BVG allocates virtual MAC addresses to members of the VRRP Plus group. It responds to the gateway ARP/ND requests in the LAN, and forwards packets of hosts in the LAN.

❖ BVF

The BVF forwards packets of hosts in the LAN. If a virtual MAC address is allocated to a BVF, the BVF participates in packet forwarding; otherwise, the BVF does not participate in packet forwarding.

Overview

Feature	Description
VRRP Plus	Extend VRRP and use VRRP to implement gateway backup and load balancing in the IEEE 802.3 LAN.

4.3.1 VRRP Plus

With VRRP Plus, load balancing is automatically implemented. That is, traffic of different hosts is automatically distributed to members of the VRRP Plus group, and it is unnecessary to configure multiple VRRP groups or set the gateway addresses of hosts in the LAN to the virtual IPv4/IPv6 addresses of different VRRP groups.

Basic Principles

Hosts in a LAN use the unified gateway IPv4/IPv6 address (that is, virtual IP address of the VRRP group). When different hosts request the gateway ARP/ND, the BVG responds with different virtual MAC addresses. In this way, traffic of different hosts are distributed to different members of the VRRP Plus group, thereby implementing load balancing.

❖ **Relationship Between VRRP Plus and VRRP**

VRRP Plus relies on VRRP, and runs in the following way:

A master device in VRRP corresponds to a BVG in VRRP Plus, and a backup device in VRRP corresponds to a BVF in VRRP Plus. Gateway addresses of hosts in the LAN are set to the virtual IPv4/IPv6 address of VRRP.

❖ **MAC Address Allocation Rules of the BVG and BVF**

The BVG allocates virtual MAC addresses to BVFs. For an IPv4 VRRP Plus group, the BVG directly uses the virtual MAC address of VRRP to ensure compatibility between IPv4 VRRP Plus and VRRP. That is, the virtual MAC address used by the BVG is 00-00-5E-00-01-{VRID}, where VRID is the VRRP group number. The virtual MAC address used by a BVF is 00-1A-A9-16-{MemberID}-{VRID}, where MemberID is the member ID of the BVF in the VRRP Plus group. Currently, a VRRP Plus group can have up to four members. The BVG uses the member ID 01, and the other BVFs use the member IDs 02 to 04.

❖ **Load Balancing Policy of VRRP Plus**

The BVG responds to the gateway ARP/NS requests sent from hosts in a LAN. Based on the specific load balancing policy, the BVG responds hosts with different virtual MAC addresses. There are three types of load balancing policies:

▪ Host-dependent policy: A specified virtual MAC address is used to respond to the requests sent by a specified host.

▪ Round-robin policy: Virtual MAC addresses in the backup group are used in a cyclic manner to respond to the gateway ARP/NS requests sent by hosts.

▪ Weighted policy: The ARP/NA requests are responded based on the forwarding capability of each device.

If the load balancing mode is changed, load balancing is always implemented in the new load balancing mode. For example, if the polling response mode is previously used, and later the weighted mode is used, load balancing is implemented in weighted mode regardless of the earlier responses of the device. If the weighted policy is used, and the total weight of virtual routers in a VRRP Plus group is 0, the ARP/NS requests are not responded.

❖ **Proxy of the Virtual MAC Address**

When a device with a virtual MAC address becomes faulty in the backup group, traffic of hosts that use this virtual MAC address as the gateway MAC address will be interrupted.

The BVG in the VRRP Plus backup group can quickly detect the fault, and automatically allocates the virtual MAC address of the faulty BVF to another device in the backup group. The new device acts as the proxy of the faulty device to forward packets of the virtual MAC address. In addition, this proxy device takes over traffic of original hosts to prevent traffic interruption. The virtual MAC address allocated to a device in the backup group can be called master virtual MAC address, and the virtual MAC address used by this device on behalf of another device is called proxy virtual MAC address.

❖ **Redirection Time and Timeout of the Proxy Virtual MAC Address**

VRRP Plus provides the proxy function for the virtual MAC address so that another device can take the place of a faulty device with a virtual MAC address to forward packets. If the BVF is recovered from the fault, its forwarding role is recovered and the BVF continues to forward packets of the virtual MAC address allocated to this BVF. If the faulty BVF is not recovered, the backup group stops redirecting traffic to this virtual MAC address. That is, when ARP requests are received again, this virtual MAC address is no longer responded. After a sufficient long period of time, it is believed that hosts that use the MAC address as the gateway MAC address already update the ARP/ND table entry of the gateway address, and the traffic is already taken over by other devices. At this time, this virtual MAC address can be deleted, and packets sent to this virtual MAC address are dropped.

VRRP Plus supports configuration of the redirection time and timeout of the backup group. When a device is faulty, the backup group allocates the virtual MAC address of the faulty device to another device. Within the redirection time, the backup group continues to use this virtual MAC address to respond the ARP/NS requests. When the redirection time expires, the backup group no longer uses this virtual MAC address to respond the requests. When the timeout elapses, the backup group deletes this virtual MAC address and stops using this virtual MAC address for proxy forwarding. Figure 4-2 shows the changes to the role of the virtual MAC address within the redirection time and timeout.

Figure 4-2 Changes to the Role of the Virtual MAC Address Within the Redirection Time and Timeout

❖ **Weight-based Forwarding**

VRRP Plus supports the weight configuration of the backup group. Different weights are configured for different devices. In this way, more traffic is distributed to the device with a greater weight and less traffic is distributed to the device with a smaller weight, thereby fully utilizing the forwarding performance of different devices. When the weight of a BVF in the backup group is smaller than the lower threshold, the BVF automatically exits from the forwarding role. When the weight recovers and is greater than the upper threshold, the BVF automatically applies for

the forwarding role. The forwarding role can be recovered when one or more remaining virtual MAC addresses or proxy virtual MAC addresses exist.

❖ **Association of VRRP Plus with BFD**

VRRP Plus supports association with bidirectional forwarding detection (BFD) to adjust the weight based on the link status. Each device in a backup group can associate its weight with the link status. When a link is abnormal or interrupted, the device automatically decreases its weight. When the weight is too low, the device automatically exits from the forwarding role. If the backup group is currently using the weighted load balancing policy, traffic can be distributed based on the new weight. When the associated link recovers, the device can automatically restore its original weight and the forwarding role. If the backup group is currently using the weighted load balancing policy, traffic can be distributed based on the recovered weight.

❖ **Weight-based Forwarding Seizure**

VRRP Plus supports the function of seizing the forwarding role. In VRRP Plus, at most four devices can participate in load balancing. That is, a VRRP Plus backup group generates at most four virtual MAC addresses. If more than four devices are added to a VRRP Plus group, only four devices participate in packet forwarding. The remaining devices only listen to the status of other devices and do not participate in packet forwarding. Only when a device participating in packet forwarding is faulty, another device that originally does not participate in packet forwarding will take the place of the faulty device to forward packets. Assume that a VRRP Plus backup group already has four devices and all these devices participate in packet forwarding; a fifth device is added to the VRRP Plus group, and the forwarding capability of this device is strong or the original forwarding role encounters a link failure and consequently degradation of forwarding performance. In this case, if the seizure mode is enabled, the fifth device can seize the forwarding role from a device with a smaller weight (that is, with lower forwarding capability). A greater weight is configured for a device with stronger forwarding capability. When the weight of a device in listening state is found greater than that of a forwarding device, the device in listening state automatically seizes the forwarding role from the forwarding device. That is, the device with stronger forwarding capability forwards packets, whereas the device with lower forwarding capability is in listening state. This can minimize the waste of resources.

The BVG in a backup group is responsible for allocation of virtual MAC addresses. Therefore, the BVG role cannot be seized, and only the forwarding role of a BVF can be seized. If the BVG device is faulty, VRRP re-elects a new master device, which assumes the BVG role.

❖ **Factors Affecting the Forwarding Policy**

1. After VRRP Plus is configured, the ARP/NS requests are received from hosts can be responded based on different load balancing policies to implement load balancing among these hosts. However, load balancing cannot be implemented for hosts that have learned the VRRP virtual gateway addresses before configuration of VRRP Plus. Therefore, if VRRP Plus is configured after the VRRP state is changed to Master, real load balancing cannot be

implemented before aging of the ARP/NDs learned by hosts. Load balancing is implemented only after the gateway ARP/NDs recorded by the hosts age and the hosts request for new gateway addresses.

2. Periodical sending of gratuitous ARPs on an interface also affect the load balancing function of VRRP Plus. When VRRP Plus is enabled, the function of sending gratuitous ARPs of VRRP virtual IP addresses will be disabled. When an virtual IP address overlaps with an actual IP address, gratuitous ARPs of this address are no longer sent.

3. When an address conflict occurs between a host and the local device, the ARP/NA module will broadcast gratuitous ARP/NA packets of this address. If a conflict of the VRRP Plus virtual address occurs, sending gratuitous ARP/NA packet will result re-learning of the host's gateway MAC address, which negatively affects the load balancing function of VRRP Plus. Therefore, the load balancing function of VRRP Plus is currently not supported in this scenario.

4.4 Configuration

Configuration Item	Description and Command	
Configuring VRRP Plus	(Mandatory) It is used to enable the VRRP Plus function.	
	vrrp balance	Enables the VRRP Plus function of a VRRP backup group with the specified group ID in interface configuration mode.
	(Optional) It is used to configure parameters of a VRRP Plus backup group.	
	vrrp load-balancing	Configures the load balancing policy of VRRP Plus in interface configuration mode.
	vrrp timers redirect	Configures the redirection time and timeout of the proxy virtual MAC address in a VRRP Plus backup group in interface configuration mode.
	vrrp weighting	Configures the weight and upper and lower thresholds of a VRRP Plus backup group in interface configuration mode.

Configuration Item	Description and Command	
	vrrp forwarder preempt	Configures the forwarding seizure function of a VRRP Plus backup group in interface configuration mode.

4.4.1 Configure VRRP Plus

Configuration Effect

- Enable the VRRP Plus function. (By default, this function is disabled.)

Notes

- To enable the VRRP Plus function, you must configure the VRRP virtual IP address for the corresponding backup group.

Configuration Steps

❖ **Enabling VRRP Plus on an Interface**

- By default, VRRP Plus is enabled. Perform this configuration if VRRP Plus is required.

❖ **Configuring the Load Balancing Policy of VRRP Plus**

- After VRRP Plus is enabled, the host-dependent load balancing policy is used by default.

❖ **Configuring the Redirection Time and Timeout of the Proxy Virtual MAC Address in a VRRP Plus Backup Group**

- After VRRP Plus is enabled, the redirection time is set to 300s and timeout is set to 14,400s by default.

❖ **Configuring the Weight and Upper and Lower Thresholds of a VRRP Plus Backup Group**

- After VRRP Plus is enabled, the weight of the backup group is set to 100, the lower threshold to 1, and the upper threshold to 100 by default.

❖ **Configuring the Forwarding Seizure Function of a VRRP Plus Backup Group**

- After VRRP Plus is enabled, the forwarding seizure function is enabled by default.

Verification

- Run the **show** *group* **vrrp balance** command to display the VRRP backup group configuration. If the backup group has the packet forwarding tasks, "local" is displayed in the **forwarders** column, and the virtual MAC address allocated to this backup group is also displayed.

Related Commands

❖ **Enabling VRRP Plus on an Interface**

Command	vrrp *group* balance
Parameter	*group*: Indicates the ID of the VRRP group. The value range of the group ID varies according to the product
Description	model.
Command Mode	Interface configuration mode
Usage Guide	VRRP Plus can be enabled only after a VRRP group is configured.

❖ Configuring the Load Balancing Policy of a VRRP Plus Backup Group

Command	vrrp *group* load-balancing**{**host-dependent | round-robin | weighted **}**
Parameter Description	*group*: Indicates the ID of the VRRP group. **host-dependent**: Indicates the host-dependent load balancing policy. **round-robin**: Indicates the round-robin load balancing policy. **weighted**: Indicates the weighted load balancing policy.
Command Mode	Interface configuration mode
Usage Guide	After VRRP Plus is enabled, the host-dependent load balancing policy is used by default. The load balancing policy of the entire backup group is determined by the policy configured on the BVG. If you wish to use the same load balancing policy after the role of the BVG device changes, configure the same policy on all devices in the backup group.

❖ Configuring the Redirection Time and Timeout of the Proxy Virtual MAC Address in a VRRP Plus Backup Group

Command	vrrp *group* timers redirect *redirect timeout*
Parameter Description	*group*: Indicates the ID of the VRRP group. *redirect*: Indicates the redirection time. The value ranges from 0 to 3,600s. The default value is 300s, that is, 5 minutes. *timeout*: Indicates the timeout time. The value ranges from (redirect + 600) to 64,800s. The default value is 14400, that is, 4 hours.

Command Mode	Interface configuration mode
Usage Guide	After VRRP Plus is enabled, the redirection time is set to 300s and timeout is set to 14,400s by default. When a device is faulty, the backup group allocates the virtual MAC ddress of the faulty device to another device. Within the redirection time, the backup group continues to use this virtual MAC address to respond the ARP/NS requests. When the redirection time expires, the backup group no longer uses this virtual MAC address to respond the requests. When the timeout elapses, the backup group deletes this virtual MAC address.

❖ Configuring the Weight and Upper and Lower Thresholds of a VRRP Plus Backup Group

Command	vrrp *group* weighting *maximum* [lower *lower*] [upper *upper*]
Parameter Description	*maximum*: Indicates the weight of the backup group. The value ranges from 2 to 254. The default value is 100. **lower** *lower*: Indicates the lower threshold of the backup group. The value ranges from 1 to (**maximum** - 1). The default value is 1. **upper** *upper:* Indicates the upper threshold of the backup group. The value ranges from **lower** to **maximum**.
	The default value is 100.
Command Mode	Interface configuration mode
Usage Guide	After VRRP Plus is enabled, the weight and upper and lower thresholds of a VRRP Plus backup group are configured by default. You can use this command to configure different weights for different devices so that more traffic is distributed to the device with a greater weight and less traffic is distributed to the device with a smaller weight. When the weight of a BVF in the backup group is lower than the lower threshold, the BVF automatically exits from the forwarding role. When the weight recovers and is higher than the upper threshold, the forwarding role of the BVF is automatically restored.

❖ Configuring the Forwarding Seizure Function of a VRRP Plus Backup Group

Command	vrrp *group* forwarder preempt
Parameter Description	*group*: Indicates the ID of the VRRP group.

Command Mode	Interface configuration mode
Usage Guide	After VRRP Plus is enabled, the forwarding seizure function is enabled by default. VRRP Plus supports configuration of the forwarding seizure function of a backup group. When the weight of a device in listening state is found greater than that of a forwarding device, the device in listening state automatically seizes the forwarding role from the forwarding device. That is, the device with stronger forwarding capability forwards packets, whereas the device with lower forwarding capability is in listening state.

Configuration Example

❖ Enabling Load Balancing Within an IPv4 VRRP Group

Scenario Figure 4-3	
Configuration Steps	Configure a VRRP group and enable VRRP Plus respectively on Router A and Router B. Configure the local IP addresses so that Router A becomes a BVG (master) device, and Router B becomes a BVF (backup) device. - Retain default configurations of the weight, upper and lower thresholds, redirection time, timeout, and forwarding seizure of the backup group. - Set the default gateway addresses of Host 1 to Host 4 in the LAN to the virtual IP address of VRRP, that is, 192.168.12.1.

Router A	QTECHA#config QTECHA(config)#interface GigabitEthernet0/0 // 'no switchport' is used on the switch. QTECHA(config-if-GigabitEthernet 0/0)#no switchport QTECHA(config-if-GigabitEthernet 0/0)#ip address 192.168.12.3 255.255.255.0 QTECHA(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.12.1 QTECHA(config-if-GigabitEthernet 0/0)#vrrp 1 balance QTECHA(config-if-GigabitEthernet 0/0)#vrrp 1 load-balancing weighted
Router B	QTECHB#config QTECHB(config)#interface GigabitEthernet0/0 QTECHB(config-if-GigabitEthernet 0/0)#no switchport QTECHB(config-if-GigabitEthernet 0/0)#ip address 192.168.12.2 255.255.255.0 QTECHB(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.12.1 QTECHB(config-if-GigabitEthernet 0/0)#vrrp 1 balance QTECHB(config-if-GigabitEthernet 0/0)#vrrp 1 load-balancing weighted
Verification	Run the **show vrrp balance** command to display the configuration of the VRRP Plus group. If the backup group has the packet forwarding tasks, "local" is displayed in the **forwarders** column, and the virtual MAC address allocated to this backup group is also displayed.
Router A	QTECHA# show vrrp balance interface GigabitEthernet0/0 State is BVG Virtual IP address is 192.168.12.1 Hello time 1 sec, hold time 3 sec Load balancing: weighted Redirect time 300 sec, forwarder time-out 14400 sec Weighting 100 (configured 100), thresholds: lower 1, upper 100 There are 2 forwarders Forwarder 1 (local)
	MAC address: 0000.5e00.0101 Owner ID is 0000.0001.0006 Preemption disabled (BVG cannot be preempted) Forwarder 2 MAC address: 001a.a916.0201 Owner ID is 00d0.f822.33a3 Preemption enabled

Router B	QTECHB# show vrrp balance interface GigabitEthernet0/0 State is BVF
	Virtual IP address is 192.168.12.1 Hello time 1 sec, hold time 3 sec Load balancing: weighted
	Redirect time 300 sec, forwarder time-out 14400 sec
	Weighting 100 (configured 100), thresholds: lower 1, upper 100 There are 2 forwarders
	Forwarder 1 MAC address:
	0000.5e00.0101
	Owner ID is 0000.0001.0006
	Preemption disabled (BVG cannot be preempted) Forwarder 2 (local)
	MAC address: 001a.a916.0201
	Owner ID is 00d0.f822.33a3
	Preemption enabled

Common Errors

- VRRP Plus does not take effect because the VRRP virtual IP address is not configured for the related group.

4.5 Monitoring

Displaying

Description	Command
Displays the brief or detailed configuration of VRRP Plus.	**show vrrp balance**
Displays the actions of the VRRP Plus group on a specified interface.	**show vrrp balance interface**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the VRRP Plus function.	**debug vrrp balance**
Debugs errors.	**debug vrrp balance error**

QTECH
МИР ДОСТУПНЕЕ | www.qtech.ru

Debugs events of the VRRP Plus group.	**debug vrrp balance event**
Debugs the messages between the VRRP module and the track module.	**debug vrrp balance messages**
Debugs the VRRP Plus packets.	**Debug vrrp balance packets**
Debugs the VRRP Plus group status.	**debug vrrp balance state**
Debugs the timers of the VRRP Plus group.	**debug vrrp balance timer**

5.1   Overview

Communication failures will interrupt networking and thus affect services. Therefore, it is essential to rapidly locate communication failures on links with adjacent devices to ensure a timely action and service availability. Bidirectional Forwarding Detection (BFD) provides a method of rapidly detecting connectivity of the forwarding path between two adjacent routers in an underloaded way. It can quickly spot faults on the bidirectional forwarding path between two routers for

upper-layer protocols such as routing protocols and Multi-Protocol Label Switching (MPLS). As a result, a standby forwarding path is adopted to maintain the performance of the existing network.

Protocols and Standards

- draft-ietf-bfd-base-09: Bidirectional Forwarding Detection

- draft-ietf-bfd-generic-05: Generic Application of BFD

- draft-ietf-bfd-mib-06: Bidirectional Forwarding Detection Management Information Base

- draft-ietf-bfd-v4v6-1hop-09: BFD for IPv4 and IPv6 (Single Hop)

- draft-ietf-bfd-multihop-07: BFD for IPv4 and IPv6 (Multi-hop)

- draft-ietf-bfd-mpls-07: BFD For MPLS LSPs

Currently, draft-ietf-bfd-mib-06 and draft-ietf-bfd-multihop-07 are not supported.

5.2   Applications

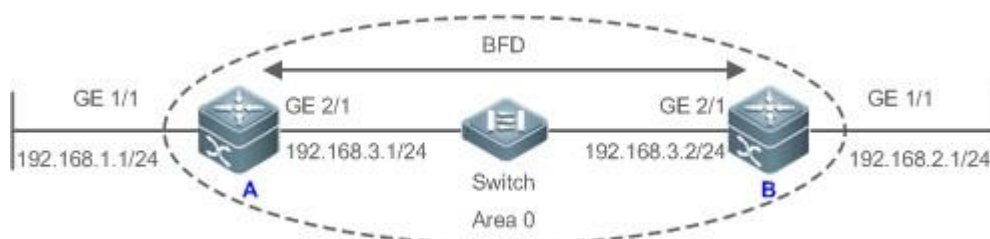| Application	Description
BFD Support for OSPF	OSPF utilizes BFD to rapidly detect the neighbor status.
BFD Support for Static Routing	Static routing utilizes BFD to rapidly detect the next-hop reachability of a route.

5.2.1   BFD Support for OSPF
Scenario

The Open Shortest Path First (OSPF) protocol dynamically discovers a neighbor by using hello packets. After BFD is enabled, a BFD session is established with the neighbor in the full adjacency to detect the neighbor status. When the neighbor fails, OSFP immediately performs network convergence. The convergence time can be shortened from 120 seconds (by default, on a non-broadcast network, OSPF hello packets are transmitted at an interval of 30 seconds and the neighbor failure time is four times the interval, that is, 120 seconds) to 1 second.

Use the following figure as an example. Router A and Router B are connected through a Layer-2 switch, OSPF is configured on the routers to establish routes, and BFD support for OSPF is enabled on the interfaces of Router A and Router B. When

the link between Router B and the Layer-2 switch malfunctions, BFD can rapidly detect the fault and advertise it to OSPF, so as to trigger fast OSPF convergence.

Figure 5-1

Remarks	**A and B are routers. Switch is a Layer-2 switch.**
	A and B are connected through the Layer-2 switch.

Deployment

- Configure IP addresses for interconnected interfaces of Router A and Router B.

- Run OSPF on Router A and Router B.

- Set BFD parameters on interconnected interfaces of Router A and Router B.

- Enable BFD support for OSPF on Router A and Router B.

5.2.2 BFD Support for BGP
Scenario

A router running the Border Gateway Protocol (BGP) is called BGP Speaker. A BGP Speaker actively initiates a Transmission Control Protocol (TCP) connection request to a specified BGP peer. After a TCP connection is established successfully, the BGP Speaker and the BGP peer exchange BGP packets to negotiate connection parameters. A BGP neighbor relationship is successfully established after consistent parameters are negotiated. After the BFD detection function is enabled on the BGP router, the BGP router creates a BFD session with a neighbor that has established the neighbor relationship with the BGP router, and the BGP router uses the BFD mechanism to detect the neighbor

status. Once the BFD neighbor is unreachable, BGP conducts network convergence immediately.

As shown in the figure below, Router A, Router B, and Router C are interconnected. The Interior Gateway Protocol (IGP) runs between Router A and Router B and between Router B and Router C to establish routes. The External Border Gateway Protocol (EBGP) runs on Router A and Router C. BFD support for BGP is enabled globally. When the link between Router B and Router A fails, BFD can rapidly identify the failure, notify the routers running BGP of the disconnection, and trigger the routers running the BGP to conduct fast convergence.

Figure 5-2

Remarks	A, B, and C are routers, and A is interconnected to C via a Layer-3 router.

Deployment

- Configure IP addresses for ports connecting Router A and Router B.

- Run the OSPF protocol on Router A and Router B.

- Configure IP addresses for ports connecting Router B and Router C.

- Run the OSPF protocol on Router B and Router C.

- Run BGP on Router A and Router C.

- Enable BFD support for BGP on Router A and Router C.

5.2.3   BFD Support for Static Routing
Scenario

BFD support for static routing prevents routers from selecting a faulty static route as the forwarding path and enables rapid routing failover by using an available backup forwarding path.

Different from dynamic routing protocols, static routing does not have the neighbor discovery (ND) mechanism. When BFD support for static routing is configured, the next-hop reachability of a static route relies on the BFD session status. If a BFD session fails, the next hop of a static route is thought unreachable and will not be added to the routing information base (RIB).

Use the following figure as an example. Router A and Router B are connected through a Layer-2 switch, static routing is configured on the routers to establish forwarding paths, and BFD support for static routing is enabled on the interfaces of Router A and Router B. When the link between Router B and the Layer-2 switch malfunctions, BFD can rapidly detect the fault and advertise it to static routing, so as to trigger the system to delete the static route from the RIB, thereby preventing routing errors.

Figure 5-3

Remarks	A and B are routers.
	A and B are connected through the Layer-2 switch.

Deployment

- Configure IP addresses for interconnected interfaces of Router A and Router B.

- Configure static routing on Router A and Router B.

- Set BFD parameters for interconnected interfaces of Router A and Router B.

- Enable BFD support for static routing on Router A and Router B.

5.3 Features

Basic Concepts

❖ Packet Format

Detection packets transmitted by BFD are User Datagram Protocol (UDP) packets, which are classified into control packets and echo packets. Echo packets concern only the local system of a BFD session. Therefore, their formats are not specified. BFD specifies the format of only control packets. Currently, there are two versions (version 0 and version 1) for the format of control packets. Version 1 is adopted by default for establishing a BFD session. If a device receives packets of version 0 from the peer system, the device automatically switches to version 0.

Figure 5-4

Field	Description
Vers	Indicates the BFD protocol version number, which is 1 currently.
Diag	Indicates the cause for the local system's last change in session state, including: 0 -- No Diagnostic. 1 -- Control Detection Time Expired 2 -- Echo Function Failed 3 -- Neighbor Signaled Session Down
Field	**Description**
	4 -- Forwarding Plane Reset 5 -- Path Down 6 -- Concatenated Path Down 7 --Administratively Down
Sta	Indicates the BFD local session state, including: 0 -- AdminDown. 1 -- Down. 2 -- Init. 3 -- Up.
P	Indicates that the transmitter in a BFD session adds this bit in a verification request upon parameter changes, waiting for the peer response.
F	Indicates the bit that must be set in the response packet for responding to the P bit.
C	Indicates the control plane independent. If set, changes of the control plane do not affect BFD detection. For example, if the control plane is OSPF, when OSPF is restarted or experiences graceful restart (GR), BFD can continue to detect the link status.
A	Indicates the authentication present. If set, a session is to be authenticated.
D	Indicates the demand request. If set, the transmitter desires to detect links in Demand mode.
M	Indicates the multipoint bit to be used in point-to-multipoint extensions. It must be set to 0 currently.

Detect Mult	Indicates the detection timeout multiplier. It is used by the detector to calculate the detection timeout time.
Length	Indicates the packet length.
My Discriminator	Indicates the discriminator of the local end connected by a BFD session.
Your Discriminator	Indicates the discriminator of the remote end connected by a BFD session.
Desired Min Tx Interval	Indicates the minimum interval of transmitting BFD packets supported by the local end.
Required Min RX Interval	Indicates the minimum interval of receiving BFD packets supported by the local end.
Required Min Echo RX Interval	Indicates the minimum interval of receiving echo packets supported by the local end. It is set to 0 if the local end does not support the echo function.
Auth Type	(Optional) Indicates the authentication type, including: Simple Password Keyed MD5 Meticulous Keyed MD5 Keyed SHA1 Meticulous Keyed SHA1
Auth Length	Indicates the authentication data length.
Authentication Data	Indicates the authentication data area.

❖ **Session Status**

A BFD session can be in any of the four basic states: Down, Init, Up, and AdminDown.

1. Down: Indicates that a session is in the Down state or is established just now.

2. Init: Indicates that the local system has communicated with the peer system and desires to bring the session to the Up state.

3. Up: Indicates that a session has been negotiated successfully.

4. AdminDown: Indicates that a session is in the AdminDown state.

BFD migrates the state machine based on the local session state and received BFD packets from the peer end.

A BFD state machine is established and torn down using a three-way handshake mechanism, to ensure that both ends know the status change.

❖ **Transmission Interval and Detection Time**

Both ends negotiate BFD parameters during the establishment of a BFD session, to determine the transmission interval and detection time.

After a BFD session is established, both ends can dynamically negotiate BFD parameters (for example, minimum transmission interval and minimum receiving interval). After protocols at both ends transmit relevant negotiation packets, they adopt the new transmission interval and detection time, without affecting the current state of the session.

Overview

Feature	Description
BFD Session Establishment	Establishes a BFD session.
BFD Session Detection	Rapidly detects a bidirectional forwarding path.
BFD Support for Applications	Rapidly advertises the BFD detection result.
BFD Protection	Protects BFD from attacks for stability.
BFD Flapping Dampening	Protects stability of associated applications in the case of line instability.

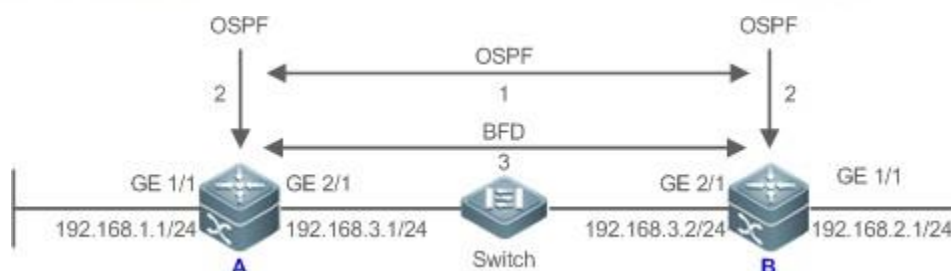### 5.3.1 BFD Session Establishment

BFD detection starts from the establishment of a BFD session.

Working Principle

❖ **Session Establishment Process**

BFD itself is unable to discover neighbors. It needs an upper-layer protocol to specify a neighbor to establish a session. As shown in the following figure, two routers running OSPF and BFD are connected through a Layer-2 switch. Figure 5-5

BFD session establishment process:

1. OSPF discovers a neighbor and establishes a connection with the neighbor.

2. OSPF instructs BFD to establish a session with the neighbor.

3. BFD establishes a session with the neighbor.

❖   **BFD Session Establishment Mode**

The BFD protocol specifies that a BFD session can be established in two modes:

▪   Active mode

   Before the establishment of a session, BFD actively transmits a control
   packet for establishing a BFD session regardless of whether it
   receives a control packet for establishing a BFD session from the peer
   end.

▪   Passive mode

   BFD does not actively transmit a control packet for establishing a BFD
   session before a session is established but wait till it receives a control
   packet for establishing a BFD session from the peer end.

The passive mode is not supported currently.

❖   **Negotiation of BFD Session Parameters**

Both ends negotiate BFD session parameters during the establishment of a
BFD session, to determine the transmission interval and detection time. Pay
attention to the following points:

1. BFD session parameters (including **Desired Min Tx Interval**, **Required Min RX
   Interval**, and **Detect Mult**) must be set for interfaces at both ends. Otherwise,
   a BFD session cannot be established.

2. Interfaces at both ends negotiate BFD session parameters and detect the
   session based on the parameters during the establishment of a BFD session.

3. After a BFD session is established, both ends can dynamically negotiate BFD
   parameters (for example, minimum transmission interval and minimum
   receiving interval). After protocols at both ends transmit relevant negotiation
   packets, they adopt the new transmission interval and detection time, without
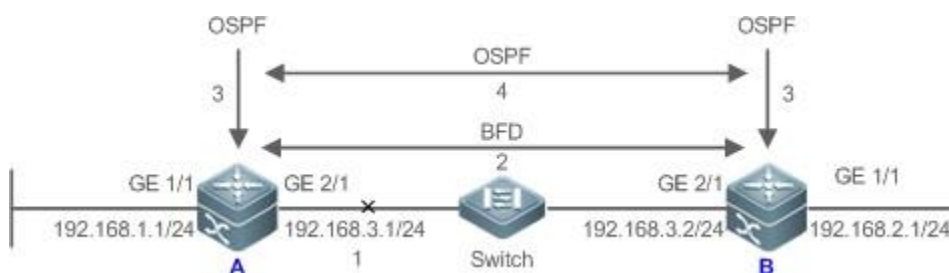   affecting the current state of the session.

5.3.2   BFD Session Detection

Link detection starts after the establishment of a BFD session. BFD periodically transmits BFD control packets. If it fails to receive BFD packets from the peer end within the detection time, it deems that the session is Down and notifies the associated application to accelerate the convergence.

Working Principle

❖   **Detection Process**

As shown in the following figure, two routers running OSPF and BFD are connected through a Layer-2 switch. Figure 5-6

Handling procedure after a BFD session is Down:

1.   The link between Router A and Switch fails.

2.   The BFD session between Router A and Router B is Down.

3.   BFD notifies the local OSPF that the forwarding path to the neighbor is faulty.

4.   OSPF processes the neighbor Down situation. If a backup forwarding path is available, it starts protocol convergence to enable the alternative forwarding path.

❖   **Detection Mode**

BFD supports the following detection modes:

▪   Asynchronous mode

In asynchronous mode, systems transmit BFD control packets periodically to each other. If a system fails to receive BFD control packets from the peer end within the detection time, it advertises that the session is Down.

▪   Query mode

In query mode, it is assumed that each system has an independent method for confirming its connection with other systems. After a BFD session is established, the system stops transmitting BFD control packets unless it needs to explicitly verify the connectivity. In such a case, the system transmits a shot-sequence BFD control packet. If a system fails to receive a returned packet within the detection time, it advertises that the session is Down. If it receives a response from the peer end, the forwarding path is reachable.

▪   Echo mode

In echo mode, the local system periodically transmits BFD echo packets and a remote system receives and loops back the packets through the forwarding path. If the local system fails to receive several consecutive echo packets within the detection time, it advertises that the session is Down. The echo function can be used together the preceding two detection modes. The echo packet detection function does not require the involvement of the control plane of the remote system. Packets are returned by the forwarding plane of the remote system, which reduces the delay and ensures faster fault detection in comparison with transmission of control packets. The enabling of the echo function in asynchronous mode can greatly

reduce transmission of control packets because the detection is accomplished by the echo function. The enabling of the echo function in query mode can thoroughly cancel transmission of control packets after a session is established. The echo function must be enabled at both ends of a BFD session. Otherwise, the echo function does not take effect.

The query mode is not supported and cannot be configured at present.

Only BFD session version 1 supports the BFD echo mode.

The echo mode is not supported for an IPv6 BFD session with the link-local address as the source or destination address.

5.3.3   BFD Support for Applications

By BFD support, the associated applications can utilize the fast fault detection of BFD to improve the protocol convergence performance. In general, the fault detection time can be shortened within 1 second.

Working Principle

After BFD support for a certain application is enabled, a BFD session is established based on the BFD configuration. When a link fault occurs, BFD can rapidly identify the fault and notify the associated application to process, thereby improving its convergence. Currently, BFD supports the following applications:

▪   BFD support for RIP

After BFD support for the Routing Information Protocol (RIP) is enabled, RIP can utilize the BFD fault detection, which is faster than the ND mechanism of RIP, to improve the protocol convergence. In general, the fault detection time can be shortened within 1

second.

For more details about BFD support for RIP, see *Configuring RIP*.

▪   BFD support for OSPF

After BFD support for OSPF is enabled, OSPF can utilize the BFD fault detection, which is faster than the ND mechanism of OSPF, to improve the protocol convergence. In general, the fault detection time can be shortened within 1 second.

For more details about BFD support for OSPF, see *Configuring OSPF*.

- BFD support for OSPFv3

After BFD support for OSPFv3 is enabled, OSPFv3 can utilize the BFD fault detection, which is faster than the ND mechanism of OSPFv3, to improve the protocol convergence. In general, the fault detection time can be shortened within 1 second.

For more details about BFD support for OSPFv3, see *Configuring OSPFv3*.

- BFD support for BGP

After BFD support for the Border Gateway Protocol (BGP) is enabled, BGP can utilize the BFD fault detection, which is faster than the ND mechanism of BGP, to improve the protocol convergence. In general, the fault detection time can be shortened within 1 second.

For more details about BFD support for BGP, see *Configuring BGP*.

- BFD support for IS-IS

The Intermediate System to Intermediate System (IS-IS) protocol dynamically discovers a neighbor by using hello packets. After BFD is enabled, IS-IS uses BFD to establish a BFD session with a neighbor that is in the Up state and detect the neighbor status. When a BFD neighbor fails, IS-IS immediately performs network convergence. The convergence time can be shortened from 30 seconds (by default, on a point-to-point network, IS-IS hello packets are transmitted at an interval of 10 seconds and the neighbor failure time is triple the interval, that is, 30 seconds) to 1 second.

For more details about BFD support for IS-IS, see *Configuring IS-IS*.

- BFD support for static routing

After BFD support for static routing is enabled, BFD prevents routers from selecting an unavailable static route as the forwarding path during routing and enables routers to rapidly switch to an available backup forwarding path.

Different from dynamic routing protocols, static routing does not have the ND mechanism. Therefore, after BFD support for static routing is configured, the next-hop reachability of a static route relies on the BFD session state. If a BFD session detects a fault, the next hop of a static route is unreachable and the static route is not added to the RIB.

If the remote system deletes a BFD session during the establishment of a BFD session, the BFD session becomes Down. In this case, the system ensures that the forwarding behavior of static routing is not affected.

For more details about BFD support for static routing, see *Configuring NSM*.

- BFD support for PBR

After BFD support for PBR is configured, BFD prevents routers from selecting an unavailable policy route as the forwarding path during routing and enables routers to rapidly switch to an available backup forwarding path.

BFD support for PBR is equivalent to that for static routing. BFD tracks and detects the forwarding path to a specified neighbor. When a BFD session fails, BFD notifies the PBR that the next hop is unreachable. Then, the policy route to the next hop does not take effect.

If the remote system deletes a BFD session during the establishment of a BFD session, the BFD session becomes Down. In this case, the system ensures that the PBR forwarding behavior is not affected.

For more details about BFD support for PBR, see *Configuring PBR*.

▪   BFD support for VRRP

The BFD support for the Virtual Router Redundancy Protocol (VRRP) can replace the ND mechanism of VRRP to rapidly detect the running status of the active and standby routers. When a fault occurs, it accelerates the active/standby router switching and improves network performance. In general, the fault detection time can be shortened within 1 second.

VRRP can also utilize BFD to track a specified neighbor. If the forwarding path to the neighbor fails during a BFD session, it automatically lowers the VRRP priority to a certain extent to trigger active/standby router switching. This configuration takes effect only when the dynamic routing protocol or other applications notify BFD to establish a session with a neighbor.

For more details about BFD support for VRRP, see *Configuring VRRP*.

▪   BFD support for VRRP Plus

The BFD support for VRRP Plus can replace the BVF detection conducted by the balancing virtual gateway (BVG) of VRRP Plus to rapidly detect the running status of balancing virtual functions (BVFs). When a fault occurs, it accelerates the forwarding entity switching and improves network performance. In general, the fault detection time can be shortened within 1 second.

VRRP Plus is based on the VRRP protocol. Therefore, no additional configuration is required for BFD support and only VRRP needs to be enabled on devices at both ends and a BFD session is correctly associated.

For more details about BFD support for VRRP Plus, see *Configuring VRRP Plus*.

▪   BFD support for Layer-3 interfaces

BFD supports changing status of Layer-3 interfaces. In interface configuration mode, use the **bfd bind peer-ip** command to detect the direct address of a specified Layer-3 interface. After this CLI command is executed, a BFD session is created and the status of a Layer-3 interface can be changed based on the detection result of the BFD session, for example, BFD Down or BFD Up. This function is often used in various types of fast

reroute (FRR), which uses BFD to detect the interface status to implement fast FRR switching.

Only LDP FRR switching is supported in BFD support for Layer-3 interfaces.

▪ BFD support for AP member ports

After BFD support for AP member ports is enabled, BFD can rapidly detect a fault occurring on a member port link so that traffic on this link is rapidly distributed to other effective member links. In general, the fault detection time can be shortened within 1 second.

For more details about BFD support for AP member ports, see *Configuring AP*.

5.3.4   BFD Protection

The BFD protection is used to protect BFD against session flapping caused by attacks (for example, a large number of ping packets attack devices).

Working Principle

The BFD protocol is very sensitive. If a BFD-enabled device is attacked (for example, attacked by a large number of ping packets) and BFD sessions flap, the BFD protection can be configured to provide protection. If both BFD and BFD protection are enabled on a device, the device discards the BFD packet from the previous hop, affecting the establishment of a BFD session between the previous-hop device and other devices.

5.3.5   BFD Flapping Dampening

A BFD session may frequently switch over between Down and Up due to link instability. As a result, an associated application (such as static routing) may frequently switch forwarding paths and the running services are affected. The BFD flapping dampening can solve this problem.

Working Principle

A BFD session may frequently switch over between Down and Up. This function allows users to set the delay for status change advertisement. After a BFD session is Up for a certain period of time, BFD notifies an associated application of BFD Up. Otherwise, BFD notifies an associated application of BFD Down.

5.4   Configuration

Configuration	Description and Command	
Configuring BFD Basic Functions	(Mandatory) It is used to establish a BFD session.	
	bfd interval	Sets BFD parameters.
	N/A	Configures the BFD support for applications. The configuration command varies with the associated applications. For details, see their configuration guides.
	(Optional) It is used to configure the BFD detection mode, slow timer, and BDF support for Layer-3 interfaces.	
	bfd echo	Configures the BFD echo mode.
	bfd slow-timer	Configures the BFD slow timer.
	bfd bind peer-ip	Configures the BFD support for Layer-3 interfaces.
Configuring BFD Protection	(Optional) It is used to protect BFD against attacks.	
	bfd cpp	Enables BFD protection.
Configuring BFD Flapping Dampening	(Optional) It is used to protect associated protocols against BFD flapping.	
	bfd up-dampening	Configures BFD flapping dampening.

5.4.1 Configuring BFD Basic Functions
Configuration Effect

- Configure BFD support for applications.

- Establish a BFD session.

- A BFD session detects link faults.

Notes

- Pay attention to the following points when setting BFD session parameters:
1. It is recommended that parameter settings be consistent at both ends of a BFD session, to ensure that application protocols associated with BFD

take effect simultaneously and prevent occurrence of one-way forwarding due to different dampening time at both ends.

2. Take into account of transmission bandwidth differences of different interfaces when setting parameters. If the minimum transmission interval and minimum receiving interval are set to very small values, data transmission may be affected due to very large BFD bandwidth occupancy.

- Pay attention to the following points when configuring BFD support for applications:

1. Ensure that it is enabled on neighbors of a BFD session. Otherwise, a BFD session cannot be established. If a dynamic routing protocol or another application requires BFD to establish a session with a neighbor, the BFD session can also be established.

2. If the interface specified by a BFD session is different from the actual BFD packet outbound interface because of IP routing, or if the interface specified during BFD session creation is different from the actual BFD packet inbound interface, a BFD session cannot be established.

- Pay attention to the following points when configuring the BFD detection mode:

1. In the process that the forwarding plane of the peer device returns echo packets transmitted by the local end to the local end, the echo packets may be lost due to congestion of the peer device, causing a session detection failure. In this case, configure Quality of Service (QoS) policies to ensure that echo packets are processed preferentially or disable the echo function.

2. The echo detection function of BFD does not support multi-hop detection. Ensure that the echo function is disabled when configuring multi-hops.

3. The echo mode takes effect only after this mode is enabled at both ends of a BFD session.

4. Before enabling the echo mode of BFD, run the **no ip redirects** command on the neighbors of a BFD session to disable the function of ICMP packet redirection, and run the **no ip deny land** command to disable the Distributed Denial of Service (DDoS) function (prevent the Land-based attack).

Configuration Steps

❖ **Setting BFD Parameters**

- Mandatory.

- BFD parameters need to be set at BFD session egresses of routers at both ends detected by BFD if no special requirements are raised.

- Take into account of transmission bandwidth differences of different interfaces when setting parameters. If the minimum transmission interval and minimum receiving interval are set to very small values, data transmission may be affected due to very large BFD bandwidth occupancy.

Command	bfd interval *milliseconds* min_rx *milliseconds* multiplier *interval-multiplier*

Parameter Description	**interval** *milliseconds*: Indicates the minimum TX interval, with the unit of milliseconds.
	min_rx *milliseconds*: Indicates the minimum RX interval, with the unit of milliseconds.
	multiplier *interval-multiplier*: Indicates the detection timeout multiplier.
Defaults	No BFD session parameter is configured.
Command Mode	Interface configuration mode
Usage Guide	The fast forwarding function must be enabled before the BFD function is enabled on routers.

❖ **Enabling the BFD Echo Mode**

▪ (Optional) Ports run in asynchronous mode by default. If a BFD session needs to run in echo mode, the echo mode needs to be configured.

▪ Complete the configuration on ports of switches or routers.

▪ A session runs in asynchronous mode as long as either of routers at both ends is configured to run in asynchronous mode. If routers at both ends are configured to run in echo mode by default, a BFD session finally runs in echo mode.

Command	bfd echo
Parameter Description	N/A
Defaults	The BFD echo mode is disabled.
Command Mode	Interface configuration mode
Usage Guide	This command cannot be configured on AP ports.
	By default, when BFD session parameters are set, the system automatically enables the echo mode.
	The minimum TX interval and minimum RX interval of echo packets adopt the **Interval milliseconds** and
	min_rx milliseconds parameters of a session.
	Before enabling the echo mode of BFD, run the **no ip redirects** command on the neighbors of a BFD
	session to disable the function of ICMP packet redirection, and run the **no ip deny land** command to disable the Distributed Denial of Service

(DDoS) function (prevent the Land-based attack).

❖ **Configuring the BFD Slow Timer**

▪ (Optional) The default slow timer is 3,000 milliseconds. The value can be changed as required.

▪ Configure this function in global configuration mode of switches or routers.

▪ In BFD echo mode or session building, the slow timer is used to control packets. If the value increases, the required time for negotiating and establishing a BFD session becomes longer, and the time required for transmitting slow BFD packets in echo mode is longer.

Command	bfd slow-timer [*milliseconds*]
Parameter Description	*milliseconds***:** Indicates the BFD slow timer, with the unit of milliseconds. The value ranges from 1,000 to 30,000 and the default value 2,000 is adopted if it is not set.
Defaults	The transmission interval of slow control packets is 2,000 milliseconds.
Command Mode	Global configuration mode
Usage Guide	This command is used to specify the slow timer in echo mode.

❖ **Configuring the BFD Support for Layer-3 Interfaces**

▪ (Optional) Currently, this function is used only when MPLS LDP is used for FRR.

▪ Configure this function on interfaces of switches or routers.

Command	bfd bind peer-ip *src-address* [source-ip *dst-address*] process-pst
Parameter Description	*src-address*: Indicates the peer IP address of an interface. *dst-address*: Indicates the local IP address of an interface.
Defaults	BFD support for Layer-3 interfaces is not configured by default.

Command Mode	Interface configuration mode
Usage Guide	This command is used to enable BFD support for Layer-3 interfaces so as to rapidly detect connectivity of Layer-3 interfaces.

❖ **Configuring the BFD Support for Applications**

▪ Mandatory.

▪ This function is disabled by default.

▪ The configuration command varies with the associated applications. For details, see their configuration guides.

▪ This function must be configured at both ends so that a BFD session can be established.

▪ In RIP routing configuration mode, run the **bfd all interfaces** command to enable BFD support for RIP on all interfaces. For details, see *Configuring RIP*.

▪ In OSPF routing configuration mode, run the **bfd all interfaces** command to enable BFD support for OSPF on all interfaces. For details, see *Configuring OSPF*.

▪ In OSPFv3 routing configuration mode, run the **bfd all interfaces** command to enable BFD support for OSPFv3 on all interfaces. For details, see *Configuring OSPFv3*.

▪ In BGP routing configuration mode, run the **neighbor** *address* **fall-over bfd** command to enable BFD support for BGP. For details, see *Configuring BGP*.

▪ In IS-IS routing configuration mode, run the **bfd all interfaces** command to enable BFD support for IS-IS on all interfaces. For details, see *Configuring IS-IS*.

▪ In global configuration mode, run the **ip route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* [source *ip-address*] command to enable BFD support for static routing. For details, see *Configuring NSM*.

▪ Run the **set ip next-hop verify-availability** *next-hop-address* **bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* command to enable BFD support for PBR. For details, see *Configuring PBR*.

▪ Run the **set ipv6 next-hop verify-availability** *next-hop-address* **bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* command to enable BFD support for IPv6 PBR. For details, see *Configuring PBR*.

▪ Run the **vrrp bfd** *interface-type interface-number ip-address* command to enable BFD support for VRRP. For details, see *Configuring VRRP*.

▪ VRRP Plus is based on the VRRP protocol. Therefore, no additional configuration is required for BFD support for VRRP Plus. Only VRRP needs to
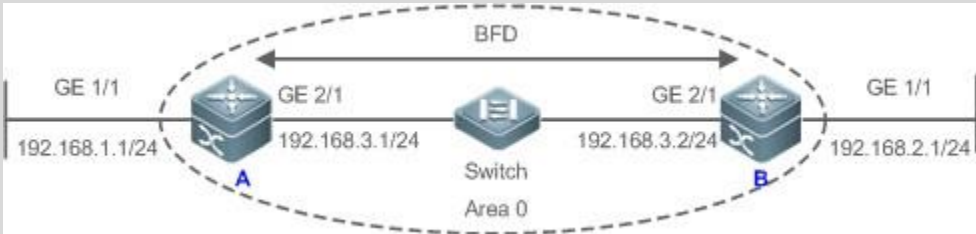
be enabled on devices at both ends and a BFD session is correctly associated.

Verification

- The verification command varies with the associated applications. For details, see their configuration guides.

Configuration Example

❖ **Configuring BFD support for OSPF**

Scenario Figure 5-7	
Configuration Steps	- Configure IP addresses for interconnected interfaces of Router A and Router B. - Run OSPF on Router A and Router B. - Set BFD parameters for interconnected interfaces of Router A and Router B. - Enable BFD support for OSPF on Router A and Router B.

A	`A#configure terminal A(config)#interface GigabitEthernet2/1`
	`A(config-if-GigabitEthernet2/1)# no switchport  //The configuration is not required on routers.`
	`A(config-if-GigabitEthernet2/1)#ip address 192.168.3.1 255.255.255.0`
	`A(config-if-GigabitEthernet2/1)#bfd interval 200 min_rx 200 multiplier 5 A(config-if-GigabitEthernet2/1)# exit`
	`A(config)#interface GigabitEthernet1/1`
	`A(config-if-GigabitEthernet1/1)# no switchport  //The configuration is not required on routers.`
	`A(config-if-GigabitEthernet1/1)#ip  address  192.168.1.1  255.255.255.0 A(config-if-GigabitEthernet1/1)# exit`
	`A(config)# router ospf 123`
	`A(config-router)# log-adj-changes detail`
	`A(config-router)# network 192.168.3.00.0.0.255 area 0`
	`A(config-router)# network 192.168.1.00.0.0.255 area 0 A(config-router)# bfd all-interfaces`

	`A(config-router)# end`

B	B#configure terminal B(config)#interface GigabitEthernet2/1
	B(config-if-GigabitEthernet2/1)# no switchport //The configuration is not required on routers.
	B(config-if-GigabitEthernet2/1)#ip address 192.168.3.2 255.255.255.0
	B(config-if-GigabitEthernet2/1)#bfd interval 200 min_rx 200 multiplier 5 B(config-if-GigabitEthernet2/1)# exit
	B(config)#interface GigabitEthernet1/1
	B(config-if-GigabitEthernet1/1)# no switchport //The configuration is not required on routers.
	B(config-if-GigabitEthernet1/1)#ip address 192.168.2.1 255.255.255.0 B(config-if-GigabitEthernet1/1)# exit
	B(config)# router ospf 123
	B(config-router)# log-adj-changes detail
	B(config-router)# network 192.168.3.00.0.0.255 area 0
	B(config-router)# network 192.168.2.00.0.0.255 area 0 B(config-router)# bfd all-interfaces
	B(config-router)# end
Verification	Display verification.
A	A# show bfd neighbors details
	OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int 192.168.3.1 192.168.3.2 1/2 Up 532 (3) Up Ge2/1
	Local Diag: 0, Demand mode: 0, Poll bit: 0
	MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
	Received MinRxInt: 50000, Received Multiplier: 3
	Holdown (hits): 600(22), Hello (hits): 200(84453)
	Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 Registered protocols: OSPF
	Uptime: 02:18:49
	Last packet: Version: 1 - Diagnostic:0
	I Hear You bit: 1 - Demand bit: 0
	Poll bit: 0 - Final bit: 0
	Multiplier: 3 - Length: 24
	My Discr.: 2 - Your Discr.: 1 Min tx interval: 50000 - Min rx interval: 50000 Min Echo interval: 0

| B | `B# show bfd neighbors details`

`OurAddr    NeighAddr   LD/RD   RH/RS   Holdown(mult)`
`           State       Int 192.168.3.2 192.168.3.1     2/1     Up 532 (5 )`

`Local Diag: 0, Demand mode: 0, Poll bit: 0`

`MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3`

`Received MinRxInt: 200000, Received Multiplier: 5`

`Holdown (hits): 600(22), Hello (hits): 200(84453)`

`Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago Registered protocols: OSPF`

`Uptime: 02:18:49`

`Last packet: Version: 1 - Diagnostic: 0`
`I Hear You bit: 1      - Demand bit: 0`
`Poll bit: 0            -`
`Final bit: 0 Multiplier: 5-`
`Length: 24`
`My Discr.: 1         - Your Discr.: 2`
`Min tx interval: 200000 - Min rx`
`interval: 200000 Min Echo interval:`
`0` |

❖ Configuring BFD Support for BGP

Scenario Figure 5-8	
Configuration Steps	▪ Configure IP addresses for ports connecting Router A and Router B. ▪ Run the OSPF protocol on Router A and Router B. ▪ Configure IP addresses for ports connecting Router B and Router C. ▪ Run the OSPF protocol on Router B and Router C. ▪ Configure EBGP on Router A and Router C, and enable BFD support for BGP.

| A | ```
A# configure terminal
A(config)# interface GigabitEthernet2/1
A(config)# bfd multi-hop interval 200 min_rx 200 multiplier 5 A(config-if-GigabitEthernet2/1)# no switchport
//This command is required on the switch
A(config-if-GigabitEthernet2/1)# ip address 192.168.3.1 255.255.255.0 A(config-if-GigabitEthernet2/1)# exit
A(config)# interface GigabitEthernet1/1 A(config-if-GigabitEthernet1/1)# no switchport
//This command is required on the switch
A(config-if-GigabitEthernet1/1)# ip address 192.168.1.1 255.255.255.0 A(config-if-GigabitEthernet1/1)# exit
A(config)# router ospf 123
A(config-router)# log-adj-changes detail
A(config-router)# network 192.168.3.0 0.0.0.255 area 0
A(config-router)# network 192.168.1.0 0.0.0.255 area 0 A(config-router)# exit
A(config)#router bgp 100
A(config-router)# neighbor 192.168.4.1 remote-as 200
A(config-router)# neighbor 192.168.4.1 ebgp-multihop 3
A(config-router)#  neighbor  192.168.4.1  update-source  192.168.3.1 A(config-router)# neighbor 192.168.4.1 fall-over bfd
A(config-router)# end
``` |
|---|---|
| B | ```
B# configure terminal
B(config)# interface GigabitEthernet2/1 B(config-if-GigabitEthernet2/1)# no switchport
//This command is required on the switch
B(config-if-GigabitEthernet2/1)# ip address 192.168.3.2 255.255.255.0
``` |
|  | ```
B(config-if-GigabitEthernet2/1)#     exit     B(config)#     interface GigabitEthernet2/2 B(config-if-GigabitEthernet2/2)# no switchport
//This command is required on the switch
B(config-if-GigabitEthernet2/2)# ip address 192.168.4.2 255.255.255.0 B(config-if-GigabitEthernet2/2)# exit
B(config)# router ospf 123
B(config-router)# log-adj-changes detail
B(config-router)# network 192.168.3.0 0.0.0.255 area 0
B(config-router)# network 192.168.4.0 0.0.0.255 area 0 B(config-router)# end
``` |

| **C** | ```
C# configure terminal
C(config)# interface GigabitEthernet2/1
C(config)# bfd multi-hop interval 200 min_rx 200 multiplier 5 C(config-if-GigabitEthernet2/1)# no switchport
//This command is required on the switch
C(config-if-GigabitEthernet2/1)# ip address 192.168.4.1 255.255.255.0 C(config-if-GigabitEthernet2/1)# exit
C(config)# interface GigabitEthernet1/1 C(config-if-GigabitEthernet1/1)# no switchport
//This command is required on the switch
C(config-if-GigabitEthernet1/1)# ip address 192.168.2.1 255.255.255.0 C(config-if-GigabitEthernet1/1)# exit
C(config)# router ospf 123
C(config-router)# log-adj-changes detail
C(config-router)# network 192.168.4.0 0.0.0.255 area 0
C(config-router)# network 192.168.2.0 0.0.0.255 area 0 C(config-router)# exit
C(config)#router bgp 200
C(config-router)# neighbor 192.168.3.1 remote-as 200
C(config-router)# neighbor 192.168.3.1 ebgp-multihop 3
C(config-router)# neighbor 192.168.3.1 update-source 192.168.4.1 C(config-router)# neighbor 192.168.3.1 fall-over bfd
C(config-router)# end
``` |
| **Verification** | Check whether the configurations take effect. |
| **A** | ```
A# show bfd neighbors details
 OurAddr    NeighAddr   LD/RD   RH/RS   Holdown(mult)   State   Int 192.168
 Session state is Up and not using echo function.
 Local Diag: 0,     Demand mode: 0,     Poll bit: 0
``` |
|  | ```
MinTxInt: 2000000,    MinRxInt: 2000000,     Multiplier: 5
Received MinRxInt 2000000, Multiplier: 5
 Holdown (hits): 10000(1), Hello
 (hits): 2000(150)  Rx Count: 31, Rx
 Interval (ms) min/max/avg: 0/0/2000
Tx  Count: 206,  Tx  Interval  (ms)  min/max/avg:  0/0/2000  Registered
protocols: BGP
Uptime: 0:00:50 Last packet:
 Version       :       1             - Diagnostic  : 3
 State bit     :      Init           - Demand bit   : 0
 Poll bit      :       0             - Final bit    : 0
 Multplier     :       5             - Length       : 24
 My Discr      :     8192            - Your Discr   : 8192
 Min tx interval  :2000000           - Min rx
  interval: 2000000 Min Echo interval:        0
``` |

| C | ```
B# show bfd neighbors details

OurAddr    NeighAddr   LD/RD   RH/RS   Holdown(mult)   State   Int 192.168
Session state is Up and not using echo function.
Local Diag: 0,        Demand mode: 0,      Poll bit: 0
MinTxInt: 2000000,        MinRxInt: 2000000,       Multiplier: 5
Received MinRxInt 2000000, Multiplier: 5
Holdown (hits): 10000(0), Hello (hits): 2000(794)
Rx Count: 5280, Rx Interval (ms) min/max/avg: 0/0/2000 Tx Count: 2470,
Tx Interval (ms) min/max/avg: 0/0/2000 Registered protocols: BGP
Uptime: 0:01:13 Last packet:
 Version        :       1           - Diagnostic  : 0
 State bit      :       Up          - Demand bit   : 0
 Poll bit       :       0           - Final bit    : 0
 Multplier      :       5           - Length       : 24
 My Discr       :     8192          - Your Discr   : 8192
 Min tx interval  :2000000          - Min rx
 interval: 2000000 Min Echo interval:        0
``` |

Common Errors

- BFD parameters are not set for device interfaces at one end.

- The BFD support for applications is disabled.

- The BFD support for applications is enabled only at one end.

5.4.2   Configuring BFD Protection

Configuration Effect

- If a BFD-enabled device is attacked (for example, attacked by a large number of ping packets) and BFD session flaps accordingly, the BFD protection can be enabled to provide protection.

Notes

- The BFD basic functions must be configured.

- If both BFD and BFD protection are enabled on a device, the device discards the BFD packet from the previous hop, affecting the establishment of a BFD session between the previous-hop device and other devices.

- This function and limitations are applicable only to switches.

Configuration Steps

❖ **Enabling BFD Protection**

- Optional.

- Configure this function in global configuration mode on switches or routers.

- The BFD protection function raises the processing priority of BFD packets and ensures normal running of BFD services in a scenario in which devices are attacked.

Command	bfd cpp
Parameter Description	N/A
Defaults	The BFD protection function is enabled by default.
Command Mode	Global configuration mode
Usage Guide	Enable the BFD protection function to provide protection if a device encounters BFD flapping due to attacks.

Verification

Run the **show running-config** command to verify the configuration on an interface.

Configuration Example

❖ **Enabling BFD Protection**

Configuration Steps	▪ **Configure this function on a switch on a network where attacks exist.** ▪ **Configure the BFD protection function.**
	`QTECH#configure terminal` `QTECH(config)# bfd cpp QTECH(config)# end`
Verification	N/A

5.4.3 Configuring BFD Flapping Dampening
Configuration Effect

▪ A BFD session may frequently switch over between Down and Up due to link instability. As a result, a relevant application (such as static routing) may frequently switch forwarding paths and the running services are affected.

▪ Users can set the delay for status change advertisement, after which BFD notifies an associated application of BFD Up. After a BFD session is Up for a certain period of time, BFD notifies an associated application of BFD Up. Otherwise, BFD notifies it of BFD Down. The purpose is to reduce flapping of associated protocols caused by instable links.

Notes

▪ The BFD basic functions must be configured.

▪ If a BFD session does not frequently switch over between Down and Up, the

enabling of BFD flapping dampening will delay notifying an associated application of BFD Up.

Configuration Steps

❖ **Configuring BFD Flapping Dampening**

- (Optional) The BFD flapping dampening is disabled on ports by default. If a BFD session frequently switches over between Down and Up, it is advised to enable this function.

- Configure this function on ports of switches or routers.

- With BFD flapping dampening enabled, it is relieved that associated applications, such as route re-calculation, process quantities of advertisements because of frequent status BFD change. The larger the configured time is, the longer the required BFD stability time is. BFD notifies an application module of BFD Up only after the stability time reaches the configured time.

Command	bfd up-dampening[*milliseconds*]
Parameter Description	*milliseconds*: Indicates the delay for status change advertisement, after which BFD notifies an associated application of BFD Up, with the unit of milliseconds. The value ranges from 0 to 300,000. The value 0 indicates that BFD notifies the application layer immediately when a session switches over from Down to Up and the default value is 0.
Defaults	The BFD flapping dampening function is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	This function needs to be enabled only when the link is instable. If a BFD session does not frequently switch over between Down and Up, the enabling of BFD flapping dampening will delay notifying an associated application of BFD Up.

Verification

Run the **show running-config** command to verify the configuration on an interface.

Configuration Example

❖ **Configuring BFD Flapping Dampening with the Advertisement Delay as 60,000 Milliseconds**

Configuration Steps	▪ **Configure this function in an environment where BFD frequent flaps due to link instability.** ▪ **Set the delay for status change advertisement to 60,000 milliseconds.**
	```QTECH#configure terminal``` ```QTECH(config)# interface fastEthernet 0/2 QTECH(config)# bfd up-dampening 60000 QTECH(config)# end```
Verification	N/A

5.5 Monitoring

Displaying

Description	Command
Displays BFD session information.	**show bfd neighbors** [**vrf** *vrf-name*] [**client** {**ap** |**bgp**|**ospf**|**rip**|**vrrp**|**static-route** | **pbr**| **vrrp-balance** | **pst** }][**ipv4** *ip-address* | **ipv6** *ip-address*][**details**]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs BFD events.	**debug bfd event**[**interface** *interface-type interface-number* | **ipv4** *ip-address* | **ipv6** *ipv6-address*]
Debugs BFD packets.	**debug bfd packet**[**interface** *interface-type interface-number* | **ipv4** *ip-address* | **ipv6** *ipv6-address*]

6.1   Overview

When the Layer-3 port on a Layer-3 device frequently goes Up and Down due to manual enabling/disabling or other external causes, the routing table on the device will flap repeatedly. If a routing protocol is configured, the protocol may propagate the flap to the entire network, causing repeated updates and recalculation of neighboring routes, which wastes network bandwidths and destabilizes the network. Repeated route updates and recalculation on devices consume many CPU resources, which affects the normal running of customer networks.

IP Event Dampening detects abnormal Up/Down flapping and automatically suppresses frequent port state changes, which prevents the propagation of single-point link failures by a routing protocol. When the port is restored, it will be automatically unsuppressed, thus reducing network flaps and CPU resource consumption while improving network stability.

Protocols and Standards

- RFC2439: BGP Route Flap Dampening

At its core, the suppression algorithm used by IP Event Dampening is the same as that used by BGP Route Flap Dampening.

6.2   Applications

Application	Description
Routed Port Flap Dampening	Monitors the state change of the Layer-3 port on a router, and suppresses frequent port flapping.

6.2.1   Routed Port Flap Dampening
Scenario

In a network that runs a routing protocol, when a port on a router connected to another router frequently goes Up and Down, neighboring routes will be repeatedly updated and recalculated. The routing protocol may propagate the flap to the entire network, causing a network flap. IP Event Dampening can be enabled on the connected routers to monitor port state changes and suppress frequent port flapping, thus reducing network flaps and CPU resource

consumption while improving network stability.

Figure 6-1

Remarks	A and B are routers.

Deployment

Configure IP Event Dampening on portGE0/1 on Router A and portGE0/1 on Router B respectively.

The subinterfaces and the virtual templates of interfaces on routers do not support the dampening feature.

6.3   Features

Basic Concepts

❖ Penalty

A port that goes Up or Down gets a penalty for each state change, but the penalty decays exponentially when the port is stable. In this way, port behaviors can be sensed and controlled intelligently.

❖ **Suppress Threshold**

When the cumulative penalty of a port exceeds a suppress threshold, the port is considered to flap and will be suppressed.

❖ **Half-Life Period**

The half-life period is the period required for the penalty to decrease to half of the original value when the port is stable. It defines the speed at which the penalty decays exponentially. The shorter the half-life period, the faster the penalty decays, and the faster the port is detected to be stable, but the flap detection sensitivity is reduced.

❖ **Reuse Threshold**

When the port no long flaps and its penalty decays to a certain degree (below the suppress threshold), the port is considered to be stable and is unsuppressed.

❖ **Maximum Suppress Time**

When a port keeps flapping and reaches a very large penalty, the port will not be usable for a long time. To avoid this problem, the maximum suppress time is defined to always maintain the port suppression duration below a certain value no matter how long the port has flapped.

Overview

Feature	Description
Port Flap Suppression	Configure the criteria and parameters of flap suppression on ports to enable switches or routers to identify and suppress frequently flapping ports, which ensures route stability and avoids route flap propagation.

6.3.1 Port Flap Suppression
Working Principle

A port configured with IP Event Dampening is assigned a penalty. The port gets a penalty of 1,000 each time when it goes Down, but the penalty decreases with time. If the port goes Down again, the penalty increases accordingly. When the cumulative penalty exceeds the suppress threshold, the port will be suppressed. For the affected upper-layer protocol, the suppressed port is always Down no matter what the actual port state is. When the penalty decreases to the reuse threshold, the port will be unsuppressed, and the upper-layer protocol can sense the actual port state.

If a Layer-3 port is not configured with IP Event Dampening, or is not suppressed by it, the routing protocol or other protocol concerned about the port status still work normally. When the port is suppressed, the upper-layer protocol considers the port to be Down. Any state change of the port before the port is unsuppressed does not affect the routing table and the route calculation and advertisement performed by the upper-layer routing protocol.

Related Configuration

❖ **Configuring IP Event Dampening**

▪ By default, IP Event Dampening is disabled on Layer-3 ports.

▪ Run the **dampening** [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]] command to enable or disable IP Event Dampening on Layer-3 ports.

6.4 Configuration

Configuration	Description and Command

www.qtech.ru

Enabling IP Event Dampening	(Mandatory)It is used to suppress Layer-3 port flapping.	
	dampening	Configures IP Event Dampening.

6.4.1 Enabling IP Event Dampening

Configuration Effect

When a port configured with IP Event Dampening keeps flapping until the predefined threshold is exceeded, the port is set to Down.

Notes

- When a Layer-3 port on a switch is converted to a Layer-2 port (for example, from a routed port to a switch port), the IP Event Dampening configuration on the port will be deleted.

- Only the main interface on a router can be configured with IP Event Dampening. The configuration takes effect for all subinterfaces of the main interface, but you cannot run the **dampening** command directly on subinterfaces and virtual templates.

Configuration Steps

❖ **Configuring IP Event Dampening**

- Mandatory.

- Perform the configuration in Layer-3 interface configuration mode.

- You can specify the half-life period, reuse threshold, suppress threshold, maximum suppress time, and initial penalty. If you do not set these parameters, their default values will be used.

Verification

Use any one of the following commands to check whether the configuration takes effect:

- **show running-config**

- **show interfaces** [*interface-id*] **dampening**, which is used to check the IP Event Dampening configuration on a specified port

Related Commands

❖ **Enabling IP Event Dampening on a Port**

Command	dampening [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [restart [*restart-penalty*]]]]

Parameter Description	*half-life-period*: Indicates the half-life period. Value range: <1–30>; default value: 5s.
	reuse-threshold: Indicates the reuse threshold. Value range: <1–20,000>; default value: 1,000.
	suppress-threshold: Indicates the suppress threshold. Value range: <1–20,000>; default value: 2,000. *max-suppress:* Indicates the maximum suppress time. Value range: <1–255>; default value: four times the half-life period.
	restart *restart-penalty:* Indicates the initial penalty. Value range: <1–20,000>; default value: 2,000.
Command Mode	Interface configuration mode
Usage Guide	IP Event Dampening can affect direct routes, host routes, static routes, dynamic routes, and VRRP. When a port is suppressed based on the configured criteria, the affected modules determine that the port is Down and therefore delete corresponding routes. No data packet will be transmitted through the port.
	When the **dampening** command is rerun on a port configured with IP Event Dampening, the dampening information on the port will be cleared, but the flap count is retained, unless you use the **clear counters** command to clear the counters on the port.
	If the **max-suppress** parameter is set to a very small value, making the maximum penalty smaller than the
	suppress threshold, the port will never be suppressed. When such a configuration error occurs, the following message indicating a configuration failure will be printed: % Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time If the available system memory is insufficient to run the dampening command, the following message indicating a configuration failure will be printed: % No memory, configure dampening fail!

Configuration Example

❖ Configuring IP Event Dampening on Layer-3 Ports

Scenario Figure 6-2	

Configuration Steps	Enable IP Event Dampening on port GigabitEthernet 0/1 on Router A and on port GigabitEthernet 0/1 on Router B respectively, and set **half-time-period** to 30s, **reuse-threshold** to 1,500, **suppress-threshold** to 10,000, and **max-suppress** to 120s.
A	QTECH(config)#interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#dampening 30 1500 10000 100
B	QTECH(config)#interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#dampening 30 1500 10000 100
Verification	Run the **show interfaces dampening** command to check the IP Event Dampening configuration on the corresponding ports.

	```QTECH#show interfaces dampening GigabitEthernet 0/1```
	 ``` Flaps Penalty Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart```
	 ```0 0 FALSE 0 30 1500 1000 100 15119 0```

Common Errors

▪ The port on a Layer-3 switch is not converted to a routed port by using the **no swithport** command before IP Event Dampening is configured.

6.5 Monitoring

Clearing

Description	Command
Clears the interface counters.	**clear counters**

For details about the **clear counter** command, see the related chapter for the "Interface" command.

Displaying

Description	Command
Displays the counters on suppressed ports.	**show dampening interface**

Displays the IP Event Dampening configuration on ports.	**show interfaces dampening**

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Enables debugging of IP Event Dampening.	**debug dampening interface**

7.1 Overview

In order to improve the reliability of networks, the two devices at core layer and convergence layer of traditional networks are configured with two cores to provide redundancy. Access and convergence devices are respectively connected to the cores through two links. The following figure shows a typical traditional network architecture. Redundant network architecture increases the complexity of network design and operation. At the same time, a large number of redundant links reduce the utilization of network resources and return on investment.

Figure 7-1 Traditional Network Architecture

Virtual Switching Unit (VSU) is a kind of network system virtualization technology that supports combining multiple devices into a single virtualized device. As shown in Figure 7-2, access, convergence and core layer devices can respectively form VSUs, and then these VSUs connect to one another to form an end-to-end VSU network. Compared with traditional network, this networking can:

- Simplify the network topology.

- Reduce the costs of network management and maintenance.

- Shorten application recovery time and service interruption time.
- Enhance the utilization of network resources. Figure 7-2 End-to-End VSU Networking

7.2 Applications

Application	Description
Managing Multiple Devices in a Unified Manner	Uses multiple physical devices as a logical device for unified management.
Simplifying Networking Topology	Uses a VSU as a logical device to simplify the networking topology.

7.2.1 Managing Multiple Devices in a Unified Manner
Scenario

When multiple physical devices form a VSU system, the physical devices can be viewed as a logical device. All configurations are managed on the global master device.

As shown in Figure 7-3, four devices (numbered as 1, 2, 3, and 4 from left to right) form a VSU system. Device 1 is the global master device, device 2 is the global slave device, and devices 3 and 4 are the global candidate devices.

- All devices are configured simply
on the global master device. Figure 7-3

Remarks	**The devices from left to right in Figure 7-3 are Device 1, Device 2,**

	Device 3 and Device 4.
	For details on VSL, see the description in section 1.3.1.
	Device 1 is the global master device. Device 2 is the global slave device.
	Devices 3 and 4 are the global candidate devices.

Deployment

- The global master device controls the entire VSU system, runs control-plane protocols and is involved in data forwarding.

- The global slave device is involved in data forwarding, does not run control-plane protocols, and works as the backup and takes over the work of the global master device when faulty.

- The global candidate devices are involved in data forwarding and do not run control-plane protocols. When the global slave device is faulty, a global candidate device can take over the work of the global slave device. In this case, when the global master and slave devices are faulty, the VSU system will restart.

7.2.2   Simplifying Networking Topology
Scenario

In traditional networks as shown in Figure 7-4, redundant devices and lines need to be added to increase the networking reliability; however, many algorithms also need to be introduced to prevent loops, which make the networking more complex. In the VSU system, all devices are viewed as a logical device. Different devices back up each other, and no loop prevention algorithm needs to be introduced, which can simplify the network.

- Two aggregate switches form a VSU system. It is unnecessary to configure a loop prevention algorithm. The two switches are redundant mutually.

- The access switch is connected to the aggregate switches through the uplink AP.

- When a switch in the VSU system is
faulty, the other link still works. Figure 7-4

Deployment

- The global master device controls the entire VSU system, runs control-plane protocols and is involved in data forwarding.

- The global slave device is involved in data forwarding, does not run control-plane protocols, and works as the backup and takes over the work of the global master device when the global master device is faulty.

- The access switch is oriented to users and allows access by users' devices.

7.3   Features

Basic Concepts

❖ VSU System

VSU system is a single logical entity consisting of two or multiple devices in traditional network architecture. For example, the convergence layer VSU system as shown in the following figure can be seen as a single device that interacts with the core layer and access layer.

Figure 7-5 Convergence layer VSU

In the above VSU network structure, the member devices form a logical entity through internal links and the access layer devices are connected to the VSU through aggregated links. In this way, there is no layer 2 loop between the access and convergence layers.

Figure 7-6 Access layer VSU

Except the core and convergence layer devices, the access layer devices can

also form a VSU system. A server that requires high availability can adopt multiple network cards to form an Aggregate Port (AP) to connect access layer devices. Since AP can only connect to the same access device, the risk of single device fault increases. In this case, VSU can be used to solve the problem. In the VSU mode, a server adopts multiple network cards and binds them into an AP to connect different member devices in the same VSU group. This way can prevent single point failure and network interruption caused by single link failure.

❖ **VSU Domain ID**

A VSU domain has only one ID. Only the devices with the same domain IDs can form a VSU system.

❖ **Member Device ID**

Every member device in a VSU system has a unique ID, namely, Switch ID. Switch IDs can be used in device management or configuring interfaces on member devices. You need to configure an ID for a device when adding the device to a VSU system and ensure that the ID is unique in the same VSU system. If an ID conflict occurs, the VSU system will reserve one device according priority.

❖ **Member Device Role**

A VSU system consists of several devices. When establishing a VSU system, you need to select a global master device and a global slave device. All other devices are global candidate devices.

A global master device is elected from multiple devices based on an election protocol. All other devices are global slave devices in the 1: N hot standby mode. When the 1:1 hot standby mode is supported, one device is the global master device, one device is the global slave device, and all other devices are global candidate devices.

The global master device is responsible for controlling the entire VSU system, running control plane protocols and participating in data forwarding. Other devices, including the global slave devices and candidate devices, participate in data forwarding but do not run control plane protocols. All received control plane data flows are forwarded to the global master device for processing.

The global slave device also receives the statuses of the global master device in real-time and provide 1:1 or 1:N redundancy with the global master device. If the global master device becomes faulty, the global slave device will take over services from the master device and manage the entire VSU system.

The following is the method for selecting the master device of a VSU system:

1. Rules for selecting the master device of a VSU system include (Continue with the next rule if the previous rule does not help in selecting the master device): a) Select the currently running host as the master device with the highest priority (All devices are not master devices during startup). b) Select the device with the highest priority as the master device. c) Select the device with the lowest device No. as the host. d) Select the device with the smallest MAC

address as the master device.

2. In the 1:N hot standby mode, select the device that has the most familiar configurations with the master device as the slave device to prevent dual active devices. The selection order is: the nearest/the highest priority/the smallest MAC address.

3. VSU system supports hot adding a support device. Even the hot added device has a higher priority than the master device has, the VSU system does not perform active/standby switch.

4. The startup order of member device may affect the election of master device. A member device may not join in the VSU system because it starts up too slowly. In this case, the device will be hot added to the VSU system. Even the device has a higher priority than the master device, the VSU system does not perform active/standby switchover.

Overview

Feature	Description
Virtual Switching Link (VSL)	In a VSU system, a virtual link is used to connect all devices.
Topology	Describes the internal topology of a VSU system.
Dual-Active Detection (DAD)	Avoids that dual master switches coexist in a VSU domain.
System Management	Describes possible connections between external devices and VSU devices.
Quick Blinking Location	Manages devices in the VSU system.

7.3.1 Virtual Switching Link (VSL)

Working Principle

❖ VSL

The VSU system is a network entity that consists of multiple devices. These devices need to share control information and part of data streams. The VSL is a special link used for transmission of control information and data streams among devices of the VSU system. For example, the VSL can be established between two devices through 10 Gigabit Ethernet interfaces. Figure 7-7 shows the position of the VSL in the VSU system.

Figure 7-7 VSL

The VSL exists in the form of AP groups. The data streams transmitted through the VSL balance load among the aggregation port members according to the traffic balancing algorithm.

❖ **VSL Traffic**

The control streams transmitted through the VSL between devices include:

1. The protocol packets received by the member devices: These protocol packets need to be forwarded through the VSL to the global master device for processing.

2. The protocol packets processed by the global master device: These protocol packets need to be forwarded through the VSL to the interfaces of other member devices and then sent to the peer devices by these interfaces.

The data streams transmitted through the VSL between devices include:

1. The data stream flooded on the VLAN

2. The data streams that need to be forwarded across devices and transmitted through the VSL

Furthermore, the internal management packets of the VSU system are also transmitted through the VSL. The management packets include the protocol information switched by the hot backup and configuration information delivered by the host to other member devices.

In terms of the switched port analyzer (SPAN) function, the interface associated with the VSL cannot be regarded as the source port or destination port of the SPAN.

❖ **VSL Failure**

If a certain member link connected to the VSL AP group fails to work, the VSU will adjust the configurations of the VSL aggregation port automatically to prevent the traffic from being transmitted through the faulty member link.

If all member links are disconnected to the VSL AP group, the VSU topology will change. If the original VSU topology is a ring topology, the ring will convert into a line. For details, see topology ring and line conversion in the section of *Topology Changes*.

❖ **Detecting Error Frames on a VSL Interface**

When a large number of consecutive error frames are detected on a VSL interface, the interface must be disabled and switched to another VSL interface. The detection method is as follows:

If error frames are found on a VSL interface, perform error frame correction. The system detects the VSL interface every 5 seconds by default. If the number of error frames is greater than the value of *num* as compared with that detected last time, it is assumed that error frames are detected once. If error frames are detected consecutively for the value of *times*, it is assumed that the interface is abnormal. If multiple VSL links are available when error frames are detected, the VSL will be switched. The last VSL will not be switched in order to prevent

topology splitting.

Different user scenarios have different requirements for *num* and *times*. The default value of *num* is *3* and that of *times* is *10*. If users have strict requirements on the scenarios, select smaller values for *num* and *times*; if reverse, select greater values.

7.3.2   Topology

The VSU system supports line topology and ring topology. Devices are connected through a VSL to form a line that is called the line topology.

Working Principle

❖ **Topology**

The line topology is simple. It uses a very few ports and cables. Two devices are connected with a communication link only. Therefore, the VSL has low reliability.

Figure 7-8 Line topology

Expect for the line topology, devices can also form a ring topology, as shown in Figure 7-9. In the ring topology, the two communication links between devices can back up for each other and perform link redundancy to improve the reliability of the VSU system.

Figure 7-9 Ring Topology

You are advised to select the ring topology for the VSU system, thus the normal operation of the whole VSU system will not be affected by any single faulty device or VSL.

Besides selecting the ring topology networking, you are advised to configure multiple VSLs for every VSL member to improve the reliability of a single VSL. At least two links are recommended and a maximum of four links can be configured. A reasonable configuration comprises more than two VSLs crossing different cards.

❖ **Topology Convergence**

Before the establishment of the VSU, the member devices need to discover

neighbors through topology discovery protocols and check devices in the VSU system to confirm the range of the management domain. Then a global master device is selected to manage the whole VSU system and a global slave device is selected for backup of the master device. Then the whole VSU topology is converged. As the start up time differs for different devices, the first convergence time of the topology is also different.

❖ **Topology ring and Line Conversion**

In a ring topology, if a VSL link is disconnected, the ring topology will convert into a line topology. The whole VSU system will still run normally without network disconnection. To prevent other VSL links and nodes from being faulty, you are advised to locate the VSL failures and recover the availability of the VSL. After the VSL link is recovered, the line topology will convert into the ring topology.

Figure 7-10 Ring-to-line and line-to-ring

❖ **Topology Splitting**

In the line topology, if the VSL link is disconnected, the line topology will be split, as shown in Figure 7-11. A VSU group is split into two groups. In this condition, two devices with the absolutely same configurations may exist on the network, which will cause abnormal operation of the network. Therefore, the multi-active detection (MAD) function (for details, see 1.1.4.6 Multi-Active Detection) needs to be deployed to solve the problem of topology splitting.

Figure 7-11 Topology splitting

❖ **Topology Combining**

If the two VSU groups are connected through the VSL link, the line topology will be combined. During the topology combining, restart one VSU group and then hot add the other VSU group.

The principle of topology combining: Minimizing influences on the services during topology combining. The rules are as follows (Judge from the first item. If you cannot select the optimal topology, continue to judge the next item):

▪ Use the device priority as the first criteria for judging topology combining. Reserve the VSU group containing a device with the highest priority.

▪ If the previous item cannot help make a judgment, select the VSU group with a smaller switch ID (that of the two global master switches).

▪ If the previous item cannot help make a judgment, reserve the VSU group with a smaller MAC address (that of the global master switches).

Figure 7-12 Topology combining

During topology combining of two VSU groups, the two VSU groups need to be elected. The VSU group that fails the election will restart automatically and hot add to the other VSU group.

7.3.3 Dual-Active Detection (DAD)
Working Principle

When the VSL is disconnected, the slave device switches to the master device. If the original master device is still running, a series of problems including IP address conflict on the LAN will be caused due to there are two master devices and their configurations are the same completely. In this condition, the VSU system must detect the two devices and take recovery measures. The VSU system provides two methods to perform MAD as follows:

▪ Bidirectional forwarding detection (BFD)

▪ AP-based detection

❖ **MAD Rules**

1. Select the VSU group with the highest priority.

2. If the previous item cannot help make a judgment, select the VSU group with more physical devices.

3. If the previous item cannot help make a judgment, select the VSU group with a higher health. (Health: total bandwidth of all physical interfaces (except for management and VSL interfaces) in the UP state in the topology.)

4. If the previous item cannot help make a judgment, select the VSU group with a smaller switch ID (that of the two global master switches).

5. If the previous item cannot help make a judgment, reserve the VSU group with a smaller MAC address (that of the two global master switches).

6. If the previous item cannot help make a judgment, reserve the VSU group with a greater startup time (that of the global master switches).

If DAD is not configured, network interruption may be caused after topology splitting.

❖ BFD

The VSU system supports the BFD to detect multiple master devices. Figure 7-13 shows the topology. A link is added for the two devices on the edges for MAD specially. When the VSL link is disconnected between the global master and slave devices, two master devices exist concurrently. If the BFD function is set, the two master devices will send the BFD packets to each other through the BFD link. Thereby the same devices are detected on the current system. Finally shut down the VSU system of a master device according to some rules (for details, see the topology combining rules in the section 1.1.4.4 *Topology Changes*) and enter the recovery state to avoid network abnormality.

Figure 7-13 BFD

When there is a pair of BFD links, you are advised to deploy the detection links at the two ends of the topology.

You need to adopt the extension BFD and you cannot configure the dual-active detection port by using the existing BFD configurations and commands.

❖ MAD

The VSU system also supports the MAD dual-active detection mechanism. Figure 7-14 shows the topology. The VSU system and the upstream device both need to support the MAD function. When the VSL link is disconnected, two master devices exist concurrently. The two master devices respectively send the MAD packets to

the member ports of the MAD-APs and then the MAD packets are forwarded to each other through the upstream device. As shown in Figure 7-14, the MAD-AP has four member ports. Each member port is connected to a different device of the VSU system. When the topology splitting occurs, the four member ports all send and receive the MAD packets. Thereby the same devices are detected on the current system. Finally shut down the VSU system of a master device according to some rules (for details, see the topology combining rules in the section of *Topology Changes* and enter the recovery state to avoid network abnormality.

Figure 7-14 MAD based on upstream and downstream devices

In the topology above, the upstream device must be QTECH device and support the MAD packet forwarding function.

7.3.4   VSU Traffic Forwarding
Working Principle

❖   **Cross-device AP Group**

An AP binds multiple physical links together to form a logical link. The VSU system supports the AP across the member devices.

As shown in Figure 7-15, two devices form a VSU group. The external access device Switch A is connected to the VSU in the form of the AP. In terms of Switch A, there is no difference between the AP in Figure 7-15 and the common AP group.

Figure 7-15 Cross-device aggregation port

❖   **Troubleshooting**

You are advised to configure the cross-device AP with the physical link between the peripheral device and each VSU device. On the one hand, the VSL bandwidth

can be reserved (prioritize the AP member of the same chassis as the egress to transmitted the cross-chassis AP traffic and prevent unnecessary traffic from being transmitted through the VSL link). On the other hand, the network reliability can be improved (if a certain chassis is faulty, the member ports of normal devices can work normally).

The follows sections describe the possible faults of the cross-device AP and the consequences.

- Single link failure

If a single link of the cross-device AP is faulty but other links still work normally, the cross-device AP will reallocate the traffic for the remaining normal links.

- Link failure of all cross-device AP member ports on the global master device

If the links of all cross-device AP member ports on the global master device fail to work, only the member ports of other member devices continue working normally. In terms of the data stream transmitted through the AP to the VSU system, if the data stream forwarding egress is on the global master device, the system will forward the data stream to the corresponding egress on the global master device through the VSL link.

The control plane protocols are still running on the global master device. Therefore, the protocol packets that enter the VSU system need to be forwarded to the global master device through the VSL link for protocol computing.

- Failure of all links of other member devices

If all links of the cross-device AP and a single device A fail to work, only the member ports of other member devices continue working normally. In terms of the data stream transmitted through the AP to the VSU system, if the data stream forwarding egress is on the member device A, the system will forward the data stream to the corresponding egress on the member device A through the VSL.

- Failure of all links

If all links of the cross-device AP fail to work, the interface status will be Link-Down.

- Global master device fault

If the global master device is faulty, the hot backup switching is performed to switch the original slave device to the master device. Meanwhile, the member ports on other member devices continue working. The link failure is detected on the peer device connected to the VSU through this AP. Therefore, the traffic balancing algorithm needs to be adjusted to allocate the data stream to normal links.

- Member device fault

If a member device is faulty, the AP member link connected to this member device is disconnected. However, other member links still work normally. The link failure is detected on the peer device connected to the VSU through this AP. Therefore, the traffic balancing algorithm needs to be adjusted to allocate the data stream forwarding paths to normal links.

❖ **Traffic Balancing**

In a VSU system, traffic may have multiple egresses. The AP and ECMP have their own traffic balancing algorithms, for example, using destination or source MAC addresses. For details, see the *Configuring Aggregate Port*. The local forwarding first (LFF) can be configured detailed in this configuration manual. Packets received by a device are forwarded on this device first. In this way, packets can be forwarded to other devices without using a VSL.

7.3.5   System Management
Working Principle

❖ **Access to the Console**

The master device console of VSU system manages multiple devices on the system simultaneously. The consoles of the slave and candidate devices do not support command line input. However, you can configure the VSU system on the master device for a specified member device and log in to the master device console through the serial port of the slave device. A session can be used to redirect to the master console of a device.

❖ **Slot Naming**

In terms of the chassis device, in the VSU mode, the slot is named with the device number (Switch ID). Therefore, the slot number turns from one-dimensional into two-dimensional. For example, cable clip 1/1 indicates the slot numbered 1 of the slot 1 on a member device.

❖ **Interface Naming**

In the VSU working mode, a slot number may occur in multiple devices. Therefore, the interface is named with the device number (Switch ID).

For example, interface gigabitEthernet 1/0/1 indicates the Gigabit port 1 on the slot 0 of the device whose ID is 1; interface gigabitEthernet 2/0/2 indicates the Gigabit port 2 on the slot 0 of the device whose ID is 2.

❖ **Access to the File System**

In the VSU working mode, you can access to the file system on other member devices from the master device. The detailed access method is the same to that of the local file system. The unique difference is that different URL prefixes are used.

❖ **System Upgrade**

Generally the VSU system requires version consistency of the main program version numbers of the member devices. However, there are so many member devices that it takes too much time and energy to perform upgrade one by one in the standalone mode and it is also easy to make mistakes. QTECH switches provide consummate system upgrade solution to help you with system upgrade by adopting the two methods as follows:

- When the VSU system is being established: the system will automatically align the main program version numbers of all member devices. Once the main program versions are discovered inconsistency, the main program of the master device will be selected to be synchronized to all member devices.
- After the VSU system is established: the main program version will be synchronized to all member devices automatically by using the file that is downloaded by the TFTP.

❖ SYSLOG

All member devices of the VSU system can display the SYSLOG. The SYSLOG generated by the master device is displayed on the master device console with the same format to that in the standalone mode. The SYSLOG generated by other member devices is also displayed on the master device console, but the message format is different from that in the standalone mode because the device number information is added.

For example, the SYSLOG information generated in the standalone state is "%VSU-5-DTM_TOPO_CVG:Node discovery done. Topology converged." The SYSLOG information generated by the member device numbered 3 is "%VSU-5-DTM_TOPO_CVG:(3) Node discovery done. Topology converged."

7.3.6 Quick Blinking Location

In a network cabling environment, the equipment room where switches are located and the operation console are often at different places. If there are many devices in the environment, network administrators cannot easily locate the locations of specific devices.

Quick blinking location provides network administrators with a method for locating devices by means of quick blinking. By enable this function for a device on the console, you can easily find the corresponding device in the equipment room.

When quick blinking location is enabled, the status LED cannot show original status until the quick blinking location is disabled.

7.4 Configuration

Configuration	Configuration and Command	
Configuring VSU in the Standalone Mode	(Mandatory) It is used to configure VSU in the standalone mode.	
	switch virtual domain	Configures the domain ID.
	switch	Configures the switch ID.
	switch priority	Configures the switch priority.

		vsl-port	Enters the VSL interface configuration mode.
Configuration		**Configuration and Command**	
		port-member interface	Configures the VSL member interface.
		switch convert mode virtual	Changes the standalone mode to the VSU mode.
		(Optional) It is used to configure the device attributes in the VSU mode.	
		switch description	Configures the device description.
		switch crc	Configures error frame check.
Configuring VSU in the VSU Mode	Configuring VSU Attributes	(Optional) It is used to configure the device attributes in the VSU mode.	
		switch domain	Changes the domain ID.
		switch renumber	Changes the switch ID.
		switch description	Configures the device description.
		switch crc	Configures error frame check.
	Configuring the VSL	(Optional) It is used to configure a VSL.	
		vsl-port	Enters the VSL interface configuration mode.
		port-member interface	Configures a VSL member interface.
	Configuring Dual-Active Detection	(Mandatory) It is used to configure DAD.	
		dual-active detection	Configures DAD.
		dual-active bfd interface	Configures the BFD DAD interface.

		dual-active interface	Configures an AP as a DAD interface.
		dual-active exclude interface	Configures an excluded interface.
	Configuring Traffic Balancing	(Optional) It is used to configure traffic balancing in the VSU mode.	
		switch virtual aggregateport-lff enable	Configures the AP LFF mode.
		switch virtual ecmp-lff enable	Configures the ECMP LFF mode.
	Changing the VSU Mode to the Standalone Mode	(Optional) It is used to change the VSU mode to the standalone mode.	
		switch convert mode standalone	Changes the VSU mode to the standalone mode.
		(Optional) It is used to quickly locate a device.	
		led-blink	Enables quick blinking location.

7.4.1 Configuring VSU in the Standalone Mode
Configuration Effect

Start up the switch in the standalone mode to set relevant VSU parameters to establish the VSU system.

Configuration Steps

❖ **Configuring VSU Attributes**

- A switch starts in the standalone mode by default. You need to set the same domain ID on the two chassis of the established VSU system. The domain ID must be unique within the local area network (LAN). Furthermore, you need to set the ID of each chassis in the VSU.

- Run the **switch virtual domain** *domain_id* command to configure the domain ID. This command is mandatory.

- Run the **switch** *switch_id* command to configure the device ID in the VSU. This command is mandatory. For devices with the same priorities in the VSU system, a device with the smallest device ID is selected as the global master

device.

- Run the **switch** *switch_id* **priority** *priority_num* command to configure the device priority. This command is mandatory.

- The value ranges from 1 to 255. A larger value means a higher priority.

- Run the **switch** *switch_id* **description** *switch1* command to configure the device alias. This command is optional. The default name is QTECH. For easy identification of devices in the network environment, this item can be selected to set the device alias.

- A maximum of 32 characters are allowed.

Command	switch virtual domain *number*
Parameter Description	*number:* Indicates domain ID of the VSU
Defaults	The default domain ID is 100.
Command Mode	config-vs-domain configuration mode
Usage Guide	Only two devices with the same domain ID can form a VSU. The domain ID must be unique within the LAN.
Command	**switch** *switch_id*
Parameter Description	*switch_id:* indicates the switch ID in the VSU system. The value varies with products.
Defaults	The default device ID is 1.
Command Mode	Domain configuration mode
Usage Guide	The device ID identifies each virtual device member. In VSU mode, the interface name format changes to "switch/slot/port" from "slot/port", in which "switch" is the device ID. If either chassis are active or if the role of the just started chassis is uncertain and both have the same priority, the chassis with a smaller ID is elected as the active one. This command can be only used to modify the device ID in standalone mode. In VSU mode, run the **switch renumber** command to modify the device ID. The modified device ID takes effect only after you restart the device, regardless of in standalone mode or in VSU mode.
Command	**switch** *switch_id* **priority** *priority_num*

Parameter Description	switch_id: Indicates a switch ID for which a priority needs to be configured. priority_num: Indicates the switch priority, ranging from 1 to 255.
Defaults	The default device priority is 100.
Command Mode	Domain configuration mode
Usage Guide	A larger value means a higher priority. A device with the highest priority is chosen as the master device. You can run this command in the standalone or VSU mode. The modified priority takes effect only after you restart the device. This command is not used to modify the value of switch_id. In the standalone mode, if switch_id is set to 1, running the **switch** 2 **priority** 200 command does not work. You can first set switch_id to **2** and then run the **switch** 2 **priority** 200 command. In the VSU mode, switch_id indicates the ID of the currently running switch. If the ID does not exist, the configuration does not take effect.
Command	**switch** switch_id **description** dev-name
Parameter Description	switch_id: Indicates the device ID. dev-name: Indicates the device description, no greater than 32 characters.
Defaults	N/A
Command Mode	Domain configuration mode
Usage Guide	This command is configured on a device in whether standalone or VSU mode and takes effect immediately after configuration.

The command used for configuring a priority can modify the priority only rather than modify a switch ID. Therefore, you must enter the current switch ID correctly for the configuration. For example, you have set the switch ID to 1. If you enter **switch** 2 **priority** 100, the priority configuration cannot take effect.

❖ **Configuring the VSL**

▪ To establish the VSU system, you need to decide which ports are configured as the VSL member ports.

▪ Run the **vsl-port** command to enter the VSL interface configuration mode. This command is mandatory.

- ▪ Run the **port-member interface** *interface-name* command to add a VSL interface. This command is mandatory.

- ▪ When the device enters the VSL interface configuration mode, the VSL interface can be configured or deleted.

Command	vsl-port
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	You can run this command in the standalone or VSU mode.

Command	port-member interface ***interface-name***
Parameter Description	*interface-name*: Indicates a two-dimensional interface name, such as Tengigabitethernet 1/1 and Tengigabitethernet 1/3.
Defaults	N/A
Command Mode	VSL interface configuration mode
Usage Guide	Add a member interface of the VSL link. *interface-name* indicates the two-dimensional interface name in the standalone mode. The two-dimensional interface can be the 10 Gigabit interface or Gigabit interface. (The Gigabit interface can be an opto-copper interface. If the media type is not specified, the Gigabit copper interface is adopted by default.) For an opto-copper interface, you must specify its optical or copper interface attribute. A VSL interface for a chassis device must be a 10 Gigabit interface. You can run this command in the VSU mode or standalone mode. The command can take effect after the command configuration is saved and the device where the VSL member interface resides is restarted.

In the standalone mode, the VSL configurations cannot take effect immediately unless the device shifts into the VSU mode and restart.

- ❖ **Configuring Error Frame Check**

- Run the **switch crc** command to configure error frame check. This command is optional. Run this command to modify the default method for checking error frames.

- If error frames are found on a VSL interface, perform error frame correction. The system detects the VSL interfaces every 5 seconds by default. If the number of error frames is greater than 3 as compared with that detected last time, it is assumed that error frames are detected once. If error frames are detected consecutively for 10 times, it is assumed that the interface is abnormal. If multiple VSL links are available when error frames are detected, the VSL will be switched.
The last VSL will not be switched in order to prevent topology splitting.

Command	switch crc errors *error_num* times *time_num*
Parameter Description	*error_num:* Configures the increase of error frames between two detections. When the number of error frames is greater than the increase, it is assumed that error frames are detected once. *time_num:* Configures the number of times after which an action needs to be taken (the action can be displaying a prompt or disabling the interface).
Defaults	The default value of **errors** is 3; the default value of **times** is 10.
Command Mode	Domain configuration mode
Usage Guide	The system detects the VSL interfaces every 5 seconds by default. If the number of error frames is greater than 3 as compared with that detected last time, it is assumed that error frames are detected once. If error frames are detected consecutively for 10 times, it is assumed that the interface is abnormal. The default
	action for an abnormal interface is displaying a log prompt. You can set the action to disabling the interface. If the interface is disabled, you must recover it by unplugging and plugging it.

Different products have different requirements for error frame check and different processing for VSL interfaces. In version 11.0, error frame check is configurable.

❖ **Changing the Standalone Mode to the VSU Mode**

- Use the **switch convert mode virtual** command to change the standalone mode to the VSU Mode.

- In the standalone mode, the software will take the following actions after you run the **switch convert mode virtual** command.

Back up the global configuration file *config.text* in the standalone mode as *standalone.text* for subsequent use. Clear the contents of the configuration file *config.text*.

Write the relevant VSU configurations to the special configuration file *config_vsu.dat*.

- If there is a *virtual_switch.text* file on the switch, the system will prompt you whether to overwrite the contents of the file *virtual_switch.text* to the file *config.text* (the file *virtual_switch.text* is a backup file for the file *config.text* when the switch shifts from the VSU mode to the standalone mode). Then you can click **Yes** or **No**. Finally the switch restarts in the VSU mode and reads VSU parameters in the file *config_vsu.dat*.

Command	switch convert mode virtual
Parameter Description	N/A
Defaults	The switch is in the standalone mode by default.
Command Mode	Privileged EXEC mode
Usage Guide	Change the standalone mode to the VSU mode.

Verification

Run the **show switch virtual config** [*switch_id*] command to check the VSU configuration of the current switch in the standalone mode.

Command	show switch virtual config **[*switch_id*]**
Parameter Description	*switch_id*: Indicates the switch ID. After this parameter is specified, only the VSU configuration of the specified device is displayed.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display the VSU configuration in the standalone or VSU mode.

The relevant VSU configurations are set for a single physical switch and the configurations are stored in the special configuration file config_vsu.dat. Therefore, you can view the current VSU configurations by running the **show switch virtual config** command rather than the **show running config** command.

In the standalone mode, the VSU running information is null. When you enter

QTECH
МИР ДОСТУПНЕЕ   www.qtech.ru

commands such as show switch virtual, the system will prompt you that the switch is in the standalone mode and there is no VSU running information.

Configuration Example

❖ **Configuring VSU in the Standalone Mode**

Scenario Figure 7-16	 **Switch 1 and Switch 2 form a VSU system. The domain ID is 100. The chassis on the left side is configured as Chassis 1, with the priority of 200, alias of Switch 1, and the VSL interfaces of 1/1 and 1/2. The chassis on the right side is configured as Chassis 2, with the priority of 100, alias of Switch 2, and the VSL interfaces of 1/1 and 1/2.**
Configuration Steps	▪ Perform the following configuration on the Switch 1: ▪ Configure VSU attributes and VSL interfaces. ▪ Change the standalone mode to the VSU mode. ▪ Perform the following configuration on the Switch 2: ▪ Configure VSU attributes and VSL interfaces. ▪ Change the standalone mode to the VSU mode.
| **Switch-1** | ```
QTECH# configure
terminal
QTECH(config)#
switch virtual
domain 100
QTECH(config-vs-
domain)#switch 1

QTECH(config-vs-domain)#switch  1  priority  200  QTECH(config-vs-
domain)#witch  1  description  switch-1  QTECH(config-vs-domain)#
switch crc errors 10 times 20 QTECH(config-vs-domain))#exit

QTECH(config)#vsl-port

QTECH(config-vsl-port)#port-member  interface  Tengigabitethernet
1/1          QTECH(config-vsl-port)#port-member          interface
Tengigabitethernet 1/2 QTECH(config)#exit

QTECH#switch convert mode virtual
``` |
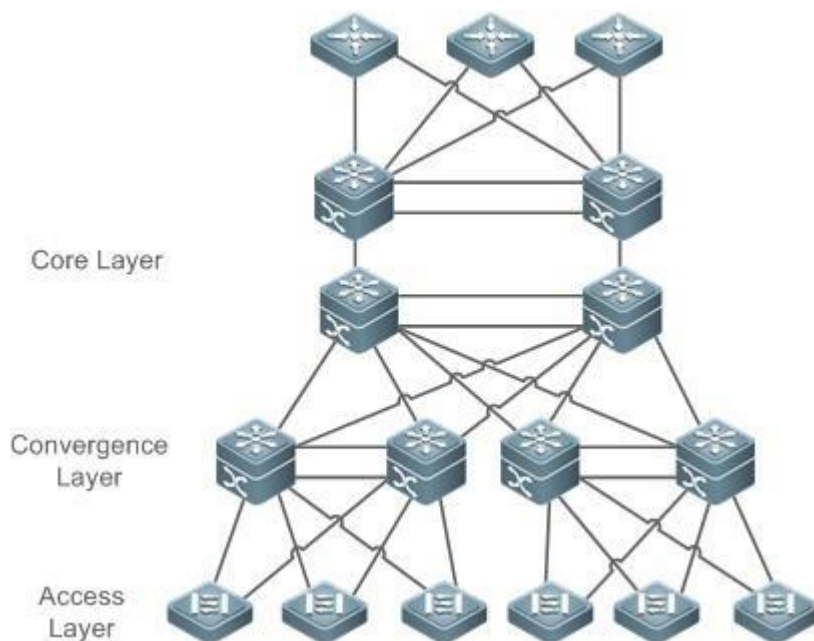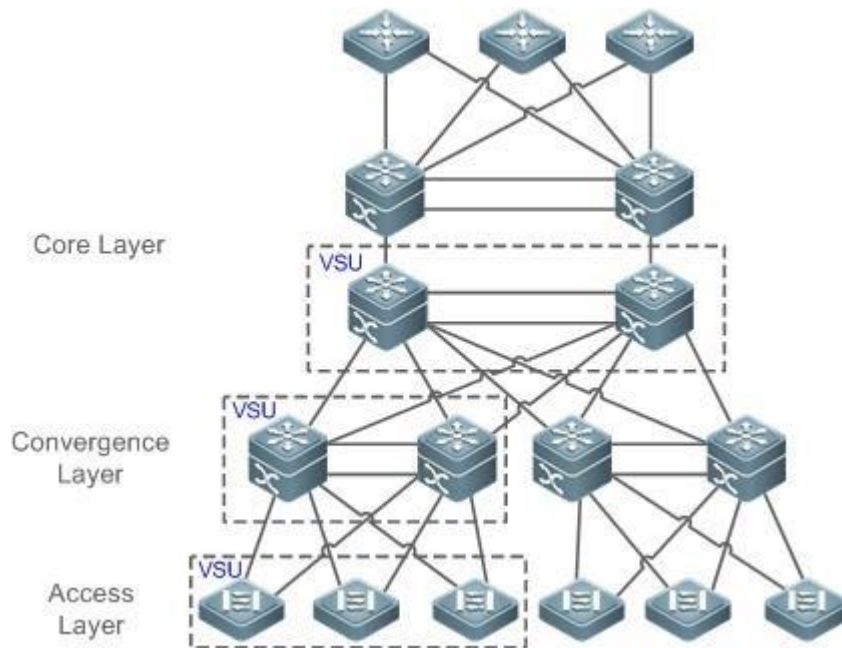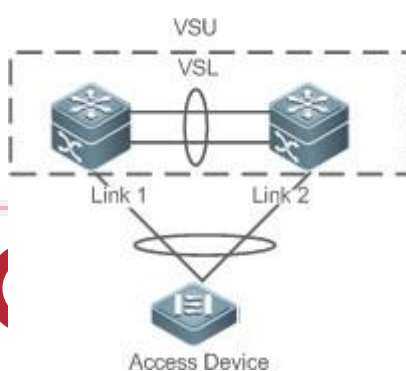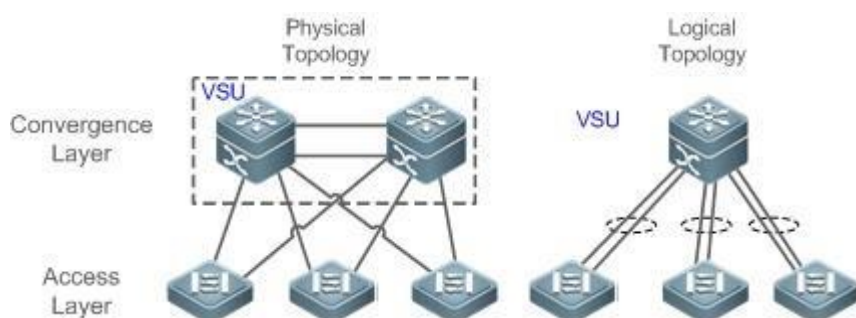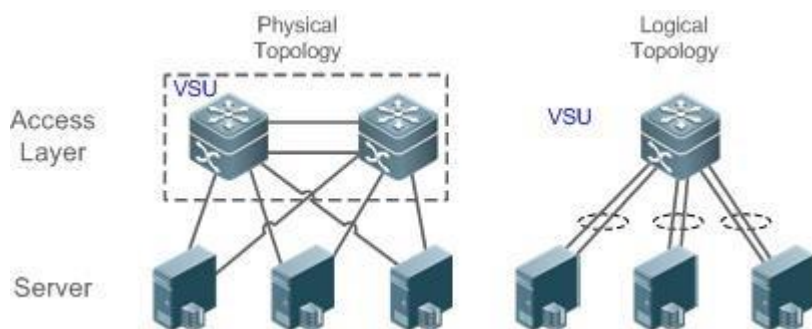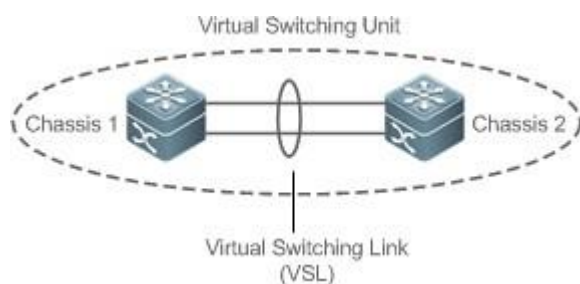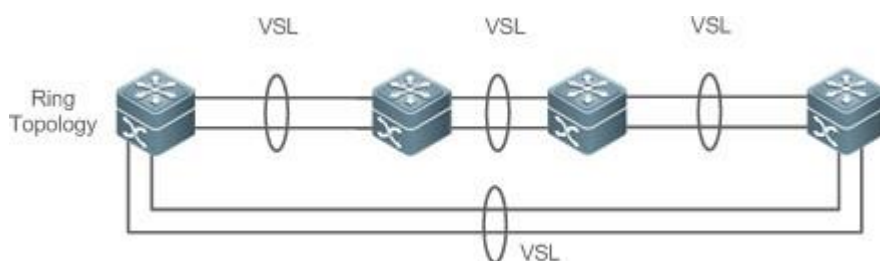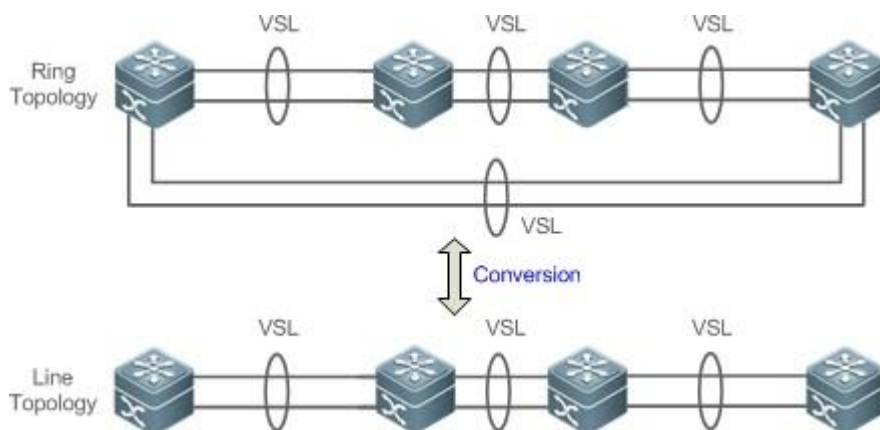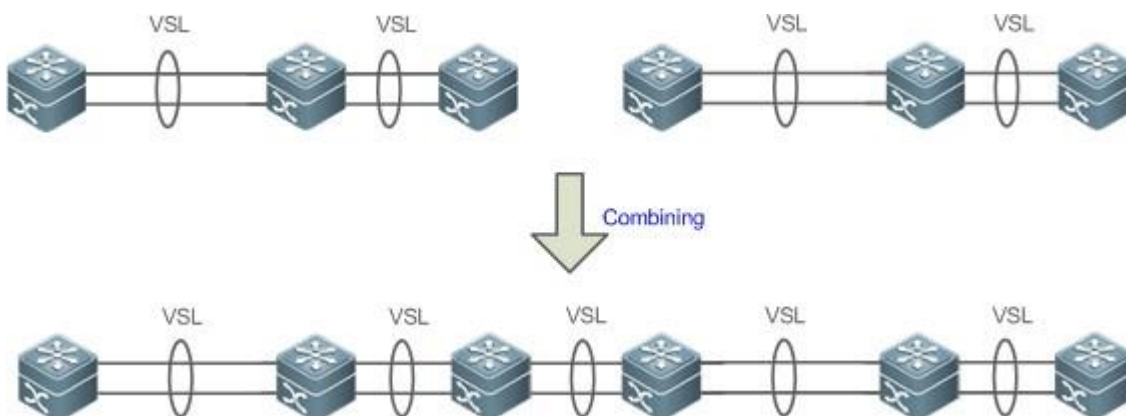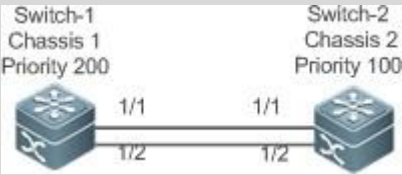| **Switch-2** | |

| | ```
QTECH(config-vs-domain)# switch 2

QTECH(config-vs-domain)# switch 2 priority 200 QTECH(config-vs-
domain)# switch 2 description switch-2 QTECH(config-vs-domain)#
switch crc errors 10 times 20 QTECH(config-vs-domain))#exit
QTECH(config)#vsl-port

QTECH(config-vsl-port)#port-member interface Tengigabitethernet
1/1        QTECH(config-vsl-port)#port-member        interface
Tengigabitethernet 1/2 QTECH(config-vsl-port)#exit
QTECH#switch convert mode virtual
``` |
| **Verification** | Run the **show switch virtual config** command to view the VSU attributes of Switch 1 and Switch 2. |
| **Switch-1** | ```
QTECH#show   switch   virtual   config   switch_id:   1   (mac:
0x1201aeda0M)
!
switch virtual domain 100
!
switch 1
switch 1 priority 100
!
switch convert mode virtual
!
port-member interface Tengigabitethernet 1/1
!
port-member interface Tengigabitethernet 1/2
!
switch crc errors 10 times 20
!
``` |
| **Switch-2** | ```
QTECH#show switch virtual config
switch_id: 2 (mac: 0x1201aeda0E)
``` |
| | ```
!
switch virtual domain 100
!
switch 2
switch 2 priority 100
!
switch convert mode virtual
!
port-member interface Tengigabitethernet 1/1
!
port-member interface Tengigabitethernet 1/2
!
switch crc errors 10 times 20
!
``` |

Common Errors

A VSL interface of a chassis device must be 10 Gigabit or higher.

7.4.2   Configuring VSU in the VSU Mode

Configuring VSU Attributes

Configuration Effect

During the VSU system running, you can modify the parameters, such as domain ID, switch ID, and priority of the master device or the slave device. However, you can only log in to the VSU master device console to modify these parameters, but cannot enter the global configuration mode from the slave device console.

Notes

- Among the commands above, the all configuration commands take effect only after the switch restarts except the

    switch *sw_id* **description** *swi*tch1 command that can take effect immediately.

Configuration Steps

❖ **Entering the Domain Configuration Mode**

- Optional.

- Run this command in the VSU mode to enter the domain configuration mode. Switches with the same domain ID form a VSU system. You can modify or configure the domain ID, switch priority, and switch ID only after entering the domain configuration mode in the VSU mode.

Command	switch virtual domain *domain_id*
Parameter Description	*domain_id*: Indicates the virtual domain ID of the VSU system.
Defaults	The default domain ID is 100.
Command Mode	config-vs-domain configuration mode
Usage Guide	Only two devices with the same domain ID can form a VSU system. The domain ID must be unique on a LAN.

❖ **Changing the Domain ID**

- ▪ Optional.

- ▪ To modify the value of *domain_id* for a device, you can configure this item
  on the master device console of the VSU system.

Command	switch *switch_id* domain *new_domain_id*
Parameter Description	*switch_id*: Indicates the ID of the currently running switch in the VSU mode, ranging from 1 to 8. *new_domain_id*: Indicates the modified domain ID, ranging from 1 to 255.
Defaults	The default domain ID is 100.
Command Mode	Domain configuration mode
Usage Guide	Run this command only in the VSU mode. In addition, the setting can take effect only after the device is restarted.

- ❖ **Changing the Switch ID**

- ▪ Optional.

- ▪ To modify the value of *switch_id* for a device, you can configure this item
  on the master device console of the VSU system.

Command	switch *switch_id* renumber *new_switch_id*
Parameter Description	*switch_id*: Indicates the ID of a switch. In a VSU system, the switch ID ranges from 1 to 16 for cassette switches, and from 1 to 4 for chassis switches. *new_switch_id*: Indicates the modified switch ID.
Defaults	N/A
Command Mode	Domain configuration mode
Usage Guide	Run this command only in the VSU mode. In addition, the setting can take effect only after the device is restarted.

- ❖ **Changing the Switch Priority**

- ▪ Optional.

- ▪ To modify the priority of a device, you can configure this item on the master device

console of the VSU system.

- A larger value means a higher priority. Select the device with the highest priority as the master device.

Command	switch *switch_id* priority *priority_num*
Parameter Description	*switch_id:* Indicates a switch ID for which a priority needs to be configured. *priority_num:* Indicates the switch priority, ranging from 1 to -255 for cassette switches.
Defaults	The default priority is 100.
Command Mode	Domain configuration mode
Usage Guide	A larger value means a higher priority. Select the device with the highest priority as the master device. You can run this command in the standalone or VSU mode. The modified priority takes effect only after you restart the device. This command is not used to modify the value of **switch_id**. In the standalone mode, if **switch_id** is set to **1**, running the **switch 2 priority 200** command does not work. You can first set **switch_id** to **2** and then run the **switch 2 priority 200** command. In the VSU mode, **switch_id** indicates the ID of the currently running switch. If the ID does not exist, the configuration does not take effect.

❖ **Configuring the Device Description**

- Optional.

- To configure the description for a device, you can configure this item on the master device console of the VSU system.

- Run the **switch** *switch_id* **description** *switch1* command to configure the device description. A maximum of 32 characters are allowed.

Command	switch *switch_id* description *dev-name*
Parameter Description	*switch_id:* Indicates a switch ID for which a priority needs to be configured. *dev_name*: Indicates the device name.
Defaults	N/A
Command Mode	Domain configuration mode

| Usage Guide | You can run this command in the standalone or VSU mode. The configuration takes effect immediately in
the VSU mode. |

❖ **Configuring Error Frame Check**

▪ Optional.

▪ Run the **switch crc errors** *error_num* **times** *time_num* command to configure the conditions for triggering error frame check.

Command	switch crc errors *error_num* times *time_num*
Parameter Description	*error_num:* Configures the increase of error frames between two detections. When the number of error frames is greater than the increase, it is assumed that error frames are detected once.
	time_num: Configures the number of times after which an action needs to be taken (the action can be displaying a prompt or disabling the interface).
Defaults	The default value of **errors** is **3**; the default value of **times** is **10**.
Command Mode	Domain configuration mode
Default Level	14
Usage Guide	N/A

❖ **Saving the Configuration File**

Run the **exit** command to exit from the virtual device configuration mode and run the **write** command to save the configurations to the *config_vsu.dat* file.

Verification

Use the **show switch virtual** [**topology | config**] command to display the current VSU running information, topology or configuration parameters.

Command	show switch virtual **[** topology	config **]**
Parameter Description	**Topology**: Indicates topology information. **Config**: Indicates the VSU configurations.
Command Mode	Privileged EXEC mode

Usage Guide	View the domain ID, and the device ID, status and role of each device.

Configuration Example

❖ Configuring VSU Attributes

Scenario Figure 7-17	**Switch 1 and Switch 2 form a VSU system. Modify the chassis ID of Switch 2 to 3 and its priority to 150. Assume that Switch 1 is the global master switch and perform the configuration on the global master switch.**
Configuration Steps	Modify the configurations of Switch 2.
| **Switch-1** | ```
QTECH#config
 QTECH(config)# switch virtual
 domain 100 QTECH(config-vs-
 domain)# switch 2 renumber  3
QTECH(config-vs-domain)# switch 2 priority 150
QTECH(config-vs-domain)# switch 2 description switch-3
``` |
| **Verification** | Run the **show switch virtual config** command for verification. |

Switch-1	``` QTECH#show switch virtual config switch_id: 1 (mac: 0x1201aeda0M) ! switch virtual domain 100 ! switch 1 switch 1 priority 100 ! switch convert mode virtual ! port-member interface Tengigabitethernet 1/1 ! port-member interface Tengigabitethernet 1/2 ! switch_id: 3 (mac: 0x1201aeda0E) ! switch virtual domain 100 ! switch 3 switch 3 priority 150 ! switch convert mode virtual ! port-member interface Tengigabitethernet 1/1 ! port-member interface Tengigabitethernet 1/2 ! switch 3 description switch-3 ! ```

7.4.2.1 Configuring the VSL

Configuration Effect

When switches form a VSU system or when the VSU system is running, you can shift between common interfaces and VSL interfaces. However, you can only log in to the master device console of the VSU system for modification, but cannot enter the global configuration mode from the slave device console.

Notes

- You can log in to the console of the VSU system by using a serial port or telnet, in order to add or delete the configurations of VSL member interfaces.

- To prevent incorrect connections in actual scenarios, the VSL AP uses dynamic negotiation. You need to configure the VSL interface pool first, and

then add the VSL interface pool to the same AP after successful negotiation. Interfaces connecting to the same device are within the same AP.

Configuration Steps

- ❖ **Entering the VSL Interface Configuration mode**

  - ▪ Run the **vsl-port** command to enter the VSL-PORT configuration mode. This command is optional.

  - ▪ When the device enters the VSL-PORT configuration mode, the VSL interface can be configured or deleted.

Command	vsl-port
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	You can run this command in the standalone or VSU mode.

- ❖ **Configuring a VSL Member Interface**

  - ▪ Run the **port-member interface** *interface-name* command to add a VSL interface. This command is optional.

  - ▪ Run the **port-member interface** command to configure a VSL member interface.

Command	port-member interface *interface-name*
Parameter Description	*interface-name*: Indicates a two-dimensional interface name, such as GigabitEthernet 0/1 and GigabitEthernet 0/3.
Defaults	N/A
Command Mode	VSL interface configuration mode
Usage Guide	You can run this command in the VSU mode or standalone mode. The command can take effect after the command configuration is saved and the device where the VSL member interface resides is restarted.

During the VSU system running, the configured VSL member links take effect immediately. VSL interfaces need to be configured for all devices.

For chassis devices, VSL interfaces must be optical interfaces of 10 Gigabit or higher; for cassette devices, VSL interfaces can be optical and copper interfaces of Gigabit or higher.

Modules on chassis devices must be modules of 10 Gigabit or higher. 40G one-to-four interfaces cannot be configured as VSL interfaces.

For a 40G port (no matter whether splitting is performed for the interface), its member interfaces (namely, four 10G interfaces) cannot be shifted to VSL member interfaces.

If an interface has been configured as an NLB reflex interface, this interface can be shifted to a VSL member interface only after the NLB reflex interface configuration is deleted.

To prevent a loop that may occur when a VSL member interface exits from the VSL AP, the system automatically sets the member interface to the shutdown state when the command is executed to make the VSL member interface exit

from the VSL AP. After the VSL member interface exits from the VSL AP, you can reconnect the link and run the **no shutdown** command to enable this interface again. When you configure a VSL interface, the system will shut it down first. If the configuration fails and you want to use it as a common interface, you can run the **no shutdown** command to enable this interface again. Add a member interface number that must be a three-dimensional interface number. For example, in the VSL-PORT configuration mode, if you run the **port-member interface** Tengigabitethernet 1/1/1 command, it indicates that you configure the global three-dimensional interface 1/1/1 as a VSL interface.

If VSU topology splitting occurs when you change a VSL interface to a common interface, the VSL interface cannot be deleted. You can disconnect the physical interface first and then delete the VSL interface.

Verification

- Use the show switch virtual link [port] to display the current VSL link running information in the VSU mode.

Command	show switch virtual link **[port]**
Parameter Description	**port**: Displays the status information of the VSL member interfaces.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

❖ **Configuring the VSL**

Scenario Figure 7-18	
Configuration Steps	Add interface 1/1/3 as the VSL interface for Switch 1 and delete interface 1/1/2 from the VSL interface.
| **Switch-1** | ```
QTECH#config QTECH(config)# vsl-port
QTECH(config-vsl-port)# port-member interface Tengigabitethernet 1/1/3

QTECH(config-vsl-port)#  no  port-member  interface  Tengigabitethernet 1/1/2
``` |
| **Verification** | Run the **show switch virtual config** command to view the VSL. Assume that Switch 1 is the global master switch and run the command on the global master switch. |

| Switch-1 | ```
QTECH#show switch virtual config
switch_id: 1 (mac: 0x1201aeda0M)
!
switch virtual domain 100
!
switch 1
switch 1 priority 100
!
switch convert mode virtual
!
port-member interface Tengigabitethernet 1/1
!
port-member interface Tengigabitethernet 1/3
!
switch_id: 3 (mac: 0x1201aeda0E)
!
switch virtual domain 100
!
switch 3
switch 3 priority 150
!
switch convert mode virtual
!
 port-member interface Tengigabitethernet 1/1
!
 port-member interface Tengigabitethernet 1/2
!
switch 3 description switch-3
!
``` |

7.4.2.2 Configuring Dual-Active Detection

Configuration Effect

Configure the relevant detection mechanism to prevent the dual-active is being generated.

Notes

- The DAD can be configured only in the VSU mode. You are not allowed to configure the DAD mechanism in the standalone mode.
- All DAD configurations will take effect immediately after being configured on the master or slave devices in global configuration mode by running

the **show running-config** command.

- The BFD-detected configuration information can be displayed only by running the dual-active detection display command rather that the BFD display command.

Configuration Steps

❖ **Configuring the BFD DAD**

- The BFD DAD requires establishing a directly connected link between two switches. The interfaces on the two ends must be physical routing interfaces. The following configuration must be performed on both chassis.

- Enter the interface configuration mode of the DAD interface and configure the DAD interface as a routing interface.

- After exiting from the interface configuration mode, run the **switch virtual domain** *domain_id* command to enter the domain configuration mode.

- In the domain mode, run the **dual-active detection bfd** command to enable BFD. This command is optional and can be used when BFD DAD needs to be configured.

- In the domain configuration mode, run the **dual-active bfd interface** *interface-name* command to configure the BFD DAD interface. This command is optional and can be used to configure the BFD DAD interface when BFD DAD is configured.

- Delete the BFD DAD interface. If no BFD DAD interface is available, BFD detection cannot be used.

Command	switch virtual domain *domain_id*
Parameter Description	*domain_id*: Indicates the domain ID.
Defaults	The default domain ID is 100.
Command Mode	config-vs-domain configuration mode
Usage Guide	Only two devices with the same domain ID can form a VSU system. The domain ID must be unique on a LAN.

Command	dual-active detection **{** aggregateport	bfd **}**
Parameter Description	**aggregateport**: Specifies the AP detection mode. **bfd**: Specifies the BFD detection mode.

Defaults	The DAD is disabled.
Command Mode	Domain configuration mode
Usage Guide	Configure this command only in the VSU mode.

Command	dual-active bfd interface *interface-name*
Parameter Description	*interface-name*: Indicates the interface type and ID.
Defaults	N/A
Command Mode	Domain configuration mode
Usage Guide	A BFD DAD interface must be a routing interface and on different switches.

The BFD detection interfaces must be directly connected physical routing ports. The two ports must be on different devices.

The interface type is not limited. The dual-active detection link is only used to transmit BFD packets with a small amount of traffic. Therefore, you are advised to adopt the Gigabit interface or 100 M interface as the dual-active detection interface.

After the layer 3 routing interface that is configured with two master devices is converted into a layer 2 switch interface (run the switchport command under this interface), the BFD dual-active detection will be cleared automatically.

You are advised to directly connect BFD detection interfaces only to the master and slave devices.

When the VSU system detects dual-active conflict and brings another VSU group to the recovery state, you can resolve the problem only by rectifying the VSL fault, but not directly restoring the VSU group in the recovery state; otherwise, dual-active conflict may be caused on the network.

❖ **Configuring the AP-based DAD**

- To configure the AP-based DAD, you must configure an aggregate port (AP) first and then specify the AP port as the DAD interface.

- Run the **port-group** *ap-num* command to add a physical member interface to the AP.

- After entering the domain configuration mode, run the **dual-active detection aggregateport** command to enable AP detection mode. This

command is optional. You can run this command when AP detection needs to be configured.

- Run the **dual-active interface** *interface-name* command to configure the AP as the DAD interface. This command is optional. Yu can run this command to configure the AP as the DAD interface when AP detection needs to be configured.

- Run the **dad relay enable** command to enable dual-active detection packet relay for upstream and downstream interfaces. This command is optional. You can run this command to relay DAD packets (dual-active detection packets) when AP-based DAD is configured.

- Disabling AP-based DAD will inactivate DAD.

- Delete the detected interface. If no AP-based DAD interface is available, AP-based DAD cannot be used.

- The AP-based DAD packet relay is disabled by default.

Command	dual-active detection { aggregateport | bfd }
Parameter Description	**aggregateport**: Specifies the AP detection mode. **bfd**: Specifies the BFD detection mode.
Defaults	The DAD is disabled.
Command Mode	Domain configuration mode
Usage Guide	Configure this command only in the VSU mode.

Command	dual-active interface *interface-name*
Parameter Description	*interface-name*: Indicates the interface type and interface ID. An AP-based DAD interface must be specified.
Defaults	N/A
Command Mode	Domain configuration mode
Usage Guide	Only one AP-based DAD interface can be configured. This interface must be created before you configure an AP as a DAD interface. Subsequently configured DAD interfaces will overwrite the previous ones.

Command	dad relay enable
Parameter Description	N/A
Defaults	The AP-based DAD packet relay is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	This command can only be executed on the AP.

You are advised to distribute the physical interfaces that are added to the AP-based detection interface to different devices.

❖ **Configuring the excluded interface in the recovery mode**

▪ When two master devices are detected, one of them must enter the recovery mode. In the recovery mode, you need to disable all service interfaces. For some special usages (for example, configuring a management switch from which you can log in to a remote interface), you can set some ports to excluded interfaces that are not disabled in the recovery mode.

▪ In the domain configuration mode, run the **dual-active exclude interface** *interface-name* command to specify an excluded interface that will not be disabled in the recovery mode. This command is optional.

Command	dual-active exclude interface *interface-name*
Parameter Description	*interface-name*: Indicates the interface type and interface ID.
Defaults	N/A
Command Mode	Domain configuration mode
Usage Guide	Configure this command only in the VSU mode. An excluded interface must be a routing interface instead of a VSL interface. You can configure multiple excluded interfaces.

In the VSU mode, the across-chassis AP LFF mode and the ECMP LFF mode are disabled by default.

After the excluded interface is converted from a routing one into a switch interface (run the **switchport** command under this interface), the configurations of the excluded interface that is associated with this interface will be cleared automatically.

Verification

Use the show switch virtual dual-active { aggregateport | bfd | summary } to display the current DAD configuration.

Command	show switch virtual dual-active **{** aggregateport	bfd	summary**}**
Parameter Description	**aggregateport**: Displays DAD information on the AP. **bfd**: Displays BFD-based DAD information. **summary**: Displays DAD summary.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

❖ **Configuring the BFD DAD**

Scenario Figure 7-19	
	▪ **Switch 1 and Switch 2 form a VSU (The domain ID is 1) system. The priorities of Switch 1 and Switch 2 are 200 and 150 respectively. The links between Te1/3/1 and Te1/3/2 of Switch 1 and Te2/3/1 and Te2/3/2 of Switch 2 are established respectively to form a VSL between Switch 1 and Switch 2. The G0/1, G0/2, G0/3 and G0/4 interfaces of Switch A are connected to G1/1/1 and G1/2/1 of Switch 1 and G2/1/1 and G2/2/1 of Switch 2 to form an AP group including four member links. The ID of the AP group is 1. All members of AP group 1 are Gigabit optical interfaces. G1/1/2 and G2/1/2 are routing interfaces.** ▪ **G1/1/2 and G2/1/2 are a pair of BFD DAD interfaces.**

Configuration Steps	▪ Configure G1/1/2 and G2/1/2 as routing interfaces. ▪ Enable the BFD DAD. ▪ Configure G1/1/2 and G2/1/2 as BFD DAD interfaces. Since Switch 1 and Switch 2 are in a VSU system, the preceding configuration can be performed on either Switch 1 or Switch 2. on the following example configures the functions on Switch 1.
| **Switch 1** | ```
QTECH(config)#    interface    GigabitEthernet    1/1/2    QTECH(config-if-
GigabitEthernet    1/1/2)#    no    switchport    QTECH(config)#    interface
GigabitEthernet    2/1/2    QTECH(config-if-GigabitEthernet    2/1/2)#    no
switchport QTECH(config-if)# switch virtual domain 1

QTECH(c config-vs-domain)# dual-active detection bfd

QTECH(config-vs-domain)# dual-active bfd interface GigabitEthernet 1/1/2
QTECH(config-vs-domain)# dual-active bfd interface GigabitEthernet 2/1/2
``` |
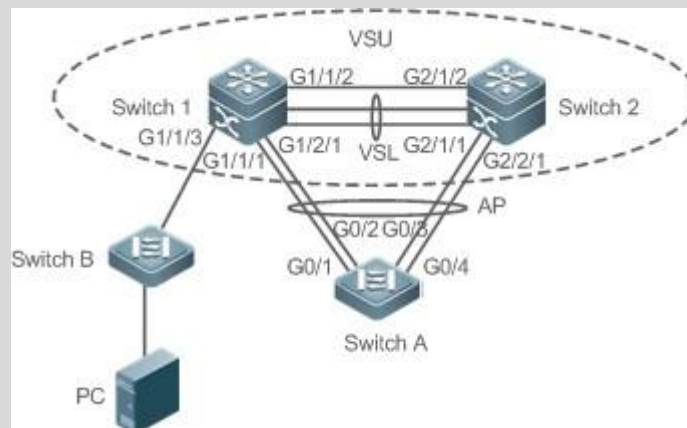| **Switch A** | ```
QTECH# configure terminal

Enter    configuration    commands,    one    per    line.    End    with    CNTL/Z.
QTECH(config)# interface aggretegateport 1
``` |
|  | ```
QTECH(config-if-aggretegateport 1)# interface range GigabitEthernet 0/1-4
QTECH(config-if-aggretegateport 1)# port-group 1

QTECH(config)# interface vlan 1

QTECH(config-if-vlan 1)#ip address 1.1.1.2 255.255.255.0 QTECH(config-if-
vlan 1)#exit

QTECH(config)#interface aggregateport 1 QTECH(config-if-AggregatePort 1)#
dad relay enable

QTECH(config-if-AggregatePort 1)# exit
``` |
| **Verification** | ▪ View the DAD configuration.
▪ View the BFD DAD configuration. |
| **Switch 1** | ```
QTECH# show switch virtual dual-
active summary  BFD dual-active
detection enabled: No  Aggregateport
dual-active detection enabled: Yes
Interfaces excluded from shutdown in
recovery mode: In dual-active
recovery mode: NO
QTECH#  show  switch  virtual  dual-active  bfd  BFD  dual-active  detection
enabled: Yes

BFD dual-active interface configured:

GigabitEthernet 1/1/2: UP GigabitEthernet 2/1/2: UP
``` |

Common Errors

▪ A BFD DAD interface is not a routing interface.
▪ Neither BFD DAD nor AP-based DAD are enabled and activated.

7.4.2.3 Configuring Traffic Balancing

Configuration Effect

In the VSU system, if egresses are distributed on multiple devices, the Local Forward First (LFF) can be configured.

Notes

The default configuration is LFF.

Configuration Steps

❖ **Configuring the AP LFF mode**

▪ In the domain configuration mode, run the **switch virtual aggregateport-lff enable** command to enable the AP LFF mode. This command is optional.

▪ The member ports of AP can be distributed on two chassis of the VSU system. You can configure whether the AP egress traffic is forwarded through local member ports first based on actual traffic conditions.

▪ If this function is disabled, traffic is forwarded based on the AP configuration rules. For details, see the *Configuring Aggregate Port*.

Command	switch virtual aggregateport-lff enable
Parameter Description	N/A
Defaults	This function is enabled by default.
Command Mode	Domain configuration mode
Usage Guide	Enable the AP LFF in the VSU mode.

❖ **Configuring the ECMP LFF mode**

▪ In the domain configuration mode, run the **switch virtual ecmp-lff enable** command to enable the ECMP LFF mode. This command is optional.

▪ The Equal-Cost MultiPath (ECMP) routing egress can be distributed on two chassis of the VSU system. You can configure whether the ECMP egress traffic is forwarded through local member ports first based on actual traffic conditions.

▪ If this function is disabled, traffic is forwarded based on the ECMP configuration rules. For details, see the *Configuring Aggregate Port*.

Command	switch virtual ecmp-lff enable

Parameter Description	N/A
Defaults	This function is enabled by default.
Command Mode	Domain configuration mode
Usage Guide	Enable the ECMP LFF in the VSU mode.

In the VSU mode, the across-chassis AP LFF mode and the ECMP LFF mode are disabled by default.

To deploy a VSU system for layer-3 switches, you are advised to configure the IP-based AP load balancing (src-ip, dst-ip abd src-dst-ip).

Verification

Use the **show switch virtual balance** command to display the current traffic balancing mode of the VSU system.

Command	show switch virtual balance
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display the configuration of the traffic balancing mode in the VSU mode.

Configuration Example

❖ **Configuring the LFF**

Scenario Figure 7-20	
	In Figure 7-20, Switch 1 and Switch 2 form a VSU system. It is assumed that Switch 1 is the global master switch and configuration is performed on Switch 1.

Configuration Steps	Configure the AP LFF.
Switch-1	QTECH#config QTECH(config)# switch virtual domain 100 QTECH(config-vs-domain)# switch virtual aggregateport-lff enable
Verification	Run the **show switch virtual balance** command for verification.
Switch-1	QTECH#show switch virtual balance Aggregate port LFF: enable Ecmp lff enable

7.4.2.4 Changing the VSU Mode to the Standalone Mode

Configuration Effect

Dismiss the VSU system into individual devices that can operate in the standalone mode.

Configuration Steps

- Run the **switch convert mode standalone** [*switch_id*] command to change the VSU mode to the standalone mode. This command is optional.

- After you run this command, the system will prompt you as follows: Whether to restore the configuration file to standalone text? If **yes**, the configuration file will be restored; if **no**, the configuration of virtual device mode will be cleared.

Command	switch convert mode standalone **[*switch_id*]**
Parameter Description	*switch_id*: Indicates the switch ID.
Defaults	The switch is in the standalone mode by default.
Command Mode	Privileged EXEC mode

Usage Guide	After you run the **switch convert mode standalone** command, the master switch backs up the global configuration files of all VSDs in the VSU mode as *vsd.virtual_switch.text.vsd* ID. Then, the master switch clears the global configuration files *config.text* of all VSDs in the VSU mode, and asks you whether to overwrite the global configuration files *config.text* with *vsd.standalone.text.vsd* ID. If you select **yes**, the content of *vsd.standalone.text.vsd* ID will overwrite the global configuration file *config.text* of all VSDs; otherwise, the master switch does not recover *config.text*. Finally, restart the switch. This command can be used in the standalone mode or VSU mode. If the command is executed in the standalone mode, the mode switching is performed on the current switch. If the command contains the *sw_id* parameter and is executed in the VSU mode, the mode switching is performed on the switch with the ID specified by *sw_id*. If the command does not contain the *sw_id* parameter, the mode switching is performed on the master switch. You are advised to switch the mode of the slave switch and then that of the master switch.

Configuration Example

❖ **Changing the VSU Mode to the Standalone Mode**

Scenario Figure 7-21	In Figure 7-21, it is assumed that Switch 1 and Switch 2 form a VSU system and Switch 1 is the global master switch.
Configuration Steps	▪ Change the mode of Switch 1 to the standalone mode. ▪ Change the mode of Switch 2 to the standalone mode.
| Switch-1 | ```
QTECH# switch convert mode standalone 1
QTECH# switch convert mode standalone 2
``` |
| Verification | Run the **show switch virtual config** command to display the switch status. |

| Switch-1 | ```
QTECH#show switch virtual config switch_id: 1 (mac: 0x1201aeda0M)
!
switch virtual domain 100
!
switch 1
switch 1 priority 100
!
switch convert mode standalone
!
port-member interface Tengigabitethernet 1/1
!
port-member interface Tengigabitethernet 1/3
!
switch_id: 2 (mac: 0x1201aeda0E)
!
switch virtual domain 100
!
switch 2
switch 2 priority 150
!
switch convert mode standalone
!
port-member interface Tengigabitethernet 1/1
!
port-member interface Tengigabitethernet 1/2
!
switch 2 description switch-2
!
``` |
|---|---|

7.4.3   Configuring Quick Blinking Location
Configuration Effect

- Enable quick blinking location of a switch to make the status LED of the switch quickly blink.

Notes

If you do not disable quick blinking location, the system automatically disables the function 30 minutes after it is enabled.

Configuration Steps

❖ **Enabling/Disabling quick blinking location**

- Mandatory. Use this function on a switch that needs to be located.

- In the privileged EXEC mode, run the **led-blink** command to enable quick blinking location.

Command	led-blink **{** enable	disable **} [** device *device_id* **]**
Parameter Description	**enable**: Enables quick blinking location. **disable**: Disables quick blinking location. *device_id*: Indicates the device ID.
Defaults	Quick blinking location is disabled by default.
Command Mode	Privileged EXEC mode
Usage Guide	Run this command without the *device_id* parameter to enable or disable the quick blinking search in the standalone mode. In the VSU mode, you can set the *device_id* parameter to enable or disable this function for a specified device. If you ignore the **device_id** parameter, you can enable or disable this function for all devices in the VSU system. If you do not disable this function, the system automatically disables the function 30 minutes after it is enabled. This configuration cannot be saved. Quick blinking location will be disabled upon restart or failover.

Verification

- Check whether the status LED of a switch quickly blinks.

Configuration Example

❖ **Enabling quick blinking location for the two VSU devices**

Scenario	**Assume that Switch 1 and Switch 2 form a VSU system and Switch 1 is the global master device.**
Configuration Steps	▪ Enter the **led-blink enable device** *2* command on the Switch 1 console to enable quick blinking location. ▪ Enter the **led-blink enable device** *2* command on the Switch 1 console to disable quick blinking location.
Verification	When quick blinking location is enabled, check whether the status LED of Switch 2 quickly blinks.

7.5 Monitoring

Displaying

Description	Command
Displays the current VSU operation, topology or configuration.	**show switch virtual** [**topology	config	role**]
Displays the current dual-active configuration.	**show switch virtual dual-active** { **bfd**	**aggregateport**	**summary** }
Redirects to the console of the master switch or any switch.	**session** { **device** *switch_id*	**master** }
Displays the current VSL running information in the VSU mode.	**show switch virtual link** [**port**]
Displays the current switch ID.	**show switch id**

8.1   Overview

The reliable network service (RNS) tests specific services provided by a peer device to monitor the service availability, integrity of the end-to-end connection, and service quality. Using the RNS test results, you can:

- Learn the network performance in time and take measures accordingly to handle related network performance problems.

- Diagnose and locate network faults.

8.2   Applications

8.2.1   Testing and Evaluating Service Performance
Scenario

As shown in the following figure, a company is going to deploy a video conference system between the headquarters and branches, and has completed the related quality of service (QoS) configurations. Before formal deployment, it must be checked whether the services can be provisioned normally under the existing service pressure of the company. The video conference system is sensitive to the User Datagram Protocol (UDP) delay and UDP transmission jitter of the network. The traditional ping tool can test the Internet Control Message Protocol (ICMP) performance, but cannot effectively evaluate the UDP transmission performance and cannot meet the requirement for jitter measurement.

Remarks	A, B, and C are switches.

Deployment

- Configure RNS on the egress switching device or switch of each branch to test the UDP jitter and delay.

- On Switch A, specify the IP address and UDP port of the egress switching device or switch in the headquarters, and then UDP packets can be automatically sent. Based on the configurations, the egress switching device or switch in the headquarters can automatically respond to the UDP packets. The egress switching device or switch of the branch processes the sent and received packets, and calculates the UDP jitter. To learn the performance in different periods of
time, you also need to configure scheduling functions, such as periodically start/stop and repeated running, for the RNS.

8.2.2 Locating Network Faults
Scenario

On the campus network as shown in Figure 8-1, Student 1 reports a Web server access failure, Student 3 reports an Internet access failure, and Student 6 reports an email sending/receiving failure.

Figure 8-1

Deployment

- The administrator directly enables the DNS function on the access switch of the dormitories to test whether the domain name service (DNS) server is faulty. If DNS fails, an ICMP echo packet is automatically triggered to test whether the Web server is reachable.

- When a fault occurs, the administrator only needs to start a test, and the subsequent tests can be automatically triggered. Then, the administrator can check the test results to locate the fault, which greatly reduces the workload for the administrator.

8.3 Features

Basic Concepts

❖ **RNS Instance**

An RNS instance can be treated as an RNS process. Before performing the RNS, you must create an RNS instance. In the RNS instance, you need to configure the RNS parameters, such as the test type, test destination address, and test frequency. The instance ID is globally unique.

Feature	Description
RNS Instance	Monitor the network connectivity, service availability, integrity of end-to-end connection, and service quality.
Track Support for the RNS	Track the test results and notify the related module of the results.

8.3.1 RNS Test

Monitor the network connectivity, service availability, integrity of end-to-end connection, and service quality. For example, test whether the DNS function of the device is normal. Currently, the RNS supports the following types of tests: ICMP echo, DNS, and TCP.

Working Principle

❖ **ICMP Echo Test**

ICMP echo is a basic function of the RNS, and is implemented in compliance with the RFC 2925. An ICMP packet is sent to check whether the destination is reachable and to calculate the network response time and packet loss rate.

An ICMP echo request packet is sent to the destination IP address based on the preset test time and frequency. Upon receipt of the ICMP echo request packet, an ICMP echo reply packet is returned from the destination IP address. Through the ICMP echo test, the response time and packet loss rate is calculated based on the information relating to the received ICMP echo reply packet, for example, the receipt time and number of packets. In this way, the current network performance and status are reflected. The ICMP echo test results and historical records will be recorded, and you can use the command line to display them.

The prerequisite for a successful ICMP echo test is that destination devices can correctly respond to ICMP echo request packets.

❖ **TCP Test**

The TCP test is used to test the availability of a TCP connection. A TCP

connection can be established based on the configured destination IP address and port ID. If the TCP connection is established successfully, the test is successful; otherwise, the test fails.

❖ **DNS Test**

In a DNS test, a DNS client is simulated to send a domain name resolution request to a specified DNS server. You can determine whether the DNS server is available and the domain name resolution speed by checking the domain name resolution result and the time required for domain name resolution. In the DNS test, the domain name resolution process is simulated, and the mapping between the resolved domain name and the IP address is not saved. The DNS test results and historical records will be recorded in the test group. You can use the command line to check the test results and historical records.

❖ **Procedure for Configuring an RNS Instance Test**

1. Create an instance and configure the test based on the test type.

2. Start the instance.

3. Use the RNS instance to construct a packet of the specific test type and send the packet to the peer end.

4. Upon receipt of the test packet, the peer end returns a reply packet of a corresponding type.

5. The RNS instance calculates the packet loss rate and round trip time based on whether a reply packet is received and the time of reply packet receipt.

6. Use the show or debug command to check the test result.

The preceding describes general procedures for RNS instance tests. For details about configuration, see the following sections.

Related Configuration

❖ **Configuring the Test Repeat Interval**

By default, the test repeat interval is 60s.

In RNS configuration mode, run the **frequency** *millisecond* command to configure the test repeat interval. Configure the frequency based on the following formula to ensure correct test calculation.

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

❖ **Configuring the Test Timeout**

The default timeout varies according to the test type. You can run the **show ip rns configuration** command to display the timeout of a specific test type.

In RNS configuration mode, run the **timeout** *milliseconds* command to configure the timeout of an instance. Configure the timeout based on a formula. For details, see the "Usage Guide" of the **frequency** command. Configure the test time threshold.

❖ **Configuring the Test Threshold**

By default, the test threshold is 5,000 ms.

In RNS configuration mode, run the **threshold** *milliseconds* command to configure the instance test threshold. Configure the threshold based on a formula. For details, see the "Usage Guide" of the **frequency** command.

❖ **Configuring a Tag for the Test**

No default configuration is available.

In RNS configuration mode, run the **tag** *text* command to configure a test tag. You can run the **tag** command to specify a tag to identify the test.

❖ **Configuring the Protocol Payload Size**

The default protocol payload size varies with the test type. By default, the protocol payload size is the minimum or appropriate size for protocol packets of the corresponding test type.

In RNS configuration mode, run the **request-data-size** *bytes* command to configure the protocol payload size. Perform this configuration in IP RNS configuration mode.

❖ **Configuring the TOS Field of the Test Packet**

By default, the TOS is 0.

In RNS configuration mode, run the **tos** number command to configure the TOS field in the IPv4 header of RNS test packets.

❖ **Configuring the VRF**

No default configuration is available.

In RNS configuration mode, run the **vrf** *vrf-name* command to virtual routing and forwarding (VRF) for the RNS instance.

8.3.2   Track Support for the RNS

Objects that can be tracked include: test result of an RNS instance, RNS list status, link status on an interface, and track list status. When the track status changes, an action of other modules is triggered.

Working Principle

The test result of an RNS instance is tracked as follows:

- Configure a track object for tracking the test result of an RNS instance.

- When the test result of the RNS instance changes, the RNS module sends a status change message to the track module.

- The track module receives the test result. After the preset delay, if the test result remains unchanged, the status of the track object is modified, and the module of the track object is notified of the modification. If the test result

recovers within the period, the status of the track object is not modified and the corresponding module is not notified.

Related Configuration

❖ **Configuring a Track Object for Tracking the Link Status of An Interface**

By default, the function of tracking the link status of an interface is disabled.

Run the **track interface line-protocol** command to configure a track object, which is used to track the link status of an interface.

If the link status of the interface is UP, the status of the track object is UP. If the link status of the interface is DOWN, the status of the track object is also DOWN.

❖ **Configuring a Track Object for Tracking the Test Result of an RNS Instance**

By default, the function of tracking the test result of an RNS instance is disabled.

Run the **track rns** command to configure a track object, which is used to track the test result of an RNS instance. The RNS instance ID ranges from 1 to 500.

If the RNS test succeeded, the track object is in Up state. If the RNS test failed, the track object is in Down state.

❖ **Configuring a Track Object for Tracking the Test Result of an RNS List**

By default, the function of tracking the test result of an RNS list is disabled.

Run the **track rns-list** command to configure a track object, which is used to track the test result of an RNS list. The RNS instance ID ranges from 1 to 500.

The result can be the AND or OR operation result of all member status. If the result of this track object is set to the OR operation result of all member status, and the OR result of the status of all the tracked RNS objects is UP, the status of this track object is UP. If the OR result of the status of all the tracked RNS objects is DOWN, the status of this track object is also DOWN. If the result of this track object is set to the AND operation result of all member status, and the AND result of the status of all the tracked RNS objects is UP, the status of this track object is UP. If the AND result of the status of all the tracked RNS objects is DOWN, the status of this track object is also DOWN.

❖ **Configuring a Track Object for Tracking the Status of a Track List**

By default, the function of tracking the status of a track list is disabled.

Run the **track list** command to configure a track object, which is used to track the status of a track list. The result can be the AND or OR operation result of all member status.

If the result of this track object is set to the OR operation result of all member status, when all RNS tests succeeded, the track object is in Up state. If one RNS test failed, the track object is in Down state. If the result of this track object is set to the OR operation result of all member status, when all RNS tests failed, the track object is in Down state. If one RNS test succeeded, the track object is in Up state.

❖ **Configuring a Track List Member**

By default, no member is configured for the track list.

Run the **object** command to configure a track list member. The status of the member can be the same as or contrary to that of the corresponding track object.

❖ **Adjusting the Delay for Notifying the Status Change of a Track Object**

By default, the delay for notifying the status change of a track object is 0.

Run the **delay** command to adjust the delay for track notification, including the delay for notifying the status change of a track object from UP to DOWN and the delay for notifying the status change of a track object from DOWN to UP. The delay ranges from 0 to 180. The unit is second.
A longer delay indicates that it takes more time before the module that is concerned with the track object is notified of the status. A shorter delay indicates that it takes less time before the module that is concerned with the track object is notified of the status.

8.4   Configuration

Configuration Item	Description and Command	
Configuring RNS Basic Functions	(Mandatory) It is used to configure basic function parameters of the RNS.	
	ip rns	Supports detailed configuration and brief configuration. ▪ Detailed configuration: An RNS operation object is defined, and used as the configuration ID for subsequent tests and parameters. ▪ Brief configuration: Subsequent configuration is not required, and tests can be started in one step. Currently, ICMP echo, DNS, and TCP tests can be started in one step.
	ip rns reaction-configuration	Configures the proactive threshold monitoring and triggering mechanism of the RNS test.
	ip rns reaction-trigger	Triggers another type of the RNS test in pending state when the monitoring threshold exceeds the expectation during an RNS test.

	ip rns schedule	Configures the scheduling method, start time, and life time of an RNS test.
	ip rns restart	Restarts an RNS test.
	ip rns reset	Clears all the IP RNS configurations.
Configuring the ICMP Echo Test	(Optional) It is used to implement the ICMP echo test.	
	icmp-echo	Creates an ICMP echo test instance.
	request-data-size	Configures the protocol payload size.
	frequency	Configures the test repeat interval.
	tag	Configures a tag.
	threshold	Configures the test time threshold.
	timeout	Configures the test timeout.
	tos	Configures the TOS field in the IPv4 header of test packets.
	vrf	Configure the VRF of a test.
Configuring the DNS Test	(Optional) It is used to implement the DNS test.	
	dns	Creates a DNS test instance.
	frequency	Configures the test repeat interval.
Configuration Item	**Description and Command**	
	tag	Configures a tag.
	threshold	Configures the test time threshold.
	timeout	Configures the test timeout.
	tos	Configures the TOS field in the IPv4 header of test packets.
	vrf	Configures the VRF of a test.

Configuring the TCP Connect Test	(Optional) It is used to implement the TCP connect test.	
	tcp-connect	Creates a TCP test instance.
	request-data-size	Configures the protocol payload size.
	frequency	Configures the test repeat interval.
	tag	Configures a tag.
	threshold	Configures the test time threshold.
	timeout	Configures the test timeout.
	tos	Configures the TOS field in the IPv4 header of test packets.
	vrf	Configure the VRF of a test.
Configuring the Track Support for the RNS	(Optional) It is used to configure the track support for other test modules.	
	track rns	Configures a track object for tracking the test result of an RNS instance.
	track rns-list	Configures a track object for tracking the status of an RNS list.
	track interface line-protocol	Configures a track object for tracking the link status of an interface.
	track list	Configures a track object for tracking the status of a track list.
	object	Configures a member object for a track list object.
	delay	Configures the delay for notifying the status change of a track object.

8.4.1   Configuring RNS Basic Functions
Configuration Effect

- Detailed configuration: Configures an RNS instance to complete basic configuration of the RNS instance.

- Brief configuration: Configure and start an RNS instance at a time. (Optional)

Notes

- In detailed configuration mode, if you do not configure the test type after entering the IP RNS mode by running the command, the RNS instance will not be created.

- In detailed configuration mode, after configuring an RNS instance, you need to run the **ip rns schedule** command to configure the startup policy; otherwise, the test will not be implemented.

Configuration Steps

❖ **Defining an RNS Operation Object**

- Mandatory.

- Unless otherwise required, define an RNS operation object on each switch.

- Brief configuration is optional.

❖ **Configuring the Proactive Threshold Monitoring and Triggering Mechanism for an RNS Test**

- Perform this configuration if it is required to configure the proactive threshold monitoring and triggering mechanism for the test.

- Perform this configuration on every switching device unless otherwise required.

❖ **Enabling an RNS Instance to Trigger Another RNS Instance**

- Perform this configuration if it is required to trigger another RNS test in pending state when the monitoring threshold exceeds the expectation during an RNS test.

- If schedule parameters are not configured for the triggered RNS instance, the default schedule parameters are applied.

- Unless otherwise required, apply this configuration to each switch.

❖ **Configuring Schedule Parameters of an RNS Instance**

- Perform this configuration on every switching device unless otherwise required.

- In the case of brief configuration, this command is already configured using the default values, and manual configuration is not required.

❖ **Restarting an RNS Instance**

www.qtech.ru

- Perform this configuration, or directly run the **ip rns schedule X start-time now** command if it is required to restart an IP RNS instance in pending state.

❖ **Clearing Configurations of All RNS Instances**

- Perform this configuration if it is required to clear configurations of all the IP RNS instances, for example, when a lot of instances are configured but configurations are found incorrect.

Verification

- Run the **show ip rns configuration** command to display configurations of RNS instances.

Related Commands

❖ **Defining an IP RNS Operation Object**

Command	ip rns *operation-number* **[{**dns *destination-hostname* name-server *ip-address*	icmp-echo *destination-ip-address*	tcp-connect *destination-ip-address port-number***}** **[**frequency *seconds***] [**timeout *milliseconds***] [**threshold *milliseconds***]]]**
Parameter Description	*operation-number*. Indicates the RNS instance ID. The value ranges from 1 to 500. For details about configuration of **frequency**, **timeout**, and **threshold**, see the configuration of the specific test type.
Command Mode	Global configuration mode

| Usage Guide | Currently, the RNS supports only IPv4-related tests, but not IPv6-related tests. At most 500 tests can be configured, depending on the performance of devices. The test function is only a value-added function. When a large number of tests are configured and consume a lot of system resources, the test function may be temporary disabled to ensure normal operation of core services, such as route forwarding. Detailed configuration (executing mandatory items of **ip rns** *operation-number*): Run this command and enter the IP-RNS configuration mode. In this mode, you can define various test types. If the test type is not configured, the RNS test is not created. After configuring an RNS test, you must run the **ip rns schedule** command to configure its schedule parameters; otherwise, the test cannot be conducted. After configuring the type of an RNS test, you can run the **ip rns** command to enter the mode of the test type. To modify the type of an RNS instance, you need to first delete the RNS instance by running the **no ip rns** command in global configuration mode. Brief configuration (executing the optional test items that proceeds **ip rns**):After optional items are executed, it is equivalent that **ip rns operation-number**, **ip rns schedule**, detailed test configuration (such as the ICMP echo test), **frequency**, **timeout**, and **threshold** are executed according to the logical sequence. Among these commands, the **ip rns schedule** command is executed to start a test by using the **start-time now life forever** parameter. For details about restrictions of other configuration items, see the related description in the detailed configuration. Similarly, to modify a briefly configured test, you need to first delete this RNS instance by running the **no ip rns** command in global configuration mode. |

❖ Configuring the Proactive Threshold Monitoring and Triggering Mechanism for the Test

Command	ip rns reaction-configuration *operation-number* react *monitored-element*[action-type *option*][threshold-type {average [*number-of-measurements*] | consecutive [*occurrences*] | immediate | never| xofy [*x-value y-value*] }] [threshold-value *upper-threshold lower-threshold*]
Parameter Description	*operation-number*: Indicates the RNS instance ID. The value ranges from 1 to 500. *monitored-element*: Specifies the monitored element. **action-type** *option*: Indicates the action taken after the test is triggered. **average** [*number-of-measurements*]: Indicates that the subsequent associated actions are triggered if the average of *number-of-*

	measurements of the monitored element exceeds the threshold. **consecutive** [*occurrences*]: Indicates that the test is triggered if the consecutive number of *occurrences* of the monitored element exceeds the threshold. The default value of *occurrences* is 5. The value ranges from
	1 to 16. **immediate**: Indicates that the test is triggered immediately after the monitored element exceeds the threshold. **never**: Indicates that the test is never triggered. **xofy** [*x-value y-value*]: Indicates that results of X tests exceed the threshold in the last Y tests. The default values of X and Y are 5. The value of X or Y ranges from 1 to 16. **threshold-value** *upper-threshold lower-threshold*: Indicate the upper and lower thresholds. ▪ When *monitored-element is* **rtt**, the thresholds are the time. For default values, see "Usage Guide". The value ranges from 0 to 60,000 ms. ▪ Note that you do not need to configure **threshold-value** when **react** is set to **timeout**.
Command Mode	Global configuration mode
Usage Guide	You can configure multiple thresholds for one RNS test to monitor different elements. The following table provides the mapping between test types and monitored elements. 	monitored-element	icmp-echo	dns
---	---	---
timeout	✓	✓
rtt	✓	✓ | The following table lists the default thresholds of each monitored element. | Monitored Element	Upper Threshold	Lower Threshold
---	---	---
timeout	-	-
rtt	5000ms	0ms	

❖ Enabling an RNS Instance to Trigger Another RNS Instance

Command	ip rns reaction-trigger *operation-number target-operatio***n**
Parameter Description	*operation-number*: Indicates the number of the source RNS instance that triggers the action. The value ranges from 1 to 500. *target-operation*: Indicates the number of the target RNS instance that is triggered. The value ranges from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	The trigger function is generally used in network fault diagnosis scenario. In a common scenario, you do not need to configure the trigger function.

❖ Configuring Schedule Parameters of an RNS Instance

Command	ip rns schedule ***operation-number*[** life**{** forever|***seconds}*] [** start-time**{** *hh***:***mm***[** :*ss***]** [*month day*|*daymonth*] |pending|now|after*hh***:***mm***:***ss}*] [** recurring**]**
Parameter Description	*operation-number*: Indicates the number of the RNS operation. The value ranges from 1 to 500. **lifeforever**: Indicates that the RNS operation life time is valid forever. **life** *seconds*: Indicates the running time of the RNS instance in seconds. *hh:mm[:ss]*: Indicates the start time of the RNS instance, in 24-hour format. *month*: Indicates the start month of the RNS instance. The default value is the current month. *day*: Indicates the start date of the RNS instance. The default value is the current date. **pending**: Indicates that the start time of the RNS instance is not defined, which is the default. **now**: Indicates that the operation start time is now, that is, the operation starts now. **after***hh:mm:ss*: Indicates that the RNS instance starts after a delay of hh:mm:ss. **recurring**: Indicates whether the RNS instance starts at the same time every day.
Command Mode	Global configuration mode

Usage Guide	If the schedule parameters of an RNS instance have been configured by running the **ip rns schedule** command, parameters cannot be modified during running. To modify the configuration, you need to run the **no ip rns schedule** command to delete the schedule parameters. life { *seconds* } indicates the running time of the RNS instance. That is, the test stops after a period of time in seconds.

❖   Restarting an RNS Test by Running the ip rns restart Command

Command	ip rns restart *operation-number*
Parameter Description	*operation-number*: Indicates the number of the RNS instance. The value ranges from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	This command restarts an RNS test for which the scheduling policy is configured and is in pending state. This command is invalid for an RNS test for which the scheduling policy is not configured.

❖   Clearing Configurations of All the IP RNS Instances by Running the ip rns reset Command

Command	ip rns reset
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command clears configurations of all the IP RNS instances. It is used only in extreme cases, for example, when a lot of RNS tests are configured but the configurations are found incorrect.

Configuration Example

❖   Configuring RNS Basic Functions

Scenario Figure 8-2	
Configuration Steps	▪ Configure instance 1 on Switch A. ▪ Configure the scheduling method, start time, and life time of instance 1. ▪ Configure the proactive threshold monitoring and triggering mechanism of instance 1. ▪ Trigger instance 2 in pending state when the monitoring threshold of instance 1 exceeds the expectation.

Switch A	```A# configure terminal A(config)# ip rns 1```
	 ```A(config-ip-rns)#icmp-echo 10.1.1.1 A(config-ip-rns-icmp-echo)#exit```
	 ```A(config)ip rns schedule 1 start-time now life forever```
	 ```A(config)ip rns reaction-configuration 1 react timeout threshold-type immediate action-type trigger A(config)ip rns reaction-trigger 1 2```

Verification	Run the **show ip rns configuration** command to display the instance configurations.
	
	 ```Router#show ip rns configuration 1 Entry number: 1```
	 ```Tag: QTECH555```
	
	 ```Type of operation to perform: icmp-echo Operation timeout (milliseconds): 5000 Operation frequency (milliseconds): 60000 Threshold (milliseconds): 5000```
	 ```Recurring (Starting Everyday): FALSE Life (seconds): 3500```
	 ```Next Scheduled Start Time:Start Time already passed```
	 ```Target address/Source address: 2.2.2.3/0.0.0.0 Request size (ARR data portion): 36```

8.4.2   Configuring the ICMP Echo Test
Configuration Effect

Create an ICMP echo test instance.

Notes

▪ The RNS basic functions must be configured.

Configuration Steps

❖ **Creating an ICMP Echo Test Instance**

▪ Mandatory.

▪ Unless otherwise required, create ICMP echo test instances on each switch.

❖ **Configuring Common Optional Parameters of the Test**

▪ Mandatory if common optional parameters of the test, for example, the repeat interval, tag, time threshold, timeout, and TOS, are required to be changed..

▪ Perform this configuration on every switching device unless otherwise required.

❖ **Configuring the Protocol Payload Size**

▪ Perform this configuration if it is required to change the protocol payload size of the test.

▪ Perform this configuration on every switching device unless otherwise required.

Verification

▪ Run the **show ip rns configuration** command to display the instance configurations.

Related Commands

❖ **Creating an ICMP Echo Test Instance**

Command	icmp-echo **{** oob **{** *destination-ip-address* **|** *destination-hostname* **[** name-server *ip-address* **]** **}** **[** source-ipaddr *ip-address* **]** via *type num* next-hop *ip-address* **}** **|** **{ {** *destination-ip-address* **|** *destination-hostname* **[** name-server *ip-address* **]** **}** **[** source-ipaddr *ip-address* **|** source-interface *interface-type interface-number***]** **[**out-interface *type num* **[** next-hop *ip-address* **]] }**
Parameter Description	**oob**: Indicates the test on the MGMT interface. *destination-ip-address*: Indicates the destination IP address. *destination-hostname*: Indicates the destination host name. **name-server** *ip-address*: Specifies the DNS server when the destination host name is configured. By default, the DNS server configured by using the **ip name-server** command is used for address resolution. **source-ipaddr** *ip-address*: Indicates the source IP address. **source-interface** *interface-type interface-numbe*r: Indicates the source interface.
	out-interface *type num*: Specifies the outgoing interface (non-MGMT interface) of the test packet. **via** *type num*: Specifies the MGMT interface as the outgoing interface of the test packet.

	next-hop *A.B.C.D*: Indicates the IP address of the next hop.
Command Mode	IP RNS configuration mode (config-ip-rns)
Usage Guide	After an ICMP echo test is started, the system sends an ICMP echo request packet to test whether the device is connected to the target host. After an ICMP-Echo test instance is created, the system enters the IP RNS ICMP echo mode. By default, the protocol payload size of an ICMP echo request packet is 36 bytes. You can run the **request-data-size** command to change the packet size. You need to configure the RNS test type (for example, ICMP echo and DNS) before configuring parameters. To modify the type of an RNS instance, you need to delete the RNS instance by running the **no ip rns** command in global configuration mode.

❖ Configuring the Protocol Payload Size of an RNS Instance

Command	request-data-size *bytes*
Parameter Description	*bytes*: Indicates the bytes of a test packet. The minimum and maximum bytes vary with the test type. You need to configure this parameter based on the command prompt in corresponding test mode.
Command Mode	IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	This command is used to stuff some bytes in the test packet so that large packets can be used for the test.

❖ Configuring the Test Repeat Interval

Command	frequency *milliseconds*
Parameter Description	*milliseconds*: Indicates the packet sending interval in ms. The default value is 60,000 ms. The value ranges from 10 to 604,800,000. The maximum value is one week.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)

Usage Guide	After an RNS instance is started, tests are conducted periodically. You can run the **frequency** command to specify the repeat interval. You need to configure the frequency based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *millisecond*s)

❖   Configuring a Tag for an RNS Instance

Command	tag *text*
Parameter Description	*text*: Sets the test tag. The value is a string of up to 79 characters.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	This command specifies a tag for a test, which is often used to indicate the function of the test.

❖   Configuring the Time Threshold for an RNS Instance

Command	threshold *milliseconds*
Parameter Description	*milliseconds*: Indicates the time threshold for the test. The value ranges from 0 to 60,000, in the unit of milliseconds. The default value is 5,000.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	Configure the threshold based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *millisecond*s)

❖   Configuring the Timeout for an RNS Instance

Command	timeout *millisecond*

Parameter Description	*millisecond*: Indicates the test timeout. The value ranges from 10 to 604,800,000. The unit is ms. The default timeout varies according to the test type.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	Configure the timeout based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

❖   Configuring the TOS Field in the IPv4 Packet Header of an IP RNS Test

Command	tos *number*
Parameter Description	*number*: Sets the TOS field in the IPv4 header of test packets. The value ranges from 0 to 255. The default value is 0.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	TOS is a 8-bit field in the IPv4 packet header. By setting the TOS, you can control the priority of the test packet. For different TOS fields, the processing priorities are different on the intermediate routers.

❖   Configuring the VRF of an RNS Test

Command	vrf *vrf-name*
Parameter Description	*vrf-name*: Specifies the VRF name.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	This command specifies the VRF of the test packet.

Configuration Example

Figure 8-3	
	Configure RNS instance 1 and related parameters on Switch A.
Switch A	A# configure terminal A(config)# ip rns 1 A(config-ip-rns)#icmp-echo 10.2.2.2 A(config-ip-rns-icmp-echo)#exit A(config)#ip rns schedule 1 start-time now life forever
	Run the **show ip rns configuration** command to display the instance configurations.
Switch A	A#show ip rns configuration 1 Entry number: 1 Tag: Type of operation to perform: icmp-echo Operation timeout (milliseconds): 5000 Operation frequency (milliseconds): 60000 Threshold (milliseconds): 5000 Recurring (Starting Everyday): FALSE Life (seconds): foerver Next Scheduled Start Time:Start Time already passed Target address/Source address: 10.2.2.2/0.0.0.0 Request size (ARR data portion): 36

8.4.3 Configuring the DNS Test
Configuration Effect

Create a DNS test instance.

Notes

- The RNS basic functions must be configured.

Configuration Steps

❖ **Creating a DNS Test Instance**

- Mandatory.

- Unless otherwise required, create DNS test instances on each switch.

❖ **Configuring Common Optional Parameters of the Test**

- Mandatory if common optional parameters of the test, for example, the repeat interval, tag, time threshold, timeout, and TOS, are required to be changed.

- Perform this configuration on every switching device unless otherwise required.

Verification

- Run the **show ip rns configuration** command to display the instance configurations.

Related Commands

❖ **Creating a DNS Test Instance**

Command	dns { oob *destination-hostname* name-server *ip-address* [source-ipaddr *ip-address*] via *type num* next-hop *ip-address* } | { *destination-hostname* name-server *ip-address* [source-ipaddr *ip-address*] [out-interface *type num* [next-hop *ip-address*]] }
Parameter Description	**oob**: Indicates the test on the MGMT interface.
	destination-hostname: Indicates the destination host name. **name-server** *ip-address*: Indicates the DNS IP address. **source-ipaddr** *ip-address:* Indicates the source IP address. **out-interface type** *num*: Specifies the outgoing interface (non-MGMT interface) of the test packet.
	via *type num*: Specifies the MGMT interface as the outgoing interface of the test packet.
	next-hop *ip-address*: Indicates the IP address of the next hop when the outgoing interface is specified.
Command Mode	IP RNS configuration mode (config-ip-rns)
Usage Guide	After a DNS test is started, the system sends a DNS parsing request packet to test whether the device is connected to the target host. After a DNS test instance is created, the system enters the IP RNS DNS mode. You need to configure the RNS test type before configuring parameters. To modify the type of an RNS instance, you need to delete the RNS instance by running the **no ip rns** command in global configuration mode.

❖ Configuring the Test Repeat Interval

Command	frequency *milliseconds*
Parameter Description	*milliseconds*: Indicates the packet sending interval in ms. The default value is 60,000 ms. The value ranges from 10 to 604,800,000. The maximum value is one week.

Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	After an RNS instance is started, tests are conducted periodically. You can run the **frequency** command to specify the repeat interval. You need to configure the frequency based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *millisecond*s)

❖ Configuring a Tag for an RNS Instance

Command	tag *text*
Parameter Description	*text*: Sets the test tag. The value is a string of up to 79 characters.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	This command specifies a tag for a test, which is often used to indicate the function of the test.

❖ Configuring the Time Threshold for an RNS Instance

Command	threshold *milliseconds*
Parameter Description	*milliseconds: Indicates the time threshold for the test. The value ranges from 0 to 60,000, in the unit of milliseconds. The default value is 5,000.*
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	Configure the threshold based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *millisecond*s)

❖ Configuring the Time Threshold for an RNS Instance

QTECH
МИР ДОСТУПНЕЕ   www.qtech.ru

Command	timeout *millisecond*
Parameter Description	*millisecond*: Indicates the test timeout. The value ranges from 10 to 604,800,000. The unit is ms. The default timeout varies according to the test type.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	Configure the timeout based on the following formula to ensure correct test calculation. (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *millisecond*s)

❖ Configures the TOS Field in the IPv4 Header of Test Packets

Command	tos *number*
Parameter Description	*number*: Sets the TOS field in the IPv4 header of test packets. The value ranges from 0 to 255. The default value is 0.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)
Usage Guide	TOS is a 8-bit field in the IPv4 packet header. By setting the TOS, you can control the priority of the test packet. For different TOS fields, the processing priorities are different on the intermediate routers.

❖ Configuring the VRF of an RNS Test

Command	vrf *vrf-name*
Parameter Description	*vrf-name*: Specifies the VRF name.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo) IP RNS TCP configuration mode (config-ip-rns-tcp)

Usage Guide	This command specifies the VRF of the test packet.

Configuration Example

Scenario Figure 8-4	
Configuration Steps	Configure RNS instance 1 and related parameters on Switch A.
Switch A	A# configure terminal A(config)# ip rns 1 A(config-ip-rns)# dns www.QTECH.com.cn name-server 10.2.2.2 A(config-ip-rns-dns)#exit A(config)ip rns schedule 1 start-time now life forever
Verification	Run the **show ip rns configuration** command to display the instance configurations.
Switch A	A#show ip rns configuration 1 Entry number: 1 Tag: Type of operation to perform: dns Operation timeout (milliseconds): 5000 Operation frequency (milliseconds): 60000 Threshold (milliseconds): 5000 Recurring (Starting Everyday): FALSE Life (seconds): forever Next Scheduled Start Time:Start Time already passed Target host name: www.QTECH.com.cn Name Server: 10.2.2.2

Common Errors

▪ The DNS IP address is incorrect.

8.4.4 Configuring the TCP Connect Test
Configuration Effect

Create a TCP test instance to implement a TCP connect test.

Notes

▪ The RNS basic functions must be configured.

▪ The target host must be able to respond to the TCP connection request.

Configuration Steps

❖ **Creating a TCP Test Instance**

▪ (Mandatory) Unless otherwise required, create TCP test instances on each switch.

❖ **Configuring Common Optional Parameters of the Test**

▪ Mandatory if common optional parameters of the test, for example, the repeat interval, tag, time threshold, timeout, and TOS, are required to be changed.

▪ Perform this configuration on every switch unless otherwise required.

Verification

▪ Run the **show ip rns configuration** command to display the instance configurations.

Related Commands

❖ **Creating a TCP Test Instance**

Command	tcp-connect { **destination-ip-address**	**destination-hostname** [name-server **ip-address] } port-number**
Parameter Description	*destination-ip-address*: Destination IP address *destination-hostname*: Indicates the destination host name. **name-server**_ip-address_: Indicates the IP address of the DNS server. *port-number*: Indicates the TCP port to be tested.
Command Mode	IP RNS configuration mode (config-ip-rns)
Usage Guide	After a TCP test is started, the system tries to establish a TCP connection to the specified port of a specified host to test whether the specified port is available. After a TCP IP RNS instance is created, the system enters the IP RNS TCP mode.

Commands for configuring common optional parameters of a test, including **frequency**, **tag**, **threshold**, **timeout**, and

tos, are provided in the description about configuring an ICMP echo test, and therefore omitted here.

Configuration Example

Scenario	
Configuration Steps	Configure RNS instance 1 and related parameters on Switch A.
| **Switch A** | ```
A# configure terminal A(config)# ip rns 1
A(config-ip-rns)# tcp-connect 10.2.2.2 8000 A(config-ip-rns-tcp)#exit
A(config)ip rns schedule 1 start-time now life forever
``` |
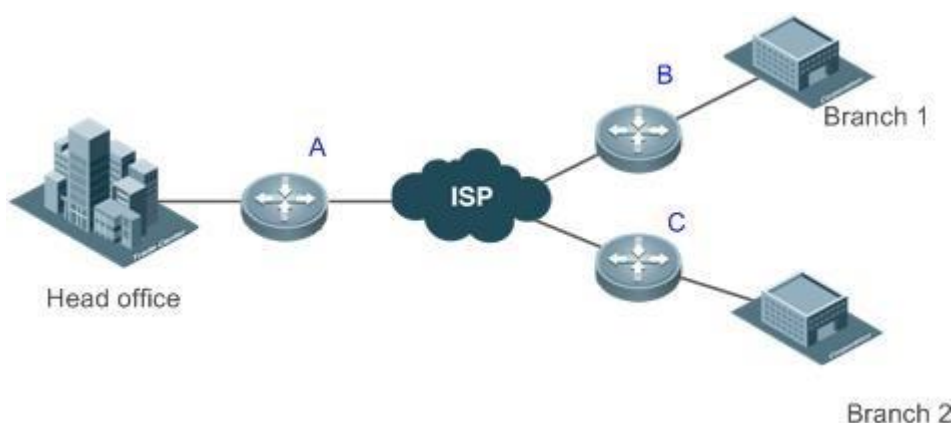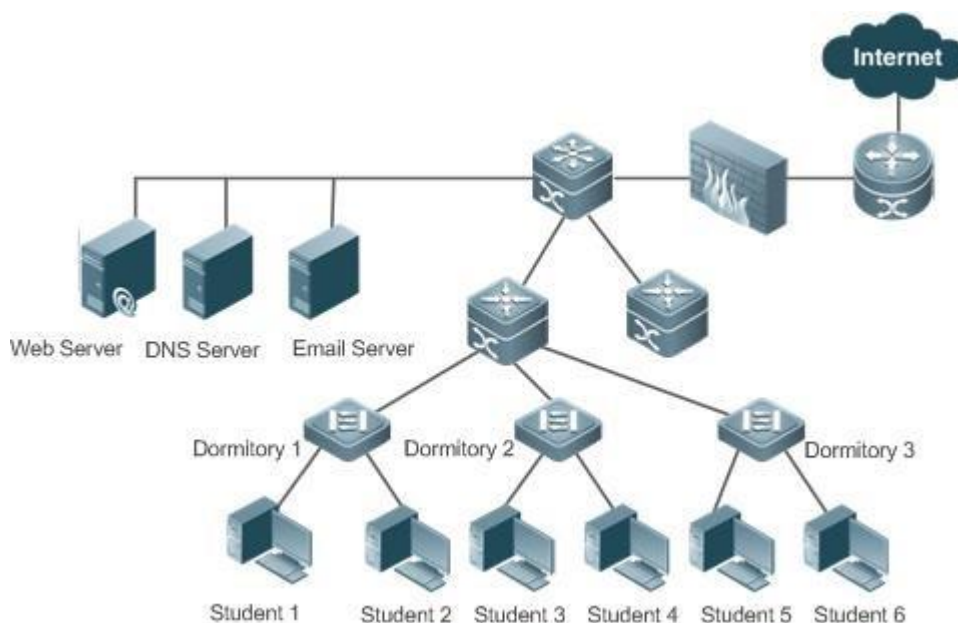| **Verification** | Run the **show ip rns configuration** command to display the instance configurations. |
| **Switch A** | ```
A#show    ip    rns
configuration 1 Entry
number: 1

Tag:

Type  of  operation  to  perform:
tcp-connect   Operation   timeout
(milliseconds):  5000  Operation
frequency (seconds): 60 Threshold
(milliseconds): 5000

Recurring        (Starting
Everyday):    FALSE    Life
(seconds): forever

Next  Scheduled  Start  Time:Start  Time
already passed Target Address: 10.2.2.2
``` |

Common Errors

- The target host does not respond to the TCP connection request.

- The TCP port for the RNS test is incorrectly configured.

8.4.5 Configuring the Track Support for the RNS
Configuration Effect

- Configure the track function to track the test result of an RNS instance.

- Configure the track function to track the link status of an interface.

- Configure the track function to track the status of a track list.

- Configure the track function to track the status of an RNS list.

Notes

- To configure the track function to track the test result of an RNS

instance, you need to configure the related RNS instance.

- To configure the track function to track the link status of an interface, you need to configure the related interface.

- To configure the track function to track the status of a track list, you need to configure the members for the related track list.

- To configure the track function to track the status of an RNS list, you need to configure the members for the related RNS list.

Configuration Steps

❖ Configuring a Track Object

- Perform this operation if it is required to create a track object.

- The following four methods are available to create a track object:

  -Create a track object for tracking the test result of an RNS instance: Perform this configuration on every switching device unless otherwise required.

  -Create a track object for tracking the link status of an interface: Perform this configuration on every switching device unless otherwise required.

  -Create a track object for tracking the status of a track list: Perform this configuration on every switching device unless otherwise required.

  -Create a track object for tracking the status of an RNS list: Perform this configuration on every switching device unless otherwise required.

❖ Configuring the Notification Delay of a Track Object

- Perform this configuration if it is required to delay notification of the status change of a track object.

- Delay for notifying the status change of a track object includes the delay for notifying the status change of a track object from UP to DOWN and the delay for notifying the status change of a track object from DOWN to UP. You can configure either delay or both of delays.

- Perform this configuration on every switching device unless otherwise required.

❖ Configuring a Track Member

- Perform this configuration if it is required to configure a track object for tracking the status of a track list.

- When configuring a track member, you can set the status of a member meeting conditions to UP or DOWN.

- Perform this configuration on every switching device unless otherwise required.

Verification

Observe the status of a track object when the status of the track object (such as test results of an RNS instance, link status of an interface, or status of a track list)

changes.

- After the preset delay, run the **show track** command to check whether the current track status changes.

Related Commands

❖ **Configuring a Track Object for Tracking the Link Status of An Interface**

Command	track *object-number* interface *interface-type interface-number* line-protocol
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700. *Interface-type interface-number*: Indicates the interface type and interface number.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the link status of an interface. When the link status of the interface is UP, the status of the corresponding track object is UP.

❖ Configuring a Track Object for Tracking the Test Result of an RNS Test

Command	track *object-number* rns *entry-number*
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700. *entry-number*: Indicates the number of an RNS instance. The value ranges from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the result of an RNS test. If the test succeeded, the track object is in Up state.

❖ Configuring a Track Object for Tracking the Status of a Track List

Command	track *object-number* list boolean **{** and **|** or **}**
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700.

Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the status of a track list. The result can be the AND or OR operation result of all member status.

❖ Configuring a Track Member

Command	object *object-number*[not]
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700.
Command Mode	Track configuration mode
Usage Guide	Run this command to configure a member for a track list. The number of track list members that can be configured is restricted only by the capacity of track objects.

❖ Configuring a Track Object for Tracking the Status of an RNS List

Command	track *object-number* rns-list *men-list*{ and | or }
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700. men-list: Indicates the RNS list that is tracked. **mem-list** can be an RNS instance or a series of RNS instances. If **mem-list** is a series of RNS instances, the format is as follows: Smallest RNS ID–Greatest RNS ID, for example, 10–20. The RNS ID ranges from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the status of an RNS list. The result can be the AND or OR operation result of all member status.

❖ Configuring the Notification Delay of a Track Object

Command	delay { up *seconds* [down *seconds*] | [up *seconds*] down *seconds* }

Parameter Description	**up** *seconds*: Specifies the delay for notifying the status change of a track object from DOWN to UP. The value ranges from 0 to 180. The unit is second. The default value is 0. **down** *seconds*: Specifies the delay for notifying the status change of a track object from UP to DOWN. The value ranges from 0 to 180. The unit is second. The default value is 0.
Command Mode	Track configuration mode
Usage Guide	When the status of a track object frequently changes, the status of the client that use this track object will frequently change as well. Using this command can delay notification of the status change of a track object. For example, if the status of a track object changes from UP to DOWN, and **delay down 10** is configured, the DOWN status of the track object is notified 10s later. If the status of the track objects changes to UP again within this period of time, no notification is sent. For the client that uses this track object, the status of the track object is always UP.

❖ Displaying the Track Object Statistics

Command	show track **[** *object-number* **]**
Parameter Description	*object-number*: Indicates the number of a track object. The value ranges from 1 to 700. The default is all track objects.
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display statistics of track objects.

Configuration Example

❖ Configuring Track Object3 for Tracking the Link Status of the Interface FastEthernet 1/0

Configuration Steps	▪ **Configure a track object for tracking the link status of an interface.** ▪ **Configure the delay for notifying the status change from UP to DOWN.**

| | ```
QTECH# configure terminal

QTECH(config)#  track  3  interface  FastEthernet  1/0  line-protocol
QTECH(config-track)# delay down 10

QTECH(config-track)# exit
``` |
| **Verification** | Change the link status of the interface FastEthernet 1/0 to DOWN.
▪ Immediately check the status of the track object, and verify that the status is still UP.
▪ Check the status of the track object 10s later, and verify that the status changes to DOWN. |
| | ```
QTECH# show track 3 Track 3
Interface FastEthernet 1/0
``` |
| **Configuration Steps** | ▪ Configure a track object for tracking the link status of an interface.
▪ Configure the delay for notifying the status change from UP to DOWN. |
| | ```
QTECH# configure terminal

QTECH(config)#  track  3  interface  FastEthernet  1/0  line-protocol
QTECH(config-track)# delay down 10

QTECH(config-track)# exit
``` |
| **Verification** | Change the link status of the interface FastEthernet 1/0 to DOWN.
▪ Immediately check the status of the track object, and verify that the status is still UP.
▪ Check the status of the track object 10s later, and verify that the status changes to DOWN. |
| | ```
The state is Up, delayed Down (5 secs remaining) 1 change, current
state last: 300 secs
Delay up 0 secs, down 10 secs
``` |

❖ Configuring Track Object 3 (When the status of track object 1 is UP, and the status of track object 2 is DOWN, the status of track object 3 is UP.)

Configuration Steps	▪ **Configuring track object 1 and track object 2.** ▪ **Configure track object 3, and its members include track object 1 and track object 2.**

```
QTECH # config

QTECH(config)#track  1  interface  gigabitEthernet  0/0  line-protocol
QTECH(config-track)#delay up 20 down 40

QTECH(config-track)#exit QTECH(config)#

QTECH(config)#track  2  interface  gigabitEthernet  0/1  line-protocol
QTECH(config-track)#delay down 30

 QTECH(config-
track)#exit
QTECH(config)# track 3
 list Boolean and
 QTECH(config-
track)#object 1

QTECH(config-track)#object 2 not

QTECH(config-track)# exit
```

Verification	When the status of track objects 1 and 2 change, check the status of track object 3.
	▪ When the status of track object 1 changes from DOWN to UP, and the status of track object 2 remains DOWN, verify that the status of track object 3 changes from DOWN to UP.
	▪ When the status of track object 1 remains UP, and the status of track object 2 changes from DOWN to
	UP, verify that the status of track object 3 changes from UP to DOWN.

```
QTECH# show track 3
Track 3
List boolean and Object 1
Object 2 not
The state is Down
1 change,current state last:10 secs Delay up 0 secs,down 0 secs
```

❖ Configuring Track Object 5 for Tracking the Test Result of RNS Instance 7

Configuration Steps	▪ **Configure an RNS test.**
	▪ **Configure a track object to track the result of the RNS test.**
	▪ **Configure the delay for notifying the test result change from successful to unsuccessful, and the delay for notifying the test result change from unsuccessful to successful.**

```
QTECH# configure terminal QTECH (config)#ip rns 7
QTECH (config-ip-rns)#icmp-echo 2.2.2.2 QTECH (config-ip-rns-icmp-
echo)#exit
QTECH (config)#ip rns schedule 7 start-time now life forever
QTECH(config)# track 5 rns 7
QTECH (config-track)# delay up 20 down 30
QTECH (config-track)# exit
```

Verification	Let the test result of RNS instance 7 change from successful to unsuccessful. ▪ When the test result changes to unsuccessful, immediately check the status of track object 7, and verify that the status is still UP. ▪ Check the status of the track object 30s later, and verify that the status changes to DOWN.

	```QTECH# show track 5```
	```Track 5```
	
	```Reliable Network Service 7 The state is Down```
	```2 change, current state last: 10 secs```
	
	```Delay up 20 secs, down 30 secs```

❖ Configuring Track Object 5 for Tracking the Test Results of an RNS List (consisting of RNS Instances 1, 2–5, and 8)

Configuration Steps	▪ **Configure and start an RNS test (see "RNS Configuration").** ▪ **Configure a track object for tracking the test result of an RNS list.** ▪ **Configure the delay for notifying the test result change from UP to DOWN, and the delay for notifying the test result change from DOWN to UP.**
	```QTECH(config)# track 5 rns-list 1,2-5,8 and QTECH (config-track)# delay up 20 down 30``` ```QTECH (config-track)# exit```
Verification	Let the test result of one of the RNS instances 1, 2-5, and 8 changes from successful to unsuccessful. ▪ When the test result changes to unsuccessful, immediately check the status of track object 7, and verify that the status is still UP. ▪ Check the status of the track object 30s later, and verify that the status changes to DOWN.

```
QTECH# show track 5 Track 5
rns-list 1,2-5,8 and The state is Down
2 change, current state last: 10 secs Delay up 20 secs, down 30 secs
```

Common Errors

- The track object for tracking an RNS test is configured, but the RNS test is not configured.

- The track object for tracking the link status of an interface is configured, but the corresponding interface is not configured.

- The track object for tracking the status of a track list, but no member of the RNS list is configured.

- The track object configured for tracking an RNS list, but the RNS test is not configured.

8.5   Monitoring

Displaying

Description	Command
Displays configurations of one or more RNS instances.	**show ip rns configuration** [*operation-number*]
Displays detailed statistics of one or more RNS instances.	**show ip rns collection-statistics** [*operation-number*]
Displays the current RNS status.	**show ip rns operational-state** [*operation-number*]
Displays the proactive threshold monitoring information of one or more RNS instances.	**show ip rns reaction-configuration** [*operation-number*]
Displays information about the test triggered by one or more RNS instances.	**show ip rns reaction-trigger** [*operation-number*]
Displays the brief statistics of one or	**show ip rns statistics** [*operation-number*]

more RNS instances.	
Displays the brief statistics of one or more track objects.	**show track** [*object-number*]

Debugging

System resources are occupied when debugging information is output. Therefore, disable debugging immediately after use.

Description	Command
Debugs the track module.	**debug track** { **all | proc-event | rdnd-event | client** }
Debugs the RNS module.	**debug rns** { **all | interface | lib | rdnd-event | restart | rns_id** [**0, 500**] **| server** }