

Reliability Configuration

Оглавление

1	CONFIGURING RLDP	6
1.1	Overview	6
1.2	Applications	6
1.2.1	Unidirectional Link Detection	6
1.2.2	Bidirectional Forwarding Detection	7
1.2.3	Downlink Loop Detection	7
1.3	Features	8
1.3.1	Deploying RLDP Detection	10
1.4	Configuration	11
1.4.1	Configuring Basic RLDP Functions	12
1.5	Monitoring	18
2	CONFIGURING DLDP	19
2.1	Overview	19
2.2	Applications	19
2.2.1	Intra-Network Segment DLDP Detection	19
2.2.2	Inter-Network Segment DLDP Detection	20
2.3	Features	20
2.3.1	DLDP Detection	22
2.3.2	MAC Address Binding	23
2.3.3	Passive DLDP Detection	23
2.4	Configuration	24
2.4.1	Enabling DLDP Detection	24
2.5	Monitoring	28
3	CONFIGURING VRRP	30
3.1	Overview	30
3.2	Applications	30
3.2.1	Routing Redundancy	30
3.2.2	Load Balancing	31
3.3	Features	33
3.3.1	VRRP	34
3.4	Configuration	39
3.4.1	Configuring IPv4 VRRP	41
3.4.2	Configuring IPv6 VRRP	55
3.4.3	Configuring VRRP-MSTP	67

3.5	Monitoring	82
4	CONFIGURING VRRP PLUS	84
4.1	Overview	84
4.2	Applications	84
4.2.1	Enabling Load Balancing Within a VRRP Group	84
4.3	Features	86
4.3.1	VRRP Plus	86
4.4	Configuration	90
4.4.1	Configure VRRP Plus	91
4.5	Monitoring	96
5	CONFIGURING BFD	98
5.1	Overview	98
5.2	Applications	98
5.2.1	BFD Support for OSPF	98
5.2.2	BFD Support for Static Routing	99
5.3	Features	100
5.3.1	BFD Session Establishment	103
5.3.2	BFD Session Detection	105
5.3.3	BFD Support for Applications	106
5.3.4	BFD Protection	109
5.3.5	BFD Flapping Dampening	110
5.4	Configuration	110
5.4.1	Configuring BFD Basic Functions	111
5.4.2	Configuring BFD Protection	118
5.4.3	Configuring BFD Flapping Dampening	119
5.5	Monitoring	121
6	CONFIGURING IP EVENT DAMPENING	123
6.1	Overview	123
6.2	Applications	123
6.2.1	Routed Port Flap Dampening	123
6.3	Features	124
6.3.1	Port Flap Suppression	125
6.4	Configuration	126
6.4.1	Enabling IP Event Dampening	126
6.5	Monitoring	128

7	CONFIGURING VSU	130
7.1	Overview	130
7.2	Applications	131
7.2.1	Managing Multiple Devices in a Unified Manner	131
7.2.2	Simplifying Networking Topology	132
7.3	Features	133
7.3.1	Virtual Switching Link (VSL)	136
7.3.2	Topology	137
7.3.3	Dual-Active Detection (DAD)	140
7.3.4	VSU Traffic Forwarding	142
7.3.5	System Management	144
7.4	Configuration	145
7.4.1	Configuring VSU in the Standalone Mode	147
7.4.2	Configuring VSU in the VSU Mode	156
7.4.2.1	Configuring VSU Attributes	156
7.4.2.2	Configuring the VSL	161
7.4.2.3	Configuring Dual-Active Detection	164
7.4.2.4	Configuring Traffic Balancing	171
7.4.2.5	Changing the VSU Mode to the Standalone Mode	173
7.5	Monitoring and Maintenance	175
8	CONFIGURING VSD	176
8.1	Overview	176
8.2	Applications	179
8.2.1	Providing Isolated Services within a Physical Service	179
8.3	Features	180
8.3.1	VSD	181
8.4	Configuration	182
8.4.1	Configuring a VSD	183
8.4.2	Restarting a VSD	187
8.4.3	VSD Switching	188
8.5	Monitoring	190
9	CONFIGURING NLB GROUP	191
9.1	Overview	191
9.2	Applications	191
9.2.1	Supporting Web Server NLB Group	191
9.3	Features	192
9.3.1	NLB Group	193

9.4	Configuration	194
9.4.1	Configuring NLB Group Attributes	194
9.4.2	Configuring the NLB Group Destination Port	195
9.5	Monitoring	197

1 CONFIGURING RLDP

1.1 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.

1.2 Applications

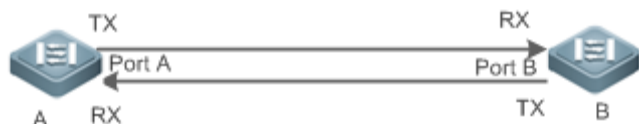
Application	Description
Unidirectional Link Detection	Detect a unidirectional link failure.
Bidirectional Forwarding Detection	Detect a bidirectional link failure.
Downlink Loop Detection	Detect a link loop.

1.2.1 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 1-1



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

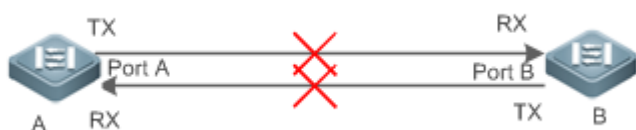
- ❖ Global RLDP is enabled.
- ❖ Configure unidirectional link detection under Port A and Port B and define a method for failure treatment.

1.2.2 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 1-2



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

Deployment

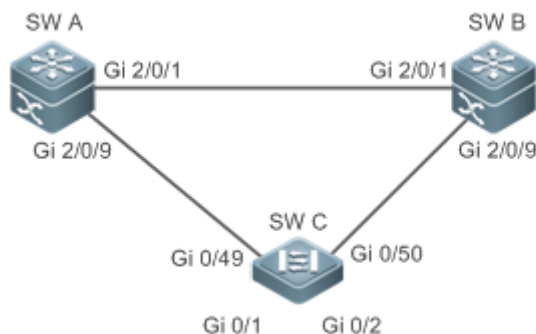
- ❖ Global RLDP is enabled.
- ❖ Configure BFD under Port A and Port B and define a method for failure treatment.

1.2.3 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 1-3



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.

1.3 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.

1. Configuring RLDP

- ❖ 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.

1.3.1 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.

1.4 Configuration

Configuration	Description and Command
Configuring Basic RLDP Functions	 (Mandatory) It is used to enable RLDP detection under global configuration mode.
	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.

1.4.1 Configuring Basic RLDP Functions

Configuration

Effect

- ❖ Enable RLDP unidirectional link detection, bidirectional forwarding detection, or downlink loop detection to discover 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 loop detection is configured on a newly-added port but not on the existing member ports, the new port clears loop detection and joins the AP. Third, 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 *SWITCH-INTF-SCG.doc*.

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.
- ❖ Specify 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

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

Enabling RLDP Detection on Interface

Command	<code>rldp port { unidirection-detect bidirection-detect loop-detect } { warning shutdown-svi shutdown-port block }</code>
Parameter Description	<p>unidirection-detect: Indicates unidirectional link detection.</p> <p>bidirection-detect: Indicates bidirectional forwarding detection.</p> <p>loop-detect: Indicates downlink loop detection.</p> <p>warning: Indicate the failure treatment is warning.</p> <p>shutdown-svi: Indicate the failure treatment is closing the SVI that the interface is on.</p> <p>shutdown-port: Indicates the failure treatment is port violation.</p> <p>block: Indicates the failure treatment is disabling learning and forwarding of a port.</p>
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	<code>rldp {detect-interval <i>interval</i> detect-max <i>num</i> neighbor-negotiation }</code>
Parameter Description	<p>detect-interval <i>interval</i>: Indicates a detection interval.</p> <p>detect-max <i>num</i>: Indicates detection times.</p> <p>neighbor-negotiation: Indicates neighbor negotiation.</p>
Command Mode	Global configuration mode
Usage Guide	Modify all RLDP parameters on all ports when necessary.

Recovering Failed Port

Command	<code>rldp reset</code>
---------	-------------------------

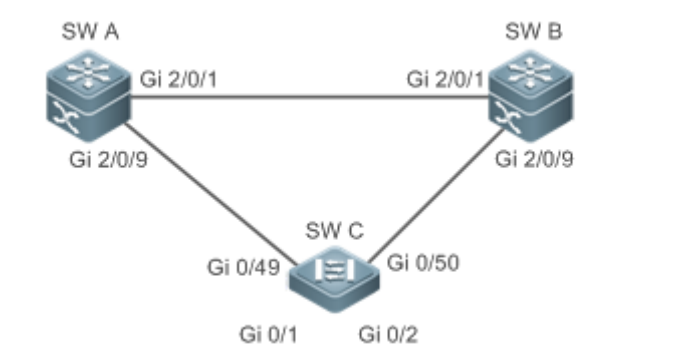
Parameter Description	N/A
Command Mode	Privileged mode
Usage Guide	Recover all failed ports to initialized state and resume detection.

Displaying RLDP State Information

Command	<code>show rldp [interface <i>interface-name</i>]</code>
Parameter Description	<i>interface-name</i> : 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

<p>Scenario Figure 1-4</p>	<p>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.</p> 
<p>Configurati on Steps</p>	<ul style="list-style-type: none"> ❖ 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

	<p>topology, and the STP is enabled on each of them. For STP configuration, refer to relevant configuration guide.</p> <ul style="list-style-type: none"> ❖ 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	<pre>A#configure terminal A(config)#rldp 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</pre>
B	<p>Apply the configuration on SW A.</p>
C	<pre>C#configure terminal C(config)#rldp 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</pre>
Verification	<ul style="list-style-type: none"> ❖ Check the RLDP information on SW A, SW B and SW C. Take SW A for example.

A	<pre>A#show rldp rldp state : enable rldp hello interval: 3 rldp max hello : 2 rldp local bridge : 08c6.b322.33aa ----- Interface GigabitEthernet 2/0/1 port state : normal neighbor bridge : 08c6.b300.51b1 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 : 08c6.b300.41b0 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</pre>
---	---

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.

1.5 Monitoring

Displaying

Description	Command
Displays RLDP state.	show rldp [interface <i>interface-name</i>]

2 CONFIGURING DLDP

2.1 Overview

The Data Link Detection Protocol (DLDP) is a protocol used to quickly detect faulty Ethernet links.

A typical Ethernet link detection mechanism detects physical link connectivity through autonegotiation at the physical layer. Such a mechanism has limitations when detecting Layer-3 data communication exceptions despite normal physical connections.

DLDP provides reliable Layer-3 link detection information. After detecting a faulty link, DLDP shuts down the logical state of Layer-3 ports to realize fast Layer-3 protocol convergence.

2.2 Applications

Application	Description
Intra-Network Segment DLDP Detection	The source IP address of the detected port and the detected IP address are in the same network segment.
Inter-Network Segment DLDP Detection	The source IP address of the detected port and the detected IP address are in different network segments.

2.2.1 Intra-Network Segment DLDP Detection

Scenario

This section describes the basic DLDP application scenario where the source IP address of the detected port and the detected IP address are in the same network segment.

In Figure 2-1, the Gi 0/1 Layer-3 port on Switch A and the Gi 0/2 Layer-3 port on Switch C are in the same network segment. To detect the Layer-3 link connectivity from Gi 0/1 to Gi 0/2, enable DLDP on Gi 0/1 or Gi 0/2.

Figure 2-1



Remarks	Device A and Device C are switches. Gi 0/1 and Gi 0/2 are Layer-3 ports in the same network segment. B is a network in the same network segment as Gi 0/1 and Gi 0/2.
----------------	---

Deployment

- ❖ Enable DLDP on Gi 0/1 or Gi 0/2.

2.2.2 Inter-Network Segment DLDP Detection

Scenario

This section describes the DLDP application scenario where the source IP address of the detected port and the detected IP address are in different network segments.

In Figure 2-2, the Gi 0/1 Layer-3 port on Switch A and the Gi 0/4 Layer-3 port on Switch D are in different network segments. To detect the Layer-3 link connectivity from Gi 0/1 to Gi 0/4, enable DLDP on Gi 0/1 and configure the DLDP next-hop IP address (IP address of the Gi 0/2 port on Switch B).

Figure 2-2



Remarks	Device A, Device B, and Device D are switches. Gi 0/1 and Gi 0/4 are Layer-3 ports in different network segments.
----------------	--

Deployment

- ❖ Enable DLDP on Gi 0/1 and configure the DLDP next-hop IP address.

2.3 Features

Basic Concepts

DLDP Detection Interval and Retransmission Times

Detection interval: Indicates the interval at which DLDP detection packets (ICMP echo) are transmitted.

Retransmission times: Indicate the maximum times DLDP detection packets can be retransmitted in the case of a DLDP detection failure.

When a network device does not receive a reply packet from the peer end within the period of the detection interval multiplied by the retransmission times, the device determines that a Layer-3 link failure occurs and shuts down the logical state of its Layer-3 port (despite the normal physical link connection). When Layer-3 link connectivity is recovered, the device restores its Layer-3 port to Up logical state.

DLDP Detection Modes

Active mode and passive mode are two DLDP detection modes.

Active mode (default): ICMP detection packets are sent actively.

Passive mode: ICMP detection packets are received passively.

DLDP Next Hop

Next hop: Indicates the next node connected to the detected IP address in inter-network segment DLDP detection.

In some cases, DLDP needs to detect IP reachability in non-directly connected network segments. You need to configure the next-hop IP address for the detected port to allow DLDP to obtain the next-hop MAC address through an ARP packet before sending a correct ICMP packet.

In this situation, you need to avoid the return of the reply packet from another link; otherwise, DLDP will misjudge that the detected port does not receive an ICMP reply.

DLDP Recovery Times

Recovery times: Indicate the times DLDP needs to receive consecutive reply packets (ICMP reply) before it can determine link failure recovery.

In some cases, link detection may be unstable. For example, a link is only intermittently pingable. In this case, DLDP repeatedly changes the link status between Up and Down, which may further destabilize the ring network.

Recovery times indicate the times DLDP needs to receive consecutive reply packets before DLDP can set the link in Down state to Up. The default recovery times are three times, indicating that the link needs to be successfully pinged three times before it is set to Up. The recovery times setting reduces link detection sensitivity but increases stability. Related parameters are adjustable according to the network condition.

DLDP Bound MAC Address

Bound MAC address: Indicates the MAC address bound to the detected IP address.

In a complex network environment, DLDP may obtain an invalid MAC address if the detected link has abnormal ARP packets transmitted (causing ARP spoofing), which will make DLDP detection abnormal.

To address this problem, you can bind the detected IP address (or next-hop IP address) to a static MAC address to avoid a DLDP failure in the case of ARP spoofing.

Overview

Feature	Description
DLDP Detection	Detects Layer-3 link connectivity. When a Layer-3 link is abnormal, DLDP shuts down the Layer-3 port.
MAC Address Binding	Binds the detected IP address to the MAC address of the detected device to avoid DLDP exceptions otherwise caused by ARP spoofing.
Passive DLDP Detection	When both ends of the detected link are enabled with DLDP, you can configure one end in passive mode to save bandwidth and CPU resources.

2.3.1 DLDP Detection

DLDP detects Layer-3 link connectivity. When a Layer-3 link is abnormal, DLDP shuts down the corresponding Layer-3 port.

Working Principle

After DLDP detection is enabled, DLDP sends an ARP packet to obtain the MAC address and outbound port of the detected device or the next-hop device. Then DLDP periodically sends IPv4 ICMP echo packets to the MAC address and outbound port to detect link connectivity. If DLDP does not receive an IPv4 ICMP reply packet from the detected device within a specific period, DLDP determines that the link is abnormal and sets the Layer-3 port to Down.

Related Configuration

❖ Enabling DLDP Detection

By default, DLDP detection is disabled on ports.

Run the **lldp** command with the detected IP address specified to enable DLDP detection.

You can configure the next-hop IP address, MAC address of the detected device, transmission interval, retransmission times, and recovery times based on the actual environment.

2.3.2 MAC Address Binding

The MAC address binding feature is used to bind the detected IP address (or next-hop IP address) to the MAC address of the detected device (or next-hop device) to avoid DLDP exceptions otherwise caused by ARP spoofing

Working Principle

You can bind the detected IP address (or next-hop IP address) to a static MAC address to avoid a DLDP failure in the case of ARP spoofing.

Related Configuration

By default, no MAC address is bound in DLDP detection.

Bind the MAC address of the detected device when you run the **lldp** command to enable DLDP detection. If the next-hop IP address is specified, bind the MAC address of the next-hop device.

After DLDP detection is enabled, DLDP sends ARP packets and ICMP packets with a fixed destination IP address and a fixed destination MAC address. If the source IP address and MAC address in the received packet do not match the bound IP address and MAC address, DLDP will not process the packet.

2.3.3 Passive DLDP Detection

When both ends of the detected link are enabled with DLDP, you can configure one end in passive mode to save bandwidth and CPU resources.

Working Principle

After the device at the local end sends an ICMP echo packet, the peer device determines link connectivity according to the packet reception time by using specific detection parameters, which are the same as those at the local end, thus saving bandwidth and CPU resources.




Related Configuration

By default, passive DLDP detection is disabled.

Run the **lldp passive** command to enable passive DLDP detection.

After passive DLDP detection is enabled, DLDP will return an ICMP reply packet upon receiving an ICMP echo packet, instead of actively sending ICMP echo packets to the peer end. If DLDP does not receive an ICMP echo packet within a specific period, it determines that the link to the peer port is abnormal.

2.4 Configuration

Configuration	Description and Command			
Enabling DLDP Detection	 (Mandatory) It is used to enable DLDP detection in interface configuration mode.			
	<table border="1"> <tr> <td>lldp</td> <td>Enables DLDP detection.</td> </tr> </table>	lldp	Enables DLDP detection.	
	lldp	Enables DLDP detection.		
	 (Mandatory) It is used to enable passive DLDP detection in interface configuration mode.			
	<table border="1"> <tr> <td>lldp passive</td> <td>Enables passive DLDP detection.</td> </tr> </table>	lldp passive	Enables passive DLDP detection.	
	lldp passive	Enables passive DLDP detection.		
 (Optional) It is used to configure the detection interval, retransmission times, and recovery times of DLDP detection in global configuration mode.				
<table border="1"> <tr> <td>lldp interval</td> <td rowspan="3">Modifies the DLDP parameters globally to apply the modifications to DLDP detection on all ports.</td> </tr> <tr> <td>lldp retry</td> </tr> <tr> <td>lldp resume</td> </tr> </table>	lldp interval	Modifies the DLDP parameters globally to apply the modifications to DLDP detection on all ports.	lldp retry	lldp resume
lldp interval	Modifies the DLDP parameters globally to apply the modifications to DLDP detection on all ports.			
lldp retry				
lldp resume				

2.4.1 Enabling DLDP Detection

Configuration Effect

- ❖ Detect Layer-3 link connectivity. When a Layer-3 link is abnormal, DLDP shuts down the Layer-3 port.

Notes

- ❖ DLDP supports the configuration of multiple IP addresses on a Layer-3 port. DLDP sets the port to Down when none of the IP addresses receives an ICMP reply. If one IP address resumes communication, DLDP sets the port to Up again.
- ❖ DLDP uses the first IP address of the Layer-3 port as the source IP address of detection packets.

Configuration Steps

Enabling DLDP Detection

- ❖ Mandatory.
- ❖ When you enable DLDP detection in interface configuration mode, you can configure the next-hop IP address, MAC address, transmission interval, retransmission times, and recovery times based on the actual environment.

Configuring a DLDP Detection Mode

- ❖ Optional.
- ❖ You can configure active or passive DLDP detection in interface configuration mode based on the actual environment.
- ❖ If DLDP detection needs to be enabled at both ends of a Layer-3 link, you can configure passive DLDP detection at one end to save bandwidth and CPU resources.

Configuring DLDP Parameters Globally

- ❖ Optional.
- ❖ You can modify the parameters of DLDP detection on all ports in global configuration mode based on requirements. The parameters include the packet transmission interval, packet retransmission times, and recovery times.

Verification

- ❖ Display the device DLDP information, including the status and statistics of DLDP detection on all ports.

Related Commands

Enabling DLDP Detection

Command	<code>dldp ip-address [next-hop-ip] [mac-address mac-addr] [interval tick] [retry retry-num] [resume resume-num]</code>
Parameter Description	<p><i>ip-address</i>: Indicates the detected IP address.</p> <p><i>next-hop-ip</i>: Indicates the next-hop IP address.</p> <p><i>mac-addr</i>: Indicates the MAC address of the detected device to be bound. If the next-hop IP address is specified, bind the MAC address of the next-hop device.</p> <p><i>tick</i>: Indicates the interval at which detection packets are transmitted. The value ranges from 5 to 6,000 ticks (1 tick = 10 ms). The default value is 100 ticks (1s).</p> <p><i>retry-num</i>: The value ranges from 1 to 3,600. The default value is 4.</p> <p><i>resume-num</i>: Indicates the recovery times. The value ranges from 1 to 200. The default value is 3.</p>
Command Mode	Interface configuration mode
Usage Guide	The port to be enabled with DLDP detection must be a Layer-3 port, such as a router port, L3AP port, and SVI port.

Configuring a DLDP Detection Mode

Command	<code>dldp passive</code>
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	You need to enable DLDP detection before configuring a DLDP detection mode.

Modifying DLDP Detection Parameters Globally

Command	<code>dldp { interval tick retry retry-num resume resume-num }</code>
Parameter Description	<p><i>tick</i>: Indicates the interval at which detection packets are transmitted. The value ranges from 5 to 6,000 ticks (1 tick = 10 ms). The default value is 100 ticks (1s).</p> <p><i>retry-num</i>: Indicates the interval at which detection packets are retransmitted. The value ranges from 5 to 3,600. The default value is 4.</p>

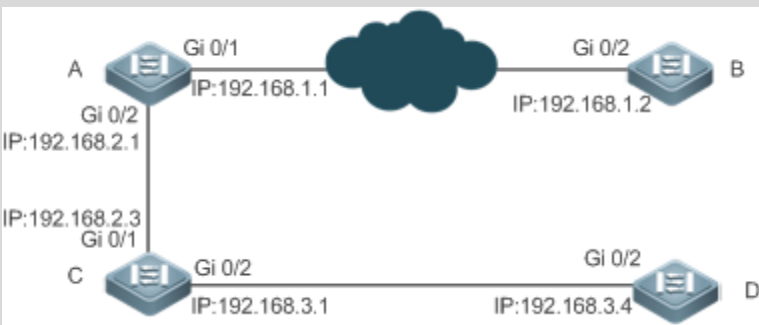
	<i>resume-num</i> : Indicates the recovery times. The value ranges from 1 to 200. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	Use this command to quickly modify the parameters of DLDP detection on all ports when the actual environment is changed.

Displaying the DLDP Status

Command	show dldp statistic [interface <i>interface-name</i>]
Parameter Description	<i>interface-name</i> : Indicates the Layer-3 port on which the DLDP status will be displayed.
Command Mode	Privileged mode, global configuration mode, and interface configuration mode
Usage Guide	Use this command to display the DLDP status on a specific port. You can also use this command to display the DLDP status on all ports.

Configuration Example

Enabling DLDP Detection on Layer-3 Ports on Device A and Device B in a Layer-3 Network

Scenario Figure 2-3	
Verification	<ul style="list-style-type: none"> ❖ Enable DLDP detection on the Gi 0/1 and Gi 0/2 router ports on Device A to detect the Layer-3 link connectivity between Device A and Device B and that between Device A and Device D. ❖ To control the Gi 0/2 router port of Device B, enable passive DLDP detection on the port.
A	<pre>A#configure terminal A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#dldp 192.168.1.2</pre>

	<pre>A(config-if-GigabitEthernet 0/1)# exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/1)#lldp 192.168.3.4 192.168.2.3</pre>
B	<pre>B#configure terminal B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/1)#lldp 192.168.1.1 B(config-if-GigabitEthernet 0/1)#lldp passive</pre>
Verification	❖ Display the DLDP status on Device A and Device B to check whether DLDP detection is enabled and works normally.
A	<pre>A# show lldp Interface Type Ip Next-hop Interval Retry Resume State ----- Gi0/1 Active 192.168.1.2 100 4 3 Up Gi0/1 Active 192.168.3.4 192.168.2.3 100 4 3 Up</pre>
B	<pre>B# show lldp Interface Type Ip Next-hop Interval Retry Resume State ----- Gi0/2 Passive 192.168.1.1 100 4 3 Up</pre>

Common Errors

- ❖ An unreachable IPv4 unicast route is misjudged as a DLDP detection failure.
- ❖ DLDP detection fails because the peer device does not support ARP/ICMP replies.
- ❖ No next-hop IP address is configured in inter-network segment DLDP detection.

2.5 Monitoring

Clearing

Description	Command
Clears DLDP statistics.	<code>clear lldp [interface <i>interface-name</i> [<i>ip-address</i>]]</code>

Displaying

Description	Command
Displays the DLDP status.	<code>show lldp [interface <i>interface-name</i>]</code>

Displays the DLDP statistics on the Up/Down port sates.

```
show dldp statistic
```

3 CONFIGURING VRRP

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

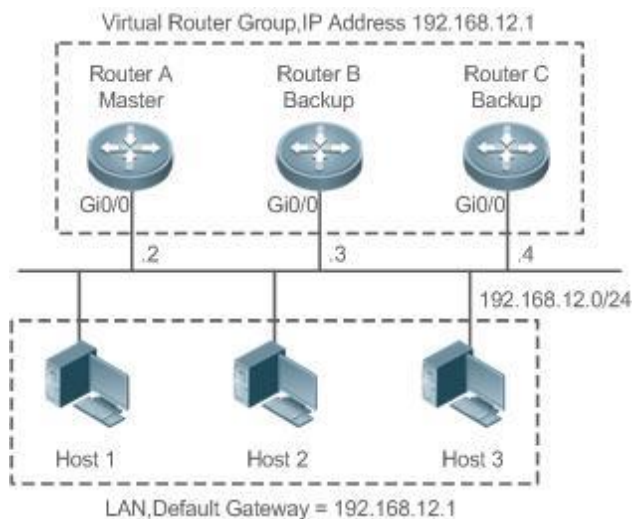
Scenario

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 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

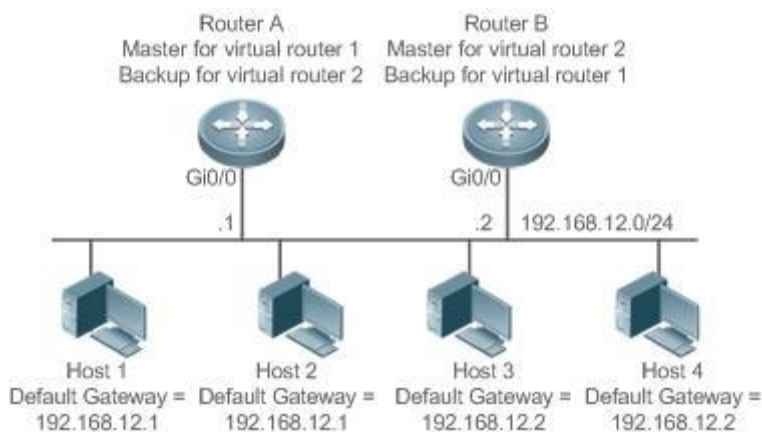
Scenario

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 (including IPv6) 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

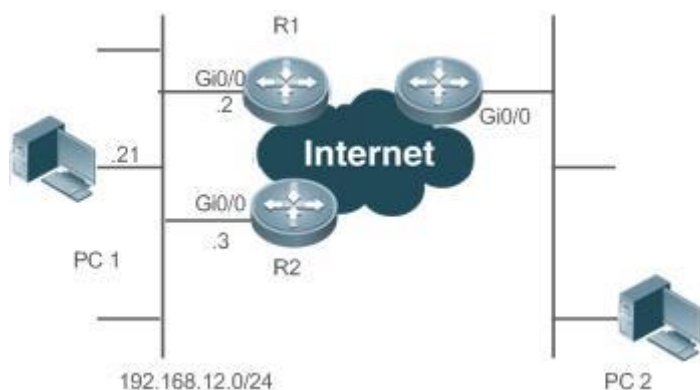
Feature	Description
VRRP	VRRP achieves redundancy for the default gateways of terminals on a multi-access media (for example, Ethernet). It enables a Backup router to forward packets when the Master router is down, providing transparent routing switch and promoting network service quality.

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.

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 Master 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-address* } [*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.

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. If VRRP and VRRP Plus are enabled simultaneously on a Super VLAN interface, sending VRRP packets to the first Up Sub VLANs under the Super VLAN is not supported.

Both the above configurations reduce VRRP packets and avoids 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.

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.
	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-address } [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	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.
	⚠ (Optional) It is used to configure IPv6 VRRP parameters.	
	vrrp ipv6 group timers advertise { advertise-interval csec centisecond-interval }	Configures the IPv6 advertisement interval.
	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.

	<code>vrrp ipv6 group track interface-type interface-number [interface-priority]</code>	Configures the IPv6 VRRP tracked interface.
	<code>vrrp ipv6 group track { ipv6-global-address { ipv6-linklocal-address interface-type interface-number } } [interval interval-value] [timeout timeout-value] [retry retry-value] [priority]</code>	Configures the IPv6 VRRP tracked IP address.
	<code>vrrp ipv6 group timers learn</code>	Configures the IPv6 VRRP learning timer.
	<code>vrrp ipv6 group description text</code>	Configures the IPv6 VRRP group description.
	<code>vrrp delay { minimum min-seconds reload reload-seconds }</code>	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.

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 <i>ipaddress</i> [<i>secondary</i>]
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group, the range of which varies with product models. <i>ipaddress</i> : 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 <i>string</i>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>string</i> : 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	<code>vrp group timers advertise { advertise-interval csec centisecond-interval }</code>
Parameter Description	<p><i>group</i>: Indicates the VRID of a VRRP group.</p> <p><i>advertise-interval</i>: Indicates the advertisement interval of a VRRP group (unit: second).</p> <p><i>csec centisecond-interval</i>: 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.</p>
Command Mode	Interface configuration mode
Usage Guide	<p>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.</p> <p>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.</p>

Configuring the IPv4 VRRP Preemption Mode

Command	<code>vrp group preempt [delay seconds]</code>
Parameter Description	<p><i>group</i>: Indicates the VRID of a VRRP group.</p> <p>delay seconds: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.</p>
Command Mode	Interface configuration mode
Usage Guide	<p>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</p>

	case the group has the highest priority and automatically becomes the Master in the group.
--	--

Configuring the IPv4 VRRP Router Priority

Command	<i>vrrp group priority level</i>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>level</i> : 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	<i>vrrp group track { interface-type interface-number bfd interface-type interface-number ipv4-address } [priority]</i>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>interface-type interface-number</i> : Indicates the interface to be tracked. <i>bfd interface-type interface-number ipv4-address</i> : A specified adjacent IP address tracked through BFD. <i>priority</i> : 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	<i>vrrp group track ipv4-address [interval interval-value] [timeout timeout-value] [retry retry-value] [priority]</i>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>ipv4-address</i> : Indicates the IPv4 address to be tracked. <i>interval interval-value</i> : Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. <i>timeout timeout-value</i> : Indicates the probe timeout of waiting for responses. If no response is received when the timeout is up, it is regarded that the

	<p>destination is inaccessible. The unit is second. Unless configured manually, the value is 1 second by default.</p> <p>retry <i>retry-value</i>: Indicates the probe retries. If the probe packet is sent continually for <i>retry-value</i> 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.</p> <p><i>priority</i>: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.</p>
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 <i>group</i> timers learn
Parameter Description	<i>group</i> : 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 <i>group</i> description <i>text</i>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>text</i> : Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups.

Configuring the IPv4 VRRP Delay

Command	vrrp delay { minimum <i>min-seconds</i> reload <i>reload-seconds</i> }
---------	---

Parameter Description	minimum <i>min-seconds</i> : Indicates the VRRP delay after an interface state changes. reload <i>reload-seconds</i> : 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
Parameter Description	first-subvlan : Sends IPv4 VRRP packets only to the first UP Sub VLAN interface in a Super 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 two methods. Packets are sent to the first UP 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, sending VRRP packets to the first Up interfaces of the Sub VLANs under the Super VLAN is not supported.

	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

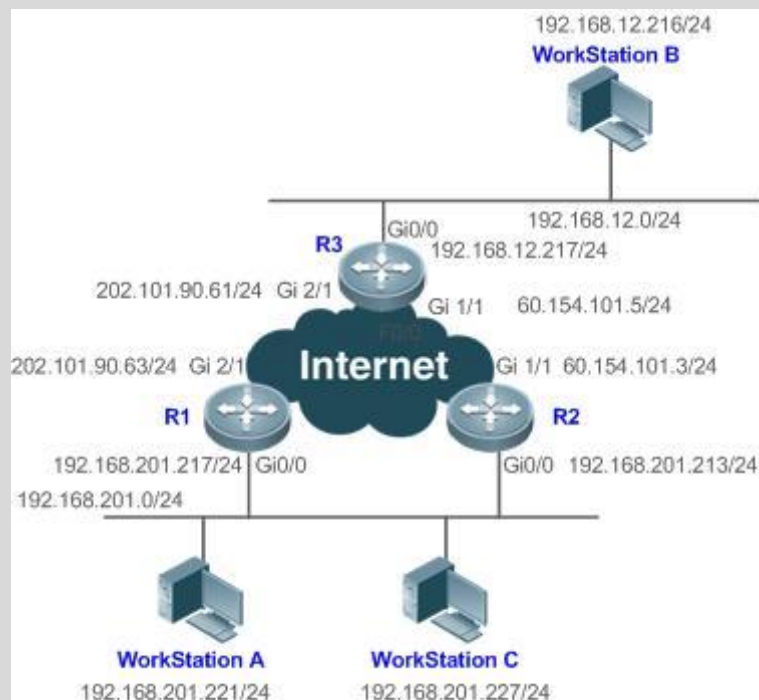
Command	<i>vrrp group bfd ip-address</i>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>ip-address</i> : Indicates the interface IP address.
Command Mode	Interface configuration mode
Usage Guide	For a Backup router, run this command to correlate an IPv4 VRRP group with BFD 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	<i>vrrp bfd interface-type interface-number ip-address</i>
Parameter Description	<i>interface-type interface-number</i> : Indicates interface type and ID. <i>ip-address</i> : 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 3-4Configurati
on 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
```

	<pre>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</pre>
R1	<pre>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</pre>
R2	<pre>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</pre>
Verification	<p>Run the show vrrp command to verify the configuration.</p> <ul style="list-style-type: none"> ❖ 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	<pre> 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 VRRP standard version is V3 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 </pre>
R2	<pre> 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 VRRP standard version is V3 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 </pre>

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

<p>Scenario Figure 3-5</p>	<p>The diagram illustrates a network topology with three routers (R1, R2, R3) and three workstations (A, B, C). R1 and R2 are connected to a local network (192.168.201.0/24) and serve as Virtual Gateways 1 and 2 respectively. R3 is connected to another local network (192.168.12.0/24). All routers are connected to an Internet cloud. The diagram shows various IP addresses and interface configurations for each router and workstation.</p>
<p>Configurati on Steps</p>	<ul style="list-style-type: none"> ❖ 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.
<p>R3</p>	<p>R3#configure terminal</p>

	<pre> 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 </pre>
R1	<pre> 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 </pre>
R2	<pre> 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 </pre>

	<pre>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</pre>
Verification	<p>Run the show vrrp command to verify the configuration.</p> <ul style="list-style-type: none"> ❖ 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	<pre>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</pre>

	<pre>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</pre>
R2	<pre>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</pre>

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

- ❖ 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.

Configures the IPv6 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 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 vrrp` command to verify the configuration.

Related Commands

Enabling IPv6 VRRP

Command	<code>vrrp group ipv6 ipv6-address</code>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group, the range of which varies with product models. <i>ipv6-address</i> : 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	<code>vrrp ipv6 group timers advertise { advertise-interval csec centisecond-interval }</code>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>advertise-interval</i> : Indicates the advertisement interval of a VRRP group (unit: second). <i>csec centisecond-interval</i> : 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	<p>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.</p> <p>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.</p>
-------------	--

Configuring the Preemption Mode

Command	<code>vrrp ipv6 group preempt [delay seconds]</code>
Parameter Description	<p><i>group</i>: Indicates the VRID of a VRRP group.</p> <p>delay seconds: Indicates the preemption delay for the Master router to claim its status. The default value is 0 second.</p>
Command Mode	Interface configuration mode
Usage Guide	<p>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.</p>

Enabling the Accept Mode for an IPv6 VRRP Group

Command	<code>vrrp ipv6 group accept_mode</code>
Parameter Description	<p><i>group</i>: Indicates the VRID of a VRRP group.</p>
Command Mode	Interface configuration mode
Usage Guide	<p>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.</p>

Configuring the IPv6 VRRP Router Priority

Command	<code>vrrp ipv6 group priority level</code>
---------	--

Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>level</i> : 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 <i>group</i> track <i>interface-type interface-number</i> [<i>priority</i>]
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>interface-type interface-number</i> : Indicates the interface to be tracked. <i>priority</i> : 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 <i>group</i> track { <i>ipv6-global-address</i> <i>ipv6-linklocal-address interface-type interface-number</i> } [<i>interval interval-value</i>] [<i>timeout timeout-value</i>] [<i>retry retry-value</i>] [<i>priority</i>]
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>ipv6-global-address</i> : Indicates the IPv6 global unicast address. <i>ipv6-linklocal-address</i> : Indicates the IPv6 link-local address. <i>interface-type interface-number</i> : Indicates the interface to be tracked. <i>interval interval-value</i> : Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default. <i>timeout timeout-value</i> : 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. <i>retry retry-value</i> : Indicates the probe retries. If the probe packet is sent continually for <i>retry-value</i> 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. <i>priority</i> : 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 <i>group</i> timers learn
Parameter Description	<i>group</i> : 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 <i>group</i> description <i>text</i>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>text</i> : Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups.

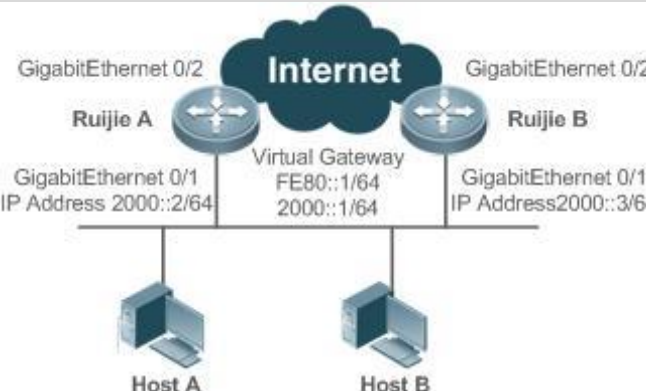
Configuring the IPv4 VRRP Delay

Command	vrrp delay { minimum <i>min-seconds</i> reload <i>reload-seconds</i> }
Parameter Description	minimum <i>min-seconds</i> : Indicates the VRRP delay after an interface state changes. reload <i>reload-seconds</i> : 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

<p>Scenario Figure 3-6</p>	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ❖ 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.
<p>QTECH A</p>	<pre> 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 </pre>

QTECH B	<pre> 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 </pre>
Verification	<p>Run the show vrrp command to verify the configuration.</p> <ul style="list-style-type: none"> ❖ 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.
QTECH A	<pre> 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 </pre>
QTECH B	<pre> QTECHB#show ipv6 vrrp 1 GigabitEthernet 0/1 - Group 1 State is Backup Virtual IPv6 address is as follow: FE80::1 </pre>

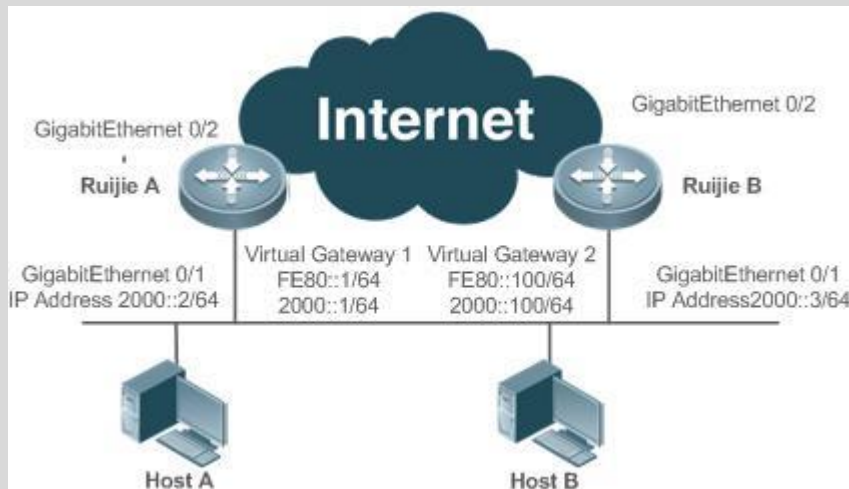
```

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
    
```

Configuration Example

Multiple VRRP Backup Groups (under IPv6)

Scenario
Figure 3-7



Configurati
on 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.

QTECH A

```

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
    
```


	<pre> 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 </pre>
QTECH B	<pre> 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 </pre>
Verification	Run the show vrrp command to verify the configuration.
QTECH A	<pre> 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 20 Master Router is FE80::1234 (local), priority is 120 Master Advertisement interval is 3 sec </pre>

	<pre> 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 </pre>
<p>QTECH B</p>	<pre> 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 </pre>

```
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
```

3.4.3 Configuring VRRP-MSTP

Configuration Effect

- ❖ Link-level and gateway-level backup are achieved and network robustness is improved greatly when MSTP 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.

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 interval 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 <i>ipaddress</i> [secondary]
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group, the range of which varies with product models. <i>ipaddress</i> : 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	<i>vrpp group authentication string</i>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>string</i> : 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	<i>vrpp group timers advertise { advertise-interval csec centisecond-interval }</i>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>advertise-interval</i> : Indicates the advertisement interval of a VRRP group (unit: second). <i>csec centisecond-interval</i> : 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	<code>vrrp group preempt [delay seconds]</code>
Parameter Description	<i>group</i> : 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	<code>vrrp group priority level</code>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>level</i> : 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	<code>vrrp group track { interface-type interface-number bfd interface-type interface-number ipv4-address } [priority]</code>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>interface-type interface-number</i> : Indicates the interface to be tracked. bfd interface-type interface-number ipv4-address : A specified adjacent IP address tracked through BFD. <i>priority</i> : 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	<code>vrrp group track ipv4-address [interval interval-value] [timeout timeout-value] [retry retry-value] [priority]</code>
Parameter Description	<p><i>group</i>: Indicates the VRID of a VRRP group.</p> <p><i>ipv4-address</i>: Indicates the IPv4 address to be tracked.</p> <p><i>interval interval-value</i>: Indicates the probe interval. The unit is second. Unless configured manually, the value is 3 seconds by default.</p> <p><i>timeout timeout-value</i>: 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.</p> <p><i>retry retry-value</i>: 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.</p> <p><i>priority</i>: Indicates the scale of VRRP priority change when the state of a monitored interface changes. The default value is 10.</p>
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	<code>vrrp group timers learn</code>
Parameter Description	<i>group</i> : 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	<code>vrrp group description text</code>
Parameter Description	<i>group</i> : Indicates the VRID of a VRRP group. <i>text</i> : Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	A VRRP description helps distinguishing VRRP groups.

Configuring the IPv4 VRRP Delay

Command	<code>vrrp delay { minimum <i>min-seconds</i> reload <i>reload-seconds</i> }</code>
Parameter Description	minimum <i>min-seconds</i> : Indicates the VRRP delay after an interface state changes. reload <i>reload-seconds</i> : 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	<code>vrrp group version { 2 3 }</code>
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	<code>vrrp detection-vlan first-subvlan</code>
----------------	---

Parameter Description	first-subvlan: Sends IPv4 VRRP packets only to the first UP Sub VLAN interface in a Super 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 two methods. Packets are sent to the first UP 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, sending VRRP packets to the first UP Sub VLAN interfaces of the Super VLAN interface is not supported. 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	<i>vrrp group bfd ip-address</i>
Parameter Description	<i>group:</i> Indicates the VRID of a VRRP group. <i>ip-address:</i> 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

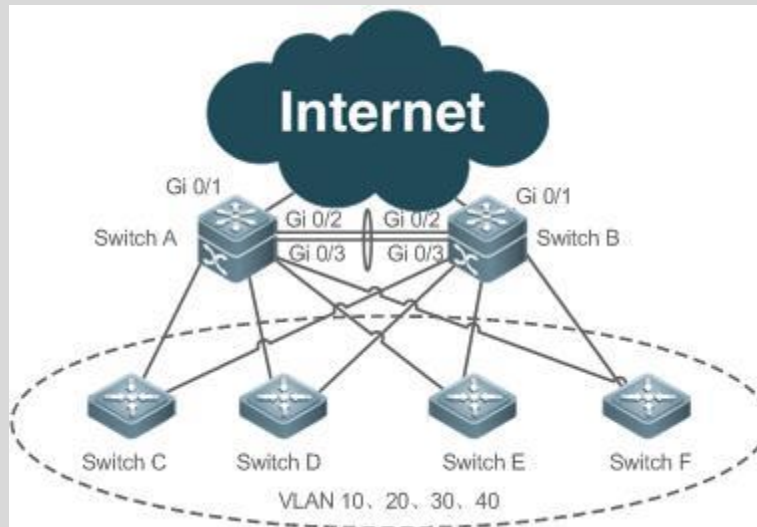
Command	<i>vrrp bfd interface-type interface-number ip-address</i>
Parameter Description	<i>interface-type interface-number:</i> Indicates interface type and ID. <i>ip-address:</i> Indicates the interface IP address.
Command Mode	Global configuration mode
Usage Guide	If global IPv4 VRRP BFD is configured, 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.

Switch A

```
//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 as 10.10.1.1/24.
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
```

	<pre>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</pre>
Switch B	<pre>//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</pre>

	<pre> 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 </pre>
Verification	
Switch A	<pre> Check the configuration. SwitchA#show running-config ! vlan 10 </pre>

```
!  
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
```

```
//Check VRRP status.
SwitchB#show vrrp brief
Interface Grp Pri timer Own Pre State Master addr Group addr
VLAN 10 10 100 3 - P Backup 192.168.10.2 192.168.10.1
VLAN 20 20 100 3 - P Backup 192.168.20.2 192.168.20.1
VLAN 30 30 120 3 - P Master 192.168.30.3 192.168.30.1
VLAN 40 40 120 3 - P Master 192.168.40.3 192.168.40.1
//Disconnect the uplink of Switch B, and check 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
```

3.5 Monitoring

Displaying

Description	Command
Displays the brief or detailed information of IPv4/IPv6 VRRP.	show [ipv6] vrrp [brief group]
Displays the information of an IPv4/IPv6 VRRP group on a specified interface.	show [ipv6] vrrp interface <i>type number</i> [brief]
Displays the statistics of VRRP packets.	show vrrp packet statistics [<i>interface-type interface-number</i>]

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 <i>acl-id</i> [icmp protocol] interface <i>type number</i> [<i>group</i>]] debug ipv6 vrrp packets [acl <i>acl-name</i> [icmp protocol] interface <i>type number</i> [<i>group</i>]]
Debugs VRRP status.	debug [ipv6] vrrp state

4 CONFIGURING VRRP PLUS

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

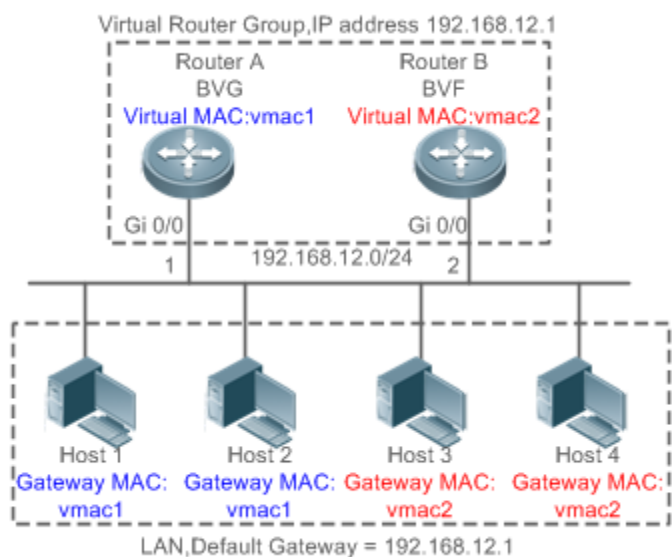
Scenario

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



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.

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 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 addresses of different VRRP groups.

Basic Principles

Hosts in a LAN use the unified gateway IPv4 address (that is, virtual IP address of the VRRP group). When different hosts request the gateway ARP, 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 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 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 requests sent by hosts.
- ❖ Weighted policy: The ARP 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 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.

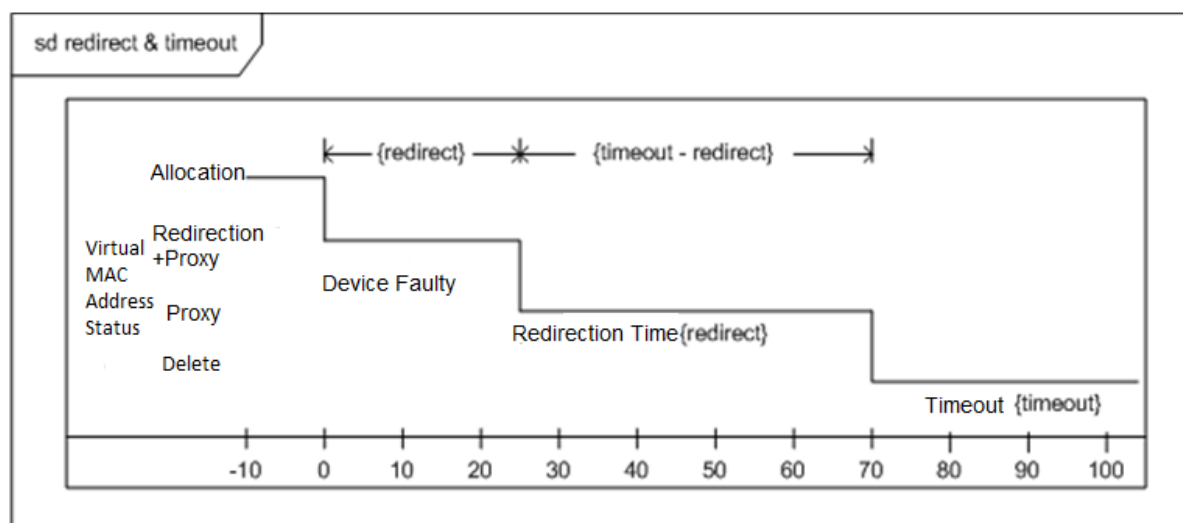
Redirection Time and Timeout of the Proxy Virtual MAC Address

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 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 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

4. Configuring VRRP Plus

1. After VRRP Plus is configured, the ARP 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 learned by hosts. Load balancing is implemented only after the gateway ARP 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 module will broadcast gratuitous ARP packets of this address. If a conflict of the VRRP Plus virtual address occurs, sending gratuitous ARP 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.
	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

- ❖ 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 [ipv6]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	<i>vrrp group balance</i>
Parameter Description	<i>group</i> : Indicates the ID of the VRRP group. The value range of the group ID varies according to the product 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	<i>vrrp group load-balancing{host-dependent round-robin weighted }</i>
Parameter Description	<i>group</i> : 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	<i>vrrp group timers redirect redirect timeout</i>
Parameter Description	<i>group</i> : Indicates the ID of the VRRP group. <i>redirect</i> : Indicates the redirection time. The value ranges from 0 to 3,600s. The default value is 300s, that is, 5 minutes. <i>timeout</i> : 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 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 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	<code>vrrp group weighting <i>maximum</i> [<i>lower lower</i>] [<i>upper upper</i>]</code>
Parameter Description	<i>maximum</i> : Indicates the weight of the backup group. The value ranges from 2 to 254. The default value is 100. <i>lower lower</i> : Indicates the lower threshold of the backup group. The value ranges from 1 to (maximum - 1). The default value is 1. <i>upper upper</i> : 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	<code>vrrp group forwarder preempt</code>
Parameter Description	<i>group</i> : 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

<p>Scenario Figure 4-3</p>	<p>The diagram illustrates a VRRP Plus configuration. Two routers, Router A (BVG) and Router B (BVF), are connected to the Internet via their Gi 0/14 interfaces. They are also connected to a LAN via their Gi 0/0 interfaces. Router A has a virtual MAC of vmac1 and Router B has a virtual MAC of vmac2. The LAN has a default gateway of 192.168.12.1. Four hosts (Host 1 to Host 4) are connected to the LAN. Host 1 and Host 2 have a gateway MAC of vmac1, while Host 3 and Host 4 have a gateway MAC of vmac2.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ❖ 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.
<p>Router A</p>	<pre> 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 </pre>
<p>Router B</p>	<pre> QTECHB#config </pre>

	<pre> 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 </pre>
Verification	<p>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.</p>
Router A	<pre> 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 08c6.b322.33a3 Preemption enabled </pre>
Router B	<pre> 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 </pre>

	Owner ID is 0000.0001.0006 Preemption disabled (BVG cannot be preempted) Forwarder 2 (local) MAC address: 001a.a916.0201 Owner ID is 08c6.b322.33a3 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
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 CONFIGURING BFD

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-v4v6-1hop-09: BFD for IPv4 and IPv6 (Single Hop)
- ❖ draft-ietf-bfd-mpls-07: BFD For MPLS LSPs

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.

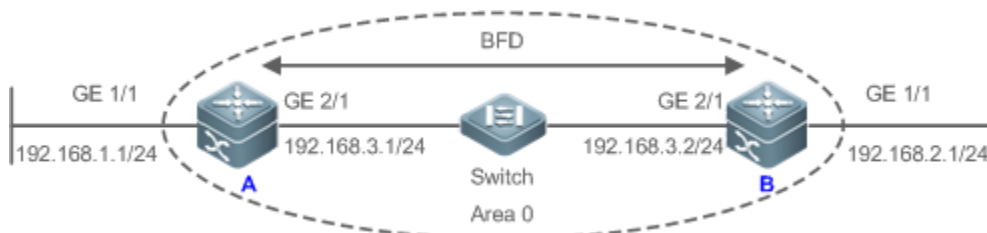
5.2.1 BFD Support for OSPF

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, OSPF 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 Static Routing

Scenario

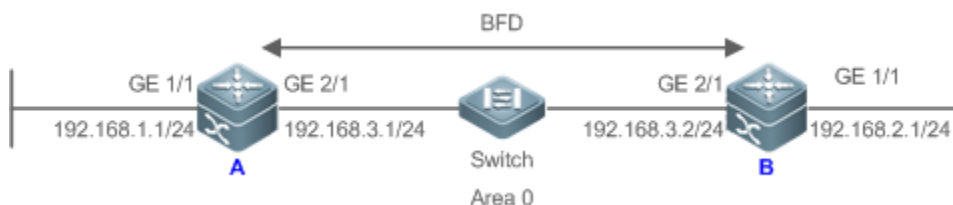
BFD support for static routing prevents routers from selecting a faulty static route as the forwarding path and enables rapid routing failover by using an available backup forwarding path.

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 5-2



Remarks	<p>A and B are routers.</p> <p>Switch is a Layer-2 switch.</p> <p>A and B are connected through the Layer-2 switch.</p>
----------------	--

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 5-3

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|-----|-----|-----|-----|
|Vers | Diag |Sta|P|F|C|A|D|M| Detect Mult | Length |
|-----|-----|-----|-----|
|                                     My Discriminator
|-----|-----|-----|-----|
|                                     Your Discriminator
|-----|-----|-----|-----|
|                                     Desired Min TX Interval
|-----|-----|-----|-----|
|                                     Required Min RX Interval
|-----|-----|-----|-----|
|                                     Required Min Echo RX Interval
|-----|-----|-----|-----|

```

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 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.

4. Down: Indicates that a session is in the Down state or is established just now.
5. Init: Indicates that the local system has communicated with the peer system and desires to bring the session to the Up state.
6. Up: Indicates that a session has been negotiated successfully.
7. 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.

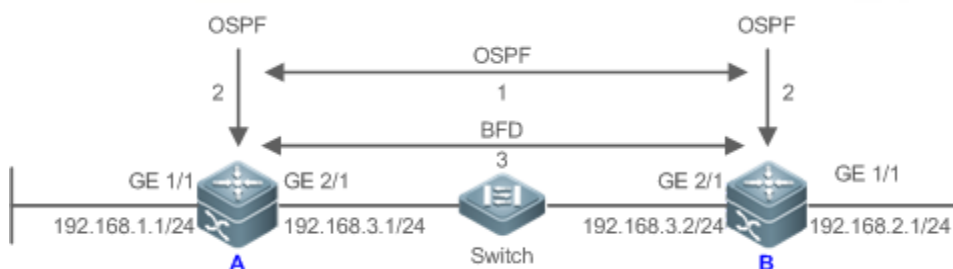
Working Principle

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 5-4



BFD session establishment process:

8. OSPF discovers a neighbor and establishes a connection with the neighbor.
9. OSPF instructs BFD to establish a session with the neighbor.
10. 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.

i 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:

11. 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.
12. Interfaces at both ends negotiate BFD session parameters and detect the session based on the parameters during the establishment of a BFD session.
13. 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

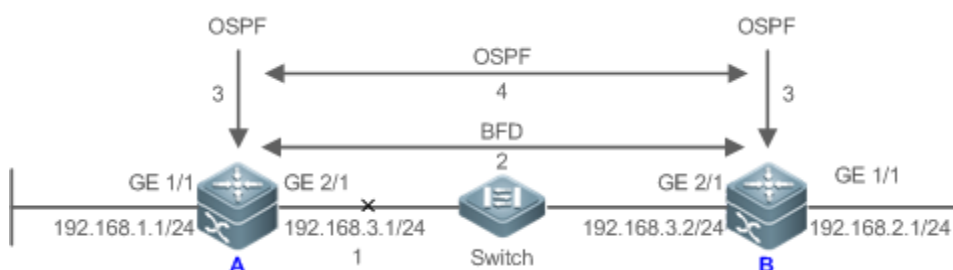
Link detection starts after the establishment of a BFD session. BFD periodically transmits BFD control packets. If it fails to receive BFD packets from the peer end within the detection time, it deems that the session is Down and notifies the associated application to accelerate the convergence.

Working Principle

Detection Process

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

Figure 5-5



Handling procedure after a BFD session is Down:

14. The link between Router A and Switch fails.
15. The BFD session between Router A and Router B is Down.
16. BFD notifies the local OSPF that the forwarding path to the neighbor is faulty.
17. 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.

- i The query mode is not supported and cannot be configured at present.
- i Only BFD session version 1 supports the BFD echo mode.
- i 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.

i 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.

i 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.

i 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.

i 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.

i 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.

i 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.

i 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.

i 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 (BVs). 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.

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

❖ BFD support for MPLS

The BFD support for Multiple protocol Label Switching (MPLS) refers that label switched paths (LSPs) use BFD to rapidly detect the neighbor status. The following detection modes are supported:

18. BFD detects static LSPs.

19. BFD detects LSPs generated by the Label Distribution Protocol (LDP).

20. BFD can detect reverse links of LSPs by using the IP protocols.

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

❖ 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.

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

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 BFD 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.	
	<code>bfd up-dampening</code>	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:
 21. 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.
 22. 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:
 23. 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.
 24. 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:
 25. 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.

26. The echo detection function of BFD does not support multi-hop detection. Ensure that the echo function is disabled when configuring multi-hops.
27. The echo mode takes effect only after this mode is enabled at both ends of a BFD session.
28. 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	<code>bfd interval <i>milliseconds</i> min_rx <i>milliseconds</i> multiplier <i>interval-multiplier</i></code>
Parameter Description	interval <i>milliseconds</i> : Indicates the minimum TX interval, with the unit of milliseconds. min_rx <i>milliseconds</i> : Indicates the minimum RX interval, with the unit of milliseconds. multiplier <i>interval-multiplier</i> : 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. This command must not be configured on the L3 AP ports.

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 Layer-3 AP interfaces. 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	<i>milliseconds</i> : Indicates the BFD slow timer, with the unit of milliseconds. The value ranges from 1,000 to 30,000 and the default value 3,000 is adopted if it is not set.
Defaults	The transmission interval of slow control packets is 3,000 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 <i>src-address</i> [source-ip <i>dst-address</i>] process-pst
Parameter Description	<i>src-address</i> : Indicates the peer IP address of an interface. <i>dst-address</i> : 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*.

- ❖ In global configuration mode, run the **ipv6 route static bfd [vrf vrf-name] interface-type interface-number gateway [source ip-address]** command to enable BFD support for IPv6 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 **vrp 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.
- ❖ Run the **bfd bind static-lsp peer-ip ip-address source-ip ip-address [local-discriminator discr-value remote-discriminator discr-value] [process-state]** command to enable BFD support for static LSP. For details, see *Configuring MPLS*.
- ❖ Run the **bfd bind ldp-lsp peer-ip ip-address nexthop ip-address [interface interface-type interface-number] source-ip ip-address [local-discriminator discr-value remote-discriminator discr-value] [process-state]** command to enable BFD for LDP LSP. For details, see *Configuring MPLS*.
- ❖ Run the **bfd bind backward-lsp-with-ip peer-ip ip-address [vrf vrf-name] interface interface-type interface-number [source-ip ip-address] { local-discriminator discr-value remote-discriminator discr-value }** command to enable BFD support for dynamic LSP. For details, see *Configuring MPLS*.

Verification

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

Configuration Example

Configuring BFD support for OSPF

Scenario Figure 5-6	
Configurati on Steps	<ul style="list-style-type: none"> ❖ 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	<pre>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 192.168.3.0.0.0.255 area 0 A(config-router)# network 192.168.1.0.0.0.255 area 0 A(config-router)# bfd all-interfaces A(config-router)# end</pre>
B	<pre>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</pre>

	<pre>B(config-router)# log-adj-changes detail B(config-router)# network 192.168.3.0.0.255 area 0 B(config-router)# network 192.168.2.0.0.255 area 0 B(config-router)# bfd all-interfaces B(config-router)# end</pre>
<p>Verification</p>	<p>Display verification.</p>
<p>A</p>	<pre>A# show bfd neighbors details OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Up 192.168.3.1 192.168.3.2 1/2 Up 532 (3) 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</pre>
<p>B</p>	<pre>B# show bfd neighbors details OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int Up 192.168.3.2 192.168.3.1 2/1 Up 532 (5) Ge2/1 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</pre>

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	

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	<code>bfd cpp</code>
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	<ul style="list-style-type: none"> ❖ Configure this function on a switch on a network where attacks exist. ❖ Configure the BFD protection function.
	<pre>QTECH#configure terminal QTECH(config)# bfd cpp QTECH(config)# end</pre>
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	<code>bfd up-dampening[<i>milliseconds</i>]</code>
Parameter Description	<i>milliseconds</i> : 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

Configura tion Steps	<ul style="list-style-type: none"> ❖ 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.
	<pre>QTECH#configure terminal QTECH(config)# interface fastEthernet 0/2 QTECH(config)# bfd up-dampening 60000 QTECH(config)# end</pre>
Verificatio n	N/A

5.5 Monitoring

Displaying

Description	Command
Displays BFD session information.	show bfd neighbors [<i>vrf vrf-name</i>] [client { bgp ospf rip vrrp static-route pbr vrrp-balance ldp-lsp static-lsp backward-lsp-with-ip pst }] [<i>ipv4 ip-address ipv6 ip-address</i>][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 [<i>interface interface-type interface-number ipv4 ip-address ipv6 ipv6-address</i>]

Debugs BFD packets.

```
debug bfd packet[interface interface-type interface-number |  
ipv4 ip-address | ipv6 ipv6-address]
```

6 CONFIGURING IP EVENT DAMPENING

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

i 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

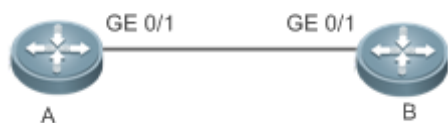
Application	Description
Routed Port Flap Dampening	Monitors the state change of the Layer-3 port on a router, and suppresses frequent port flapping.

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 longer 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 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	
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.

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 [<i>half-life-period</i> [<i>reuse-threshold suppress-threshold max-suppress</i> [<i>restart</i> [<i>restart-penalty</i>]]]]
Parameter Description	<p><i>half-life-period</i>: Indicates the half-life period. Value range: <1–30>; default value: 5s.</p> <p><i>reuse-threshold</i>: Indicates the reuse threshold. Value range: <1–20,000>; default value: 1,000.</p> <p><i>suppress-threshold</i>: Indicates the suppress threshold. Value range: <1–20,000>; default value: 2,000.</p> <p><i>max-suppress</i>: Indicates the maximum suppress time. Value range: <1–255>; default value: four times the half-life period.</p> <p>restart <i>restart-penalty</i>: Indicates the initial penalty. Value range: <1–20,000>; default value: 2,000.</p>
Command Mode	Interface configuration mode
Usage Guide	<p>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.</p> <p>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.</p> <p>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:</p> <pre>% Maximum penalty (10) is less than suppress penalty (2000). Increase maximum suppress time</pre> <p>If the available system memory is insufficient to run the dampening command, the following message indicating a configuration failure will be printed:</p> <pre>% No memory, configure dampening fail!</pre>

Configuration Example

Configuring IP Event Dampening on Layer-3 Ports

<p>Scenario Figure 6-2</p>	
<p>Configurati on Steps</p>	<p>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.</p>
<p>A</p>	<pre>QTECH(config)#interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#dampening 30 1500 10000 100</pre>
<p>B</p>	<pre>QTECH(config)#interface GigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#dampening 30 1500 10000 100</pre>
<p>Verificatio n</p>	<p>Run the show interfaces dampening command to check the IP Event Dampening configuration on the corresponding ports.</p>
	<pre>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</pre>

Common Errors

- ❖ The port on a Layer-3 switch is not converted to a routed port by using the **no swiport** command before IP Event Dampening is configured.

6.5 Monitoring

Clearing

Description	Command
Clears the interface counters.	clear counters

- i** 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.

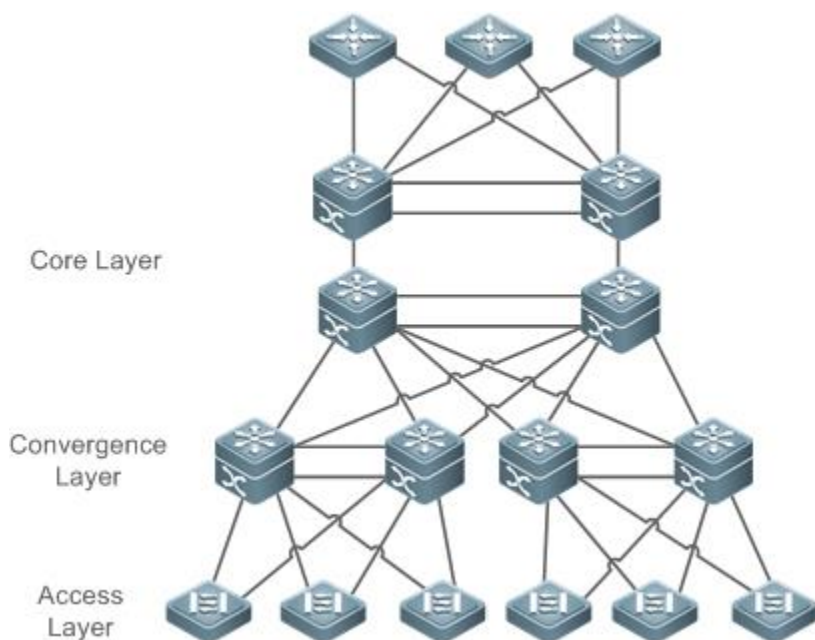
Description	Command
Enables debugging of IP Event Dampening.	debug dampening interface

7 CONFIGURING VSU

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.

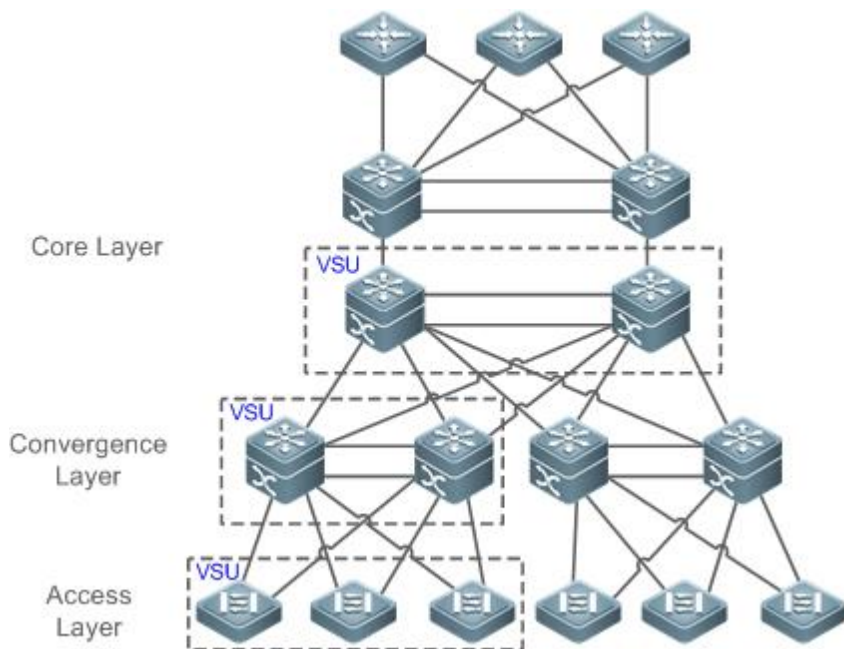
Figure 7-1 Traditional network architecture



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	<p>The devices from left to right in Figure 7-3 are Device 1, Device 2, Device 3 and Device 4.</p> <p>For details on VSL, see the description in section 1.3.1.</p> <p>Device 1 is the global master device.</p> <p>Device 2 is the global slave device.</p> <p>Devices 3 and 4 are the global candidate devices.</p>
----------------	---

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.

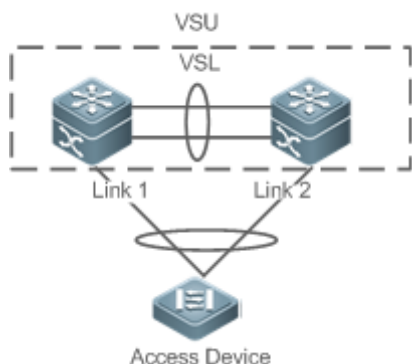
7.2.2 Simplifying Networking Topology

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.

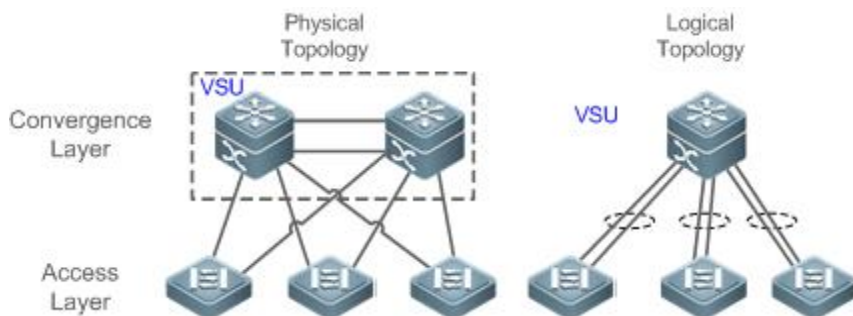
7.3 Features

Basic Concepts

VSU System

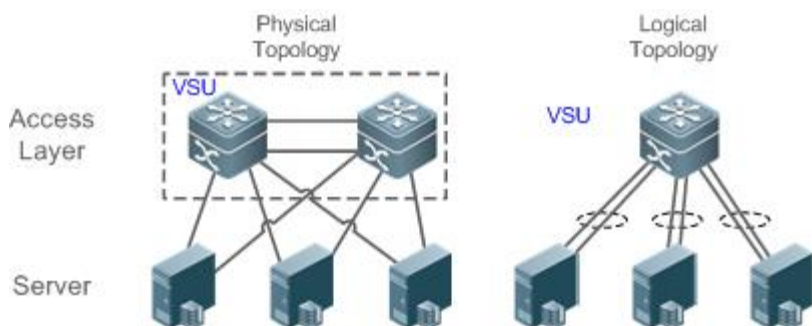
VSU system is a single logical entity consisting of two or multiple devices in traditional network architecture. For example, the convergence layer VSU system as shown in the following figure can be seen as a single device that interacts with the core layer and access layer.

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 to 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.

i 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.

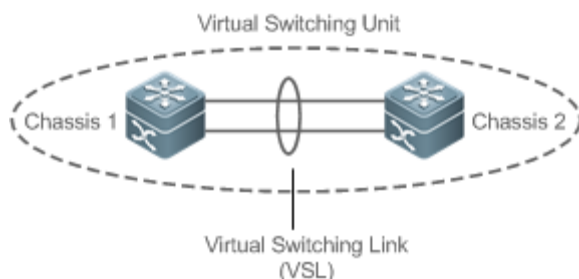
7.3.1 Virtual Switching Link (VSL)

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:

29. 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.
30. 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:

31. The data stream flooded on the VLAN
32. 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.

i 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

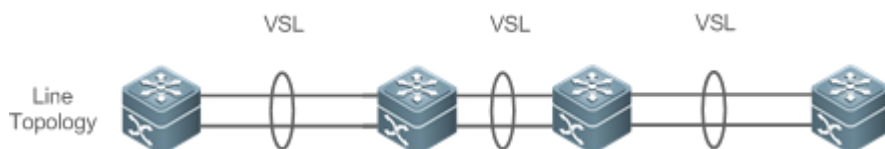
The VSU system supports line topology and ring topology. Devices are connected through a VSL to form a line that is called the line topology.

Working Principle

Topology

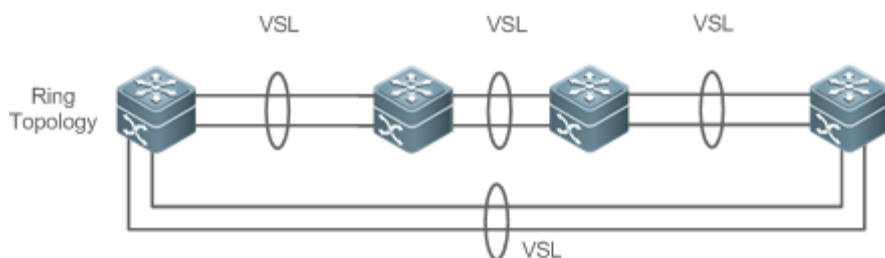
The line topology is simple. It uses a very few ports and cables. Two devices are connected with a communication link only. Therefore, the VSL has low reliability.

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



- i** 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.
- i** 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.

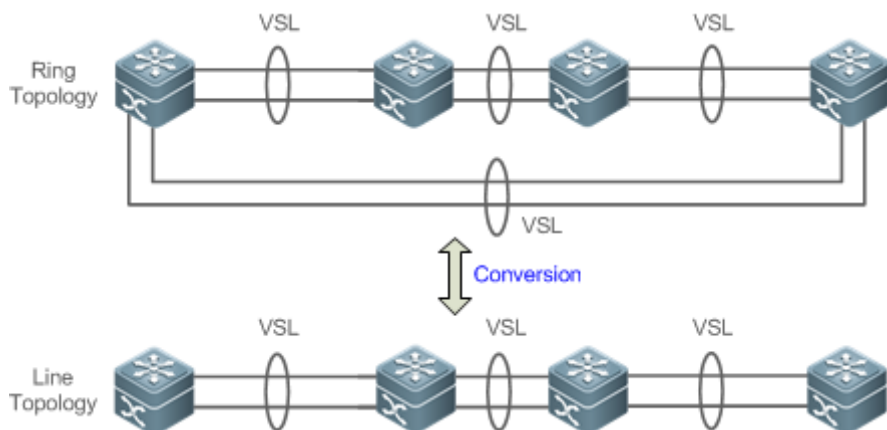
Topology Convergence

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.

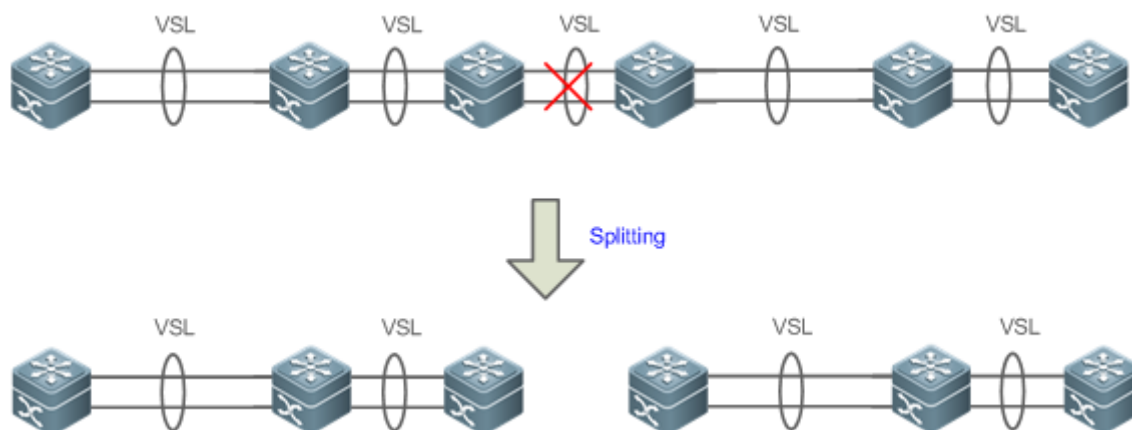
Figure 7-10 Ring-to-line and line-to-ring



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



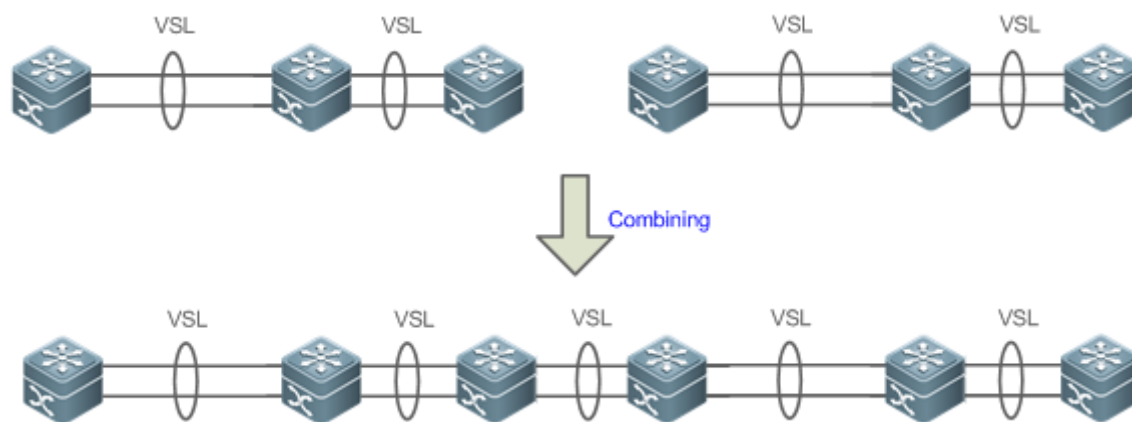
Topology Combining

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



- i** 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

33. Select the VSU group with the highest priority.
34. If the previous item cannot help make a judgment, select the VSU group with more physical devices.

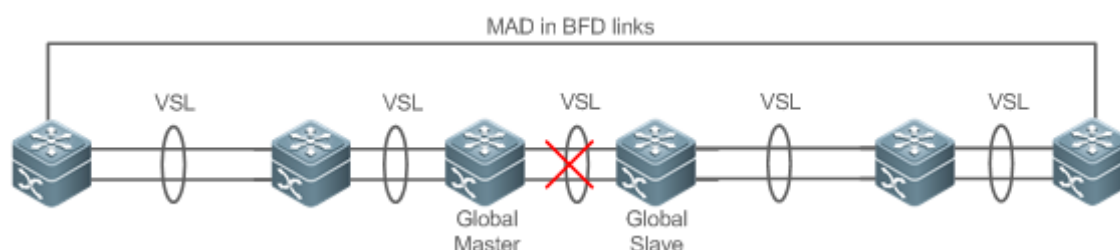
35. If the previous item cannot help make a judgment, select the VSU group with a higher health. (Health: total bandwidth of all physical interfaces (except for management and VSL interfaces) in the UP state in the topology.)
36. If the previous item cannot help make a judgment, select the VSU group with a smaller switch ID (that of the two global master switches).
37. 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).
38. 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



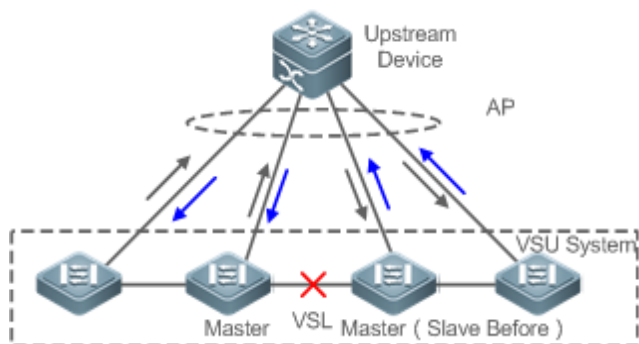
- ⚠ When there is a pair of BFD links, you are advised to deploy the detection links at the two ends of the topology.
- ⚠ You need to adopt the extension BFD and you cannot configure the dual-active detection port by using the existing BFD configurations and commands.

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 1.1.4.4 *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

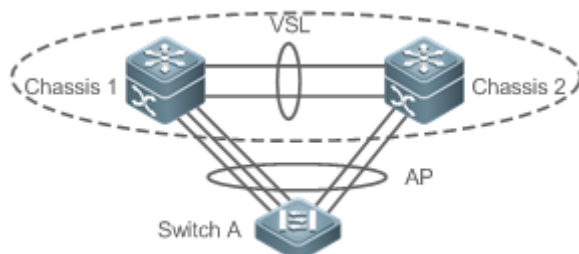
Working Principle

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.

❖ 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."

7.4 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.
	port-member interface	Configures the VSL member interface.
	switch convert mode virtual	Changes the standalone mode to the VSU mode.

		<p> (Optional) It is used to configure the device attributes in the VSU mode.</p>								
		<table border="1"> <tr> <td>switch description</td> <td>Configures the device description.</td> </tr> <tr> <td>switch crc</td> <td>Configures error frame check.</td> </tr> </table>	switch description	Configures the device description.	switch crc	Configures error frame check.				
switch description	Configures the device description.									
switch crc	Configures error frame check.									
Configuring VSU in the VSU Mode	Configuring VSU Attributes	<p> (Optional) It is used to configure the device attributes in the VSU mode.</p>								
		<table border="1"> <tr> <td>switch domain</td> <td>Changes the domain ID.</td> </tr> <tr> <td>switch renumber</td> <td>Changes the switch ID.</td> </tr> <tr> <td>switch description</td> <td>Configures the device description.</td> </tr> <tr> <td>switch crc</td> <td>Configures error frame check.</td> </tr> </table>	switch domain	Changes the domain ID.	switch renumber	Changes the switch ID.	switch description	Configures the device description.	switch crc	Configures error frame check.
		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	<p> (Optional) It is used to configure a VSL.</p>								
		<table border="1"> <tr> <td>vsl-port</td> <td>Enters the VSL interface configuration mode.</td> </tr> <tr> <td>port-member interface</td> <td>Configures a VSL member interface.</td> </tr> </table>	vsl-port	Enters the VSL interface configuration mode.	port-member interface	Configures a VSL member interface.				
		vsl-port	Enters the VSL interface configuration mode.							
	port-member interface	Configures a VSL member interface.								
	<table border="1"> <tr> <td>dual-active detection</td> <td>Configures DAD.</td> </tr> <tr> <td>dual-active bfd interface</td> <td>Configures the BFD DAD interface.</td> </tr> <tr> <td>dual-active interface</td> <td>Configures an AP as a DAD interface.</td> </tr> <tr> <td>dual-active exclude interface</td> <td>Configures an excluded interface.</td> </tr> </table>	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.	
	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 Dual-Active Detection	<p> (Mandatory) It is used to configure DAD.</p>								
		<table border="1"> <tr> <td>dual-active detection</td> <td>Configures DAD.</td> </tr> <tr> <td>dual-active bfd interface</td> <td>Configures the BFD DAD interface.</td> </tr> <tr> <td>dual-active interface</td> <td>Configures an AP as a DAD interface.</td> </tr> <tr> <td>dual-active exclude interface</td> <td>Configures an excluded interface.</td> </tr> </table>	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.
		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	<p> (Optional) It is used to configure traffic balancing in the VSU mode.</p>									
	<table border="1"> <tr> <td>switch virtual aggregateport-lff enable</td> <td>Configures the AP LFF mode.</td> </tr> <tr> <td>switch virtual ecmp-lff enable</td> <td>Configures the ECMP LFF mode.</td> </tr> </table>	switch virtual aggregateport-lff enable	Configures the AP LFF mode.	switch virtual ecmp-lff enable	Configures the ECMP LFF mode.					
	switch virtual aggregateport-lff enable	Configures the AP LFF mode.								
switch virtual ecmp-lff enable	Configures the ECMP LFF mode.									
<table border="1"> <tr> <td>switch virtual ecmp-lff enable</td> <td>Configures the ECMP LFF mode.</td> </tr> </table>	switch virtual ecmp-lff enable	Configures the ECMP LFF mode.								
switch virtual ecmp-lff enable	Configures the ECMP LFF mode.									
Changing the VSU Mode to	<p> (Optional) It is used to change the VSU mode to the standalone mode.</p>									

	the Standalone Mode	switch convert mode standalone	Changes the VSU mode to the standalone mode.
--	-------------------------------------	---------------------------------------	--

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 <i>number</i>
Parameter Description	<i>Number</i> : Indicates domain ID of the VSU
Defaults	The default domain ID is 100.
Command Mode	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 <i>switch_id</i>
Parameter Description	<i>switch_id</i> : indicates the switch ID in the VSU system. Range: 1-2.
Defaults	The default device ID is 1.
Command Mode	Domain configuration mode
Usage Guide	<p>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.</p> <p>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.</p> <p>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.</p>

Command	switch <i>switch_id</i> priority <i>priority_num</i>
Parameter Description	<p><i>switch_id</i>: Indicates a switch ID for which a priority needs to be configured.</p> <p><i>priority_num</i>: Indicates the switch priority, ranging from 1 to 255.</p>
Defaults	The default device priority is 100.
Command Mode	Domain configuration mode
Usage Guide	<p>A larger value means a higher priority. A device with the highest priority is chosen as the master device.</p> <p>You can run this command in the standalone or VSU mode. The modified priority takes effect only after you restart the device.</p> <p>This command is not used to modify the value of <i>switch_id</i>. In the standalone mode, if <i>switch_id</i> is set to 1, running the switch 2 priority 200 command does not work. You can first set <i>switch_id</i> to 2 and then run the switch 2 priority 200 command. In the VSU mode, <i>switch_id</i></p>

	indicates the ID of the currently running switch. If the ID does not exist, the configuration does not take effect.
--	---

Command	switch <i>switch_id</i> description <i>dev-name</i>
Parameter Description	<i>switch_id</i> : Indicates the device ID. <i>dev-name</i> : 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* [copper | fiber]** 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 <i>interface-name</i> [copper fiber]
Parameter Description	<i>interface-name</i> : Indicates a two-dimensional interface name, such as Tengigabitethernet 1/1 and Tengigabitethernet 1/3. copper : Indicates the copper interface attribute. fiber : Indicates the optical interface attribute.
Defaults	N/A
Command Mode	VSL interface configuration mode
Usage Guide	Add a member interface of the VSL link. <i>interface-name</i> 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	<code>switch crc errors <i>error_num</i> times <i>time_num</i></code>
Parameter Description	<i>error_num</i> : 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. <i>time_num</i> : 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 [<i>switch_id</i>]
Parameter Description	<i>switch_id</i> : 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 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

<p>Scenario Figure 7-16</p>	 <p>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.</p>
<p>Configuration Steps</p>	<ol style="list-style-type: none"> 5. Perform the following configuration on the Switch 1: <ul style="list-style-type: none"> ❖ Configure VSU attributes and VSL interfaces. ❖ Change the standalone mode to the VSU mode. 6. Perform the following configuration on the Switch 2: <ul style="list-style-type: none"> ❖ Configure VSU attributes and VSL interfaces. ❖ Change the standalone mode to the VSU mode.
<p>Switch-1</p>	<pre>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)#switch 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</pre>
<p>Switch-2</p>	<pre>QTECH# configure terminal QTECH(config)# switch virtual domain 100 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</pre>

	<pre> 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 </pre>
Verification	<p>❖ Run the show switch virtual config command to view the VSU attributes of Switch 1 and Switch 2.</p>
Switch-1	<pre> 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 ! </pre>
Switch-2	<pre> 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 ! </pre>

Common Errors

- ✔ A VSL interface of a chassis device must be 10 Gigabit or higher.

7.4.2 Configuring VSU in the VSU Mode

7.4.2.1 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 switch1** 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 <i>domain_id</i>
Parameter Description	<i>domain_id</i> : Indicates the virtual domain ID of the VSU system.
Defaults	The default domain ID is 100.
Command Mode	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 <i>switch_id</i> domain <i>new_domain_id</i>
Parameter Description	<i>switch_id</i> : Indicates the ID of the currently running switch in the VSU mode, ranging from 1 to 2. <i>new_domain_id</i> : 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 <i>switch_id</i> renumber <i>new_switch_id</i>
Parameter Description	<i>switch_id</i> : Indicates the ID of a switch. In a VSU system, the switch ID ranges from 1 to 2 for chassis switches. <i>new_switch_id</i> : 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 <i>switch_id</i> priority <i>priority_num</i>
Parameter Description	<i>switch_id</i> : Indicates a switch ID for which a priority needs to be configured. <i>priority_num</i> : Indicates the switch priority, ranging from 1 to -255.
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 <i>switch_id</i> description <i>dev-name</i>
Parameter Description	<i>switch_id</i> : Indicates a switch ID for which a priority needs to be configured. <i>dev_name</i> : 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	<i>error_num</i> : 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. <i>time_num</i> : 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

<p>Scenario Figure 7-17</p>	 <p>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.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ❖ Modify the configurations of Switch 2.
<p>Switch-1</p>	<pre>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</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ❖ Run the show switch virtual config command for verification.
<p>Switch-1</p>	<pre>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 !</pre>


```
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 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* [**copper** | **fiber**] 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 <i>interface-name</i> [copper fiber]
Parameter Description	<i>interface-name</i> : Indicates a two-dimensional interface name, such as GigabitEthernet 0/1 and GigabitEthernet 0/3. copper : Indicates the copper interface attribute. fiber : Indicates the optical interface attribute.
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.

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	<ul style="list-style-type: none"> ❖ Add interface 1/1/3 as the VSL interface for Switch 1 and delete interface 1/1/2 from the VSL interface.
Switch-1	<pre> 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 </pre>

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	<pre> 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 ! </pre>
	<pre> 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 ! </pre>

7.4.2.3 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 than 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 <i>domain_id</i>
Parameter Description	<i>domain_id</i> : Indicates the domain ID.
Defaults	The default domain ID is 100.
Command Mode	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 <i>interface-name</i>
Parameter Description	<i>interface-name:</i> 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. You 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 <i>interface-name</i>
Parameter Description	<i>interface-name</i> : 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.

- i** 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 <i>interface-name</i>
Parameter Description	<i>interface-name</i> : 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.

- ⚠** The excluded interface must be routing rather than VSL.

⚠ 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

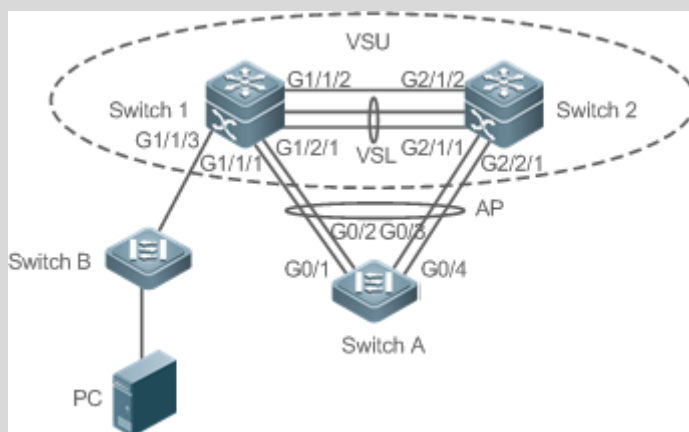
Use the **show switch virtual dual-active { aggregateport | bfd | summary }** to display the current DAD configuration.

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.

Configurati on Steps	<ul style="list-style-type: none"> ❖ 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. <p>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.</p>
Switch 1	<pre>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</pre>
Switch A	<pre>QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# interface aggregategateport 1 QTECH(config-if-aggregategateport 1)# interface range GigabitEthernet 0/1-4 QTECH(config-if-aggregategateport 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</pre>
Verificatio n	<ul style="list-style-type: none"> ❖ View the DAD configuration. ❖ View the BFD DAD configuration.
Switch 1	<pre>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</pre>

Common Errors

- ❖ A BFD DAD interface is not a routing interface.
- ❖ Neither BFD DAD nor AP-based DAD are enabled and activated.

7.4.2.4 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).

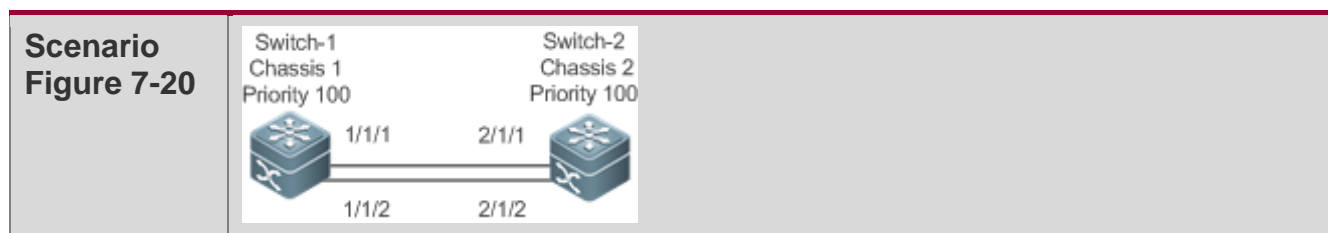
Verification

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



	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	<pre>QTECH#config QTECH(config)# switch virtual domain 100 QTECH(config-vs-domain)# switch virtual aggregateport-lff enable</pre>
Verification	❖ Run the show switch virtual balance command for verification.
Switch-1	<pre>QTECH#show switch virtual balance Aggregate port LFF: enable Ecmp lff enable</pre>

7.4.2.5 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 [<i>switch_id</i>]
Parameter Description	<i>switch_id</i> : 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 <i>vsd.virtual_switch.text.vsd ID</i> . Then, the master switch clears the global configuration files <i>config.text</i> 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

<p>Scenario Figure 7-21</p>	 <p>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.</p>
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ❖ Change the mode of Switch 1 to the standalone mode. ❖ Change the mode of Switch 2 to the standalone mode.
<p>Switch-1</p>	<pre>QTECH# switch convert mode standalone 1 QTECH# switch convert mode standalone 2</pre>
<p>Verification</p>	<p>Run the show switch virtual config command to display the switch status.</p>
<p>Switch-1</p>	<pre>QTECH#show switch virtual config switch_id: 1 (mac: 0x1201aeda0M) ! switch virtual domain 100 ! switch 1 switch 1 priority 100 ! switch convert mode standalone</pre>

	<pre>! port-member interface Tengigabitethernet 1/1 ! port-member interface Tengigabitethernet 1/3 !</pre>
	<pre>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 !</pre>

7.5 Monitoring and Maintenance

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 }
Displays the current VSL running information in the VSU mode.	show switch virtual link [port]
Redirects to the console of the master switch or any switch.	session { device switch_id master }
Displays the current switch ID.	show switch id

8 CONFIGURING VSD

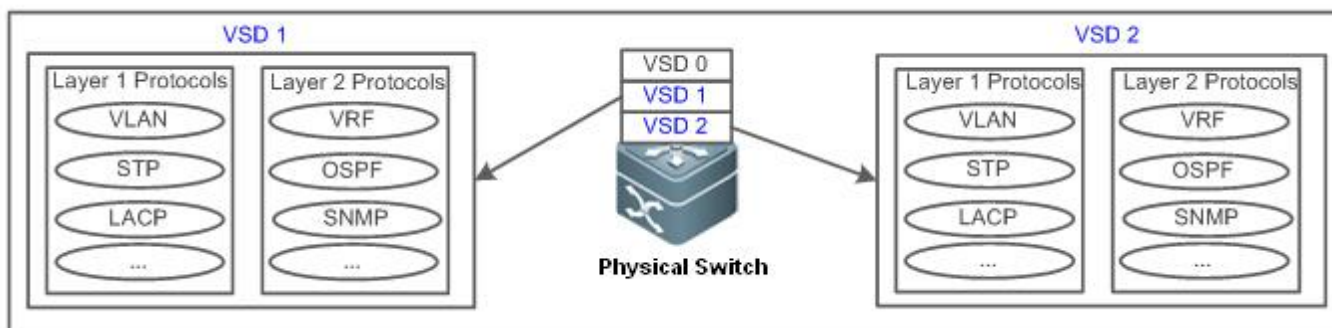
8.1 Overview

As Information Communication Technology (ICT) networks especially data center networks keep growing, service types emerge one after another. On one hand, network management becomes increasingly complicated. On the other hand, increasingly-higher requirements are posed on network properties such as service isolation, security and reliability. In addition, with the rapid improvement of hardware capacity and the maturity of multi-shelf, cluster, distributed routing & switching systems, the service processing capacity of a single physical network device has been raised to a new level. It becomes imperative to make full use of the powerful service processing capacity to resiliently meet present service demands while promoting expansibility smoothly in the future.

A Virtual Switch Device (VSD) is a network virtualization technology that divides one physical device into several logical devices. Each logical device is called a VSD, which has independent hardware and software resources, including interfaces, CPU, a routing table and a forwarding table to be separately maintained, and configuration files managed by specific administrators. From users' perspective, each VSD is an independent device.

A physical device can be virtualized into several logical devices using the VSD technology, as shown in Figure 8-1. A physical device bears several network nodes on the logical topology to maximize the utilization of existing resources and reduce operation costs. Meanwhile, different VSDs are deployed with different services to shield services from faults, thereby improving network security and reliability.

Figure 8-1 VSD



As shown in Figure 8-1, VSD0 is the system default VSD while VSD1 and VSD2 are non-default VSDs created by users.

- ❖ VSD0: administrative domain, also the default VSD. It exists by default and cannot be deleted. It creates and deletes non-default VSDs, and manages all physical resources of the device, including physical ports, CPU, and memory resources.
- ❖ VSD1: client domain, also called the non-default VSD (the same as VSD2). It is created and deleted by VSD0, with its physical resources assigned by VSD0. The client domain can use only the resources assigned by VSD0. It cannot use or obtain other resources.
- ❖ Physical port resources: physical Ethernet ports on line cards only, excluding any other types of ports such as console and management ports.

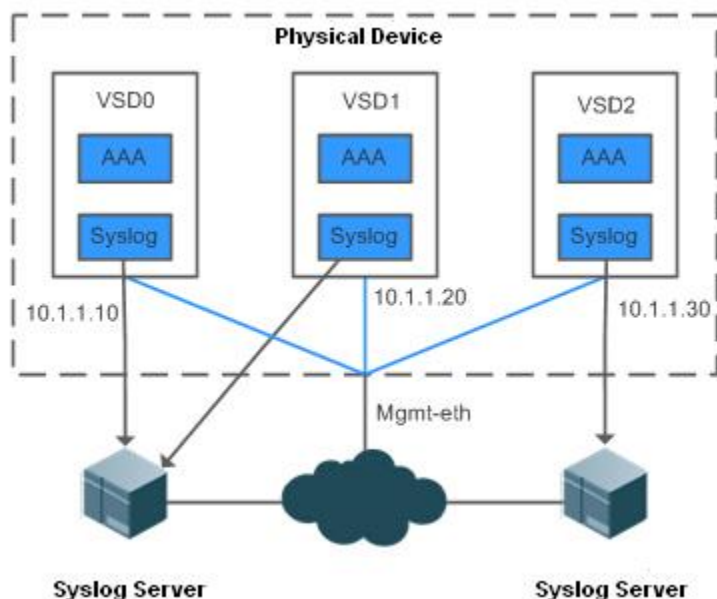
Advantages

- ❖ The VSD technology divides physical ports based on service chips to ensure superposition of service capacity, which means service specifications are exclusively shared among VSDs. For example, if the VLAN service specifications are 4063 VLANs, the VLAN service specifications are 4063 VLANs for both VSD 1 and VSD2.
- ❖ Each VSD works independently. If isolated, VSDs cannot communicate with each other, thereby achieving relatively high security.
- ❖ VSD supports flexible resource scheduling. For example, if there are new branches, the administrator can divide VSDs on demand to reduce costs in the purchase and hardware upgrade of network devices, so as to enhance utilization of present network resources.

Management

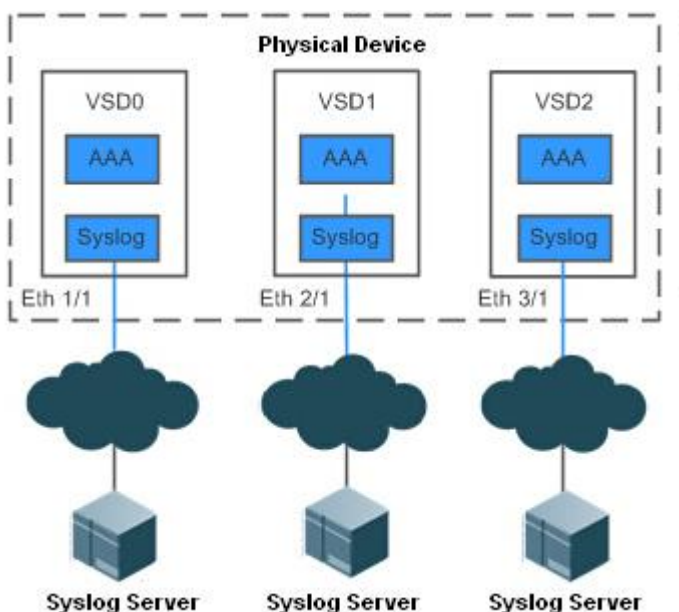
- ❖ Out-of-band management: VSDs are managed via a management (MGMT) port. All VSDs share a MGMT port on the supervisor module, and have different MGMT ports of their own with IP addresses configured. Users can log in to the VSD CLI corresponding to the specified IP address of a MGMT port.

Figure 8-2 Out-of-band Management



- ❖ In-band management: VSDs are managed via a physical Ethernet port. Users can log in to the VSD console corresponding to the specified VSD port. For example, Eth 2/1 port can only place you in the VSD1 CLI, as shown in Figure 8-3.

Figure 8-3 In-band Management



- ❖ CLI management: VSDs are managed via a serial port on the supervisor module. By default, you log in to the VSD0 CLI via the serial port.

Protocols and Standards

- ❖ VSD is a QTECH-proprietary protocol.

8.2 Applications

Application	Description
Providing isolated services within a physical device	Virtualize a physical device into several logical devices that provide isolated services.

8.2.1 Providing Isolated Services within a Physical Service

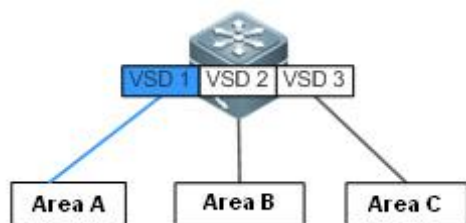
Scenario

The VSD technology can be used to virtualize one physical device into several logical devices that provide independent services.

As shown in Figure 8-4, a convergence device is virtualized into three logical devices that provide isolated services to areas A, B, and C.

- ❖ VSD1 is the uplink device of area A, VSD2 is the uplink device of area B, and VSD3 is the uplink device of area C.
- ❖ VSD1, VSD2, and VSD3 respectively connect to devices in the corresponding areas via their own links.

Figure 8-4



Deployment

- ❖ VSD1, VSD2, and VSD3 are independent logical devices, deployed with services based on requirements of areas A, B, and C.

8.3 Features

Basic Concepts

Default VSD

The VSD-capable physical device is the default VSD. Therefore, login to such a device is actually login to the default VSD. Any configuration on the physical device is applied to the default VSD. The default VSD exists originally and cannot be deleted. It has all permissions of the physical device, and uses and manages all hardware resources of the device. The default VSD not only creates and deletes non-default VSDs, but also assigns hardware resources to the non-default VSDs. By default, hardware resources that are not assigned to the non-default VSDs are used by the default VSD. The default VSD is called QTECH and numbered 0.

Non-Default VSD

In comparison, a non-default VSD has to be created by the default VSD before use. It is created without physical port resources (other resources of the physical device such as CPU and memory shared with the default VSD), and has no available physical port resources until assigned by the default VSD. Non-default VSDs cannot be created or deleted by another non-default VSD.

Physical Device Resources

Physical device resources include:

- ❖ **Physical ports:** physical port resources that exclude virtual ports and serial ports.
- ❖ **CPU:** CPU time that each VSD can use.
- ❖ **SD cards:** storage resources of external storage SD cards.
- ❖ **Memory:** physical device memory which normally means board memory.

i By default, physical port resources belong to the default VSD while other physical resources are shared between the default VSD and non-default VSDs.

MAC Address

A physical switch normally has a system MAC address. When a physical device is virtualized into several logical devices, each logical device requires a system MAC address. Therefore, each VSD will be automatically assigned a MAC address (while the system MAC of the default VSD is that of the physical device).

VSD's Master/Slave Role

A classis-type device is normally equipped with two supervisor modules to ensure high availability. When working properly, one of the supervisor modules plays the master role while the other serves as the salve. Service data of the master supervisor module will be backed up to the slave supervisor module. Once divided, each VSD is distributed on both the master supervisor module and the slave supervisor module to play roles. To prevent other VSD users from being affected by the master/slave switching executed by non-default VSD users, only the VSDO administrator can execute the master/slave switching command.

Features

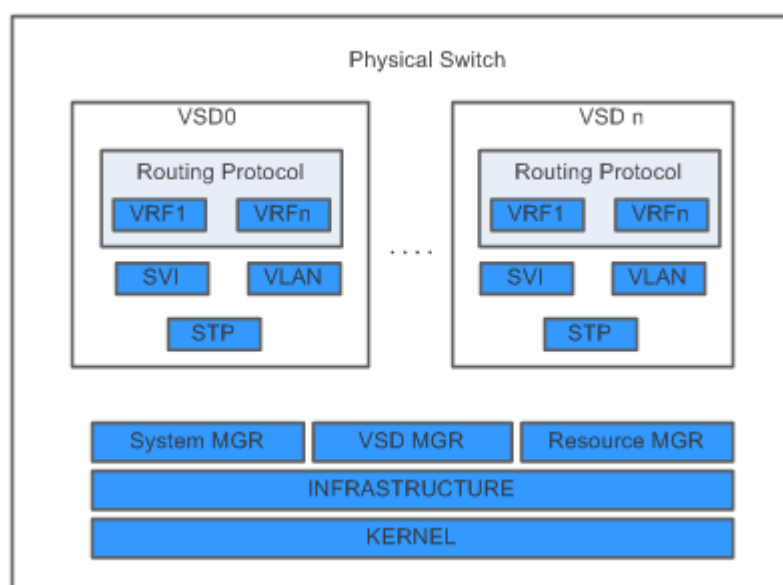
Feature	Function
VSD	Virtualize a physical device into several logical devices.

8.3.1 VSD

Working Principle

VSD can be regarded as a kind of virtualization technology that virtualizes a physical device into several logical devices. VSD virtualization is constructed based on the virtualization technology for operating systems. Different from the virtual machine technology, it utilizes system services provided by the operating system kernel to ensure mutually isolated user space services. Operating systems that adopt this virtualization include Linux Containers (Linux LXC), OpenVZ, Linux-VServer, and FreeBSD jails.




Figure 8-5 Structure of VSD 1:N Virtualization



As shown in Figure 8-5, the default VSD is VSD0 while the non-default ones created by users are VSD1 to VSDn.

- ❖ **System MGR:** When a VSD is created, the System MGR will initiate all processes required to start the VSD. When a VSD needs to enable a new service, the System MGR will initiate the corresponding service process (for example, when VSD2 starts the OSPF service, the System MGR will initiate a corresponding OSPF process). When a VSD is deleted, the System MGR will delete all service processes belonging to the VSD.
- ❖ **VSD MGR:** The VSD MGR is used to support non-default VSD management to create and delete non-default VSDs. More importantly, the VSD MGR provides the System MGR or Resource MGR with related APIs to achieve system management or resource management of non-default VSDs.
- ❖ **Resource MGR:** It allocates resources such as VLANs and VRFs to various VSDs during resource management.
- ❖ **INFRASTRUCTURE layer:** It provides interfaces between upper-layer applications and hardware resources.
- ❖ **KERNEL:** There is only one kernel as VSD is light-weight virtualization.

8.4 Configuration

Configuration	Suggestions and Related Commands	
Configuring a VSD	 Mandatory configuration, which is used to create a VSD.	
	vsd <i>vsd_name</i> [<i>id vsd_number</i>]	Creates a VSD.
	allocate interface <i>int_index</i>	Allocates physical ports to the VSD.
	allocate slot <i>slot_id</i>	Allocates multi-service cards to the VSD.
	cpu weight <i>weight_value</i>	Allocates the CPU weight to a VSD.
	memory ratio <i>limit_ratio</i>	Allocates the maximum memory ratio to a VSD.
Restarting a VSD	 Optional configuration, which is used to restart a VSD as necessary.	
	reset vsd [<i>vsd_name</i>]	Restarts a non-default VSD.
Switching Between VSDs	 Optional configuration, which is used to switch between the default VSD and a non-default VSD.	
	switchto vsd <i>vsd_name</i>	Switches from the default VSD to a non-default VSD.

	switchback	Switches back from the non-default VSD to the default VSD.
--	-------------------	--

8.4.1 Configuring a VSD

Configuration Effect

- ❖ Create a non-default VSD.
- ❖ Allocate physical port resources to the newly created non-default VSD.
- ❖ Allocate multi-service cards to the newly created non-default VSD.

Precautions


- ❖ Users can use the VSD function in a VSU environment. When allocating ports to the VSD, the line card where the ports are located will be reset, thereby disconnecting the VSL link on the line card. As there is only one VSL link in the system, the VSU will also be topologically split. It is recommended that you use the VSD function in the VSU environment and configure VSL ports on several line cards to ensure the stability of the VSU and prevent the VSU from being affected by allocating VSD ports or restarting the VSD.
- ❖ The VSD0 administrator can set any eligible port of any VSD as a VSL port to be centrally managed by VSD0. The VSD0 administrator can switch any VSL port back to a normal port that will return to the VSD of the chip where the port is located. For example, all ports on a line card are under VSD2, and only one port is set as a VSL port. When the administrator switches the VSL port to a normal port, it will return to VSD2.
- ❖ The dual-host detection port in the VSD environment must be set in VSD0. When VSD0 detects the dual host status, all VSDs enter the recovery status.

Configuration Steps

Creating a VSD


- ❖ To use the VSD function, you must configure it first.

Command	<code>vsd <i>vsd_name</i> [id <i>vsd_number</i>]</code>
Parameter Description	<i>vsd_name</i> : VSD name <i>vsd_number</i> : VSD ID. If not specified, the minimum available ID will be used.
Defaults	No VSD is created by default.
Command Mode	Global configuration mode

Usage Guide	<p>This command is used to create a VSD and enter the VSD configuration mode. If a VSD has been created, use this command to enter the VSD configuration mode.</p> <p>When entering the specified VSD configuration mode, you do not need to enter the <code>vsd_number</code>. If you enter the <code>vsd_number</code>, make sure that it is consistent with the current VSD number; otherwise, an error message appears.</p> <p> Get a corresponding license before you create a non-default VSD, with the total number of non-default VSDs created not greater than the total authorized number. The name of a VSD is independent from and irrelevant to the hostname of the device.</p>
-------------	---

Allocating Physical Port Resources

- ❖ The configuration is mandatory.

Command	allocate interface <i>int_index</i>
Parameter Description	<i>int_index</i> : Interface index
Defaults	All physical ports belong to VSD 0.
Command Mode	VSD configuration mode
Usage Guide	<p>This command is used to allocate or reclaim physical ports to or from a non-default VSD.</p> <p> If no physical port is available for a non-default VSD, the VSD can only be managed but not used. If all physical ports are allocated to a non-default VSD, the default VSD will have no physical port available. The VSL interface cannot be allocated.</p>

Allocating Multi-Service Card Resources

- ❖ The configuration is optional.
- ❖ To use a multi-service card such as a firewall card in a certain non-default VSD environment, users have to perform this configuration in VSD mode. If a multi-service card is used by a non-default VSD, other non-default VSDs cannot use this multi-service card. For example, a firewall card is used in a non-default VSD2, and then other VSDs cannot use it.

Command	allocate slot <i>slot_id</i>
Parameter Description	<i>slot_id</i> : Multi-service slot ID
Defaults	The multi-service card belongs to VSD 0.
Command Mode	VSD configuration mode
Usage Guide	This command is used to allocate multi-service card resources to a non-default VSD or to reclaim multi-service card resources from the non-default VSD.

Verification

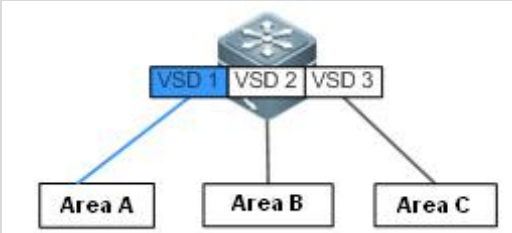
A newly created VSD is an independent logical device, and its configuration can be verified after you log in to the VSD.

- ❖ Check whether you can log in to the newly created VSD.
- ❖ Check whether you can configure ports after logging in to the VSD.

Configuration

Example

Creating Three Logical Devices on a Physical Device

Network Environment Figure 8-6	
Configuration Method	<p>Create VSD A;</p> <ul style="list-style-type: none"> ❖ Allocate physical port 1/1-24 to VSD A; ❖ Allocate multi-service card 3 to VSD A. <p>Create VSD B;</p> <ul style="list-style-type: none"> ❖ Allocate physical port 1/25-48 to VSD B; ❖ Allocate multi-service card 4 to VSD B. <p>Create VSD C;</p> <ul style="list-style-type: none"> ❖ Allocate physical port 2/1-12 to VSD C; ❖ Allocate multi-service card 5 to VSD C.

<p>VSD A</p>	<pre>QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# vsd VSDA QTECH(config-vsd)# allocate int gi 1/1 Interface-group[1/1 ~ 1/24] and their config will be removed from vsd[0]. Are you sure to continue(y/n)? [no]y QTECH(config-vsd)# allocate slot 3 Allocating slot 3 may cause some service in source vsd to stop. Are you sure to continue (y/n)? [no]y QTECH(config-vsd)#</pre>
<p>VSD B</p>	<pre>QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# vsd VSDB QTECH(config-vsd)# allocate int gi 1/25 Interface-group[1/25 ~ 1/48] and their config will be removed from vsd[0]. Are you sure to continue(y/n)? [no]y QTECH(config-vsd)# allocate slot 4 Allocating slot 4 may cause some service in source vsd to stop. Are you sure to continue (y/n)? [no]y QTECH(config-vsd)#</pre>
<p>VSD C</p>	<pre>QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# vsd VSDC QTECH(config-vsd)# allocate int gi 2/1 Interface-group[2/1 ~ 2/12] and their config will be removed from vsd[0]. Are you sure to continue(y/n)? [no]y QTECH(config-vsd)# allocate slot 5 Allocating slot 5 may cause some service in source vsd to stop. Are you sure to continue (y/n)? [no]y QTECH(config-vsd)#</pre>
<p>Verification</p>	<p>Log in to the corresponding VSD to perform relevant port configuration.</p>
<p>VSD A</p>	<pre>QTECH# switchto vsd VSDA ***** QTECH General Operating System Software Copyright (c) 1998-2013s by QTECH Networks. All Rights Reserved. Neither Decompiling Nor Reverse Engineering Shall Be Allowed. ***** QTECH-VSDA> enable QTECH-VSDA# show int</pre>

<p>VSD B</p>	<pre> QTECH# switchto vsd VSDB ***** QTECH General Operating System Software Copyright (c) 1998-2013s by QTECH Networks. All Rights Reserved. Neither Decompiling Nor Reverse Engineering Shall Be Allowed. ***** QTECH-VSDA> enable QTECH-VSDA# show int </pre>
<p>VSD C</p>	<pre> QTECH# switchto vsd VSDC ***** QTECH General Operating System Software Copyright (c) 1998-2013s by QTECH Networks. All Rights Reserved. Neither Decompiling Nor Reverse Engineering Shall Be Allowed. ***** QTECH-VSDA> enable QTECH-VSDA# show int </pre>

Common Errors

- ❖ You create a VSD without any valid license.
- ❖ The total number of non-default VSDs created exceeds the maximum number authorized.
- ❖ You reclaim a port that does not belong to a non-default VSD.
- ❖ You allocate a physical port belonging to a non-default VSD to another non-default VSD.
- ❖ No new physical port resources are available for allocation.

8.4.2 Restarting a VSD

Configuration Effect

- ❖ Restarting a single non-default VSD will only affect services in the non-default VSD.

Notes

- ❖ The interface card of the non-default VSD will be reset. If a VSL port is involved on the line card where the VSD port is located, the VSU might be topologically split. Therefore, it is recommended that the restart operation be performed only when services are not busy.
- ❖ The default VSD cannot be restarted.

Configuration Method

❖ To restart a VSD, perform this configuration.

Command	Use this command to log in from the default VSD to a non-default VSD. switchto vsd <i>vsd_name</i>	
Parameter Description	Parameter	Description
	vsd <i>vsd_name</i>	Name of a non-default VSD
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to log in from the default VSD to a non-default VSD.	

Command	Use this command to switch back from the non-default VSD to the default VSD. switchback	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to switch back from a non-default VSD to the default VSD. This command does not support login to the non-default VSD via Telnet, which means that this command is effective only when switching from the default VSD to the non-default VSD (that is to say, switchto shall go before switchback).	

Verification

When a VSD is restarted, only its services will be interrupted. Other VSDs will not be affected unless the port on the interface card is shared by two VSDs.

8.4.3 VSD Switching

Configuration Effect

❖ Switch from VSD0 to a non-default VSD or vice versa.

Notes

- ❖ Users cannot switch between VSDs if directly logging in via the out-of-band or in-band port.

Configuration Method

- ❖ To switch between VSDs, perform this configuration. The switching between non-default VSDs has to be performed via the default VSD. For example, to switch from non-default VSD1 to VSD2, you have to switch first from VSD1 to the default VSD0 and then from VSD0 to VSD2.

Verification

Check the current VSD ID after logging in.

Configuration Example

❖ Switching to a Non-default VSD

Configurati on Method	❖ Switch from VSD0 to a non-default VSD; ❖ Switch from the non-default VSD back to VSD0.
	<pre> QTECH# switchto vsd admin ***** QTECH General Operating System Software Copyright (c) 1998-2013s by QTECH Networks. All Rights Reserved. Neither Decompiling Nor Reverse Engineering Shall Be Allowed. ***** admin# </pre>
	<pre> QTECH# switchto vsd admin ***** QTECH General Operating System Software Copyright (c) 1998-2013s by QTECH Networks. All Rights Reserved. Neither Decompiling Nor Reverse Engineering Shall Be Allowed. ***** admin# switchback QTECH# </pre>
Verificatio n	Check the VSD where the current user resides.

```
QTECH# sho vsd current-vsdc
Current vsd is 0 – QTECH
QTECH #
```

Common Errors

N/A

8.5 Monitoring

Displaying

Command	Function
show vsd { current-vsdc membership detail all } [<i>vsd_name</i>]	Displays VSD information.

9 CONFIGURING NLB GROUP

9.1 Overview

NLB Group, also called the cluster service, is a cluster technology developed to support Network Load Balance (NLB) of Microsoft®.

NLB Group allows all member servers in a cluster to receive IP packets sent to the cluster. As compared with common cluster technologies, switches enabled with NLB Group can directly connect to servers without using layer-2 switches. In addition, data packets can be sent to the server only from specified ports to prevent flooding in the broadcast domains.

When setting up a cluster to provide external services, you can enable NLB Group on the switch to improve service reliability.

9.2 Applications

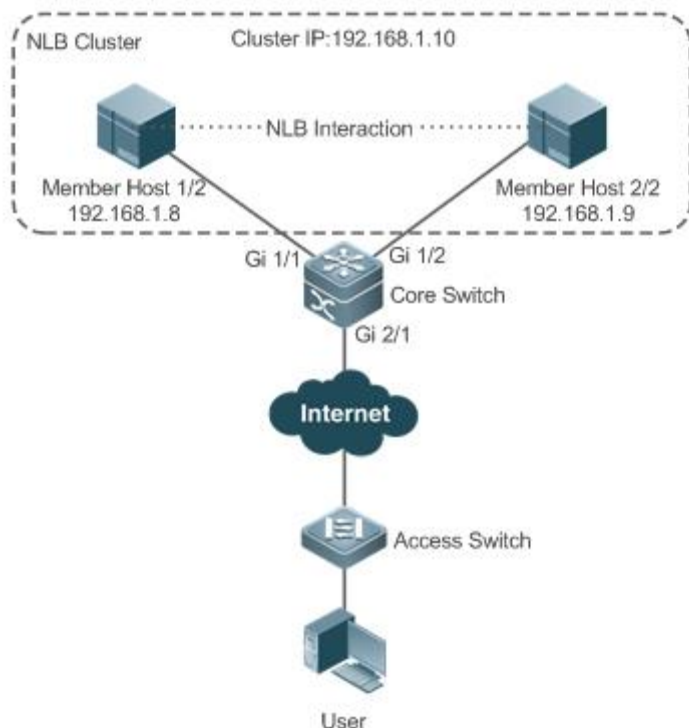
Application	Description
Supporting Web Server NLB Group	Uses NLB to set up a web server cluster with the support of NLB Group on layer-3 switches.

9.2.1 Supporting Web Server NLB Group

Scenario

As shown in Figure 9-1, a web server is set up using NLB Group to provide website services externally. By default, NLB Group is disabled on layer-3 switches, that is, IP packets sent to the cluster cannot be sent to the active and standby servers at the same time. Normally, a layer-2 switch is needed between the cluster server and layer-3 switch. In this way, IP packets can be sent to the active and standby servers at the same time but a unicast data packet has only one next-hop address. To allow the active and standby servers to receive IP data packets sent to the cluster, you need to configure the cluster service on the layer-3 switch. After this, packets sent to the NLB Group with IP address 192.168.1.10 are sent to the active and standby servers through ports Gi 1/1 and Gi 1/2 at the same time.

Figure 9-1 NLB Group Application Diagram



Deployment

- ❖ Enable NLB Group on layer-3 switches.

9.3 Features

Basic Concepts

NLB

NLB is a cluster technology built in Windows Server by Microsoft®. It provides network load balance for TCP/IP-based services and applications to improve availability and extensibility.

- ❗ For details about the NLB service, visit Microsoft® website <http://technet.microsoft.com>.

↘ VRF

NLB Group supports VPN Routing and Forwarding (VRF). VRF refers to the VPN to which the NLB Group belongs on the layer-3 switch.

NLB-Address

NLB Group IP address. NLB allows all PCs in an NLB Group to share the same IP address to provide external services.

Reflector-Port

Reflector port. To implement the NLB Group service, the layer-3 switch sends IP packets sent to the NLB Group to all member hosts of the NLB Group server through a reflector port.

⚠ A reflector port must be configured. It can only be a layer-2 switching port and no configuration is allowed on the reflector port. To ensure normal NLB Group service, the reflector port must be idle, that is, no network cable or optical fiber cable can be inserted into the port.

Destination-Port

Destination port to which packets are sent, that is, the port that connects the member host in the NLB Group and layer-3 switch, for example, Gi 1/1 and Gi 1/2 in Figure 9-1.

⚠ The NLB Group server communicates with the layer-3 switch using SVI, but not the routed port.

Overview

Feature	Description
NLB Group	Supports NLB Group of Microsoft.

9.3.1 NLB Group

Working Principle

Using Figure 9-1 for example, the following describes the working principle of NLB Group:

39. A user sends an IP packet whose destination IP address is the NLB Group IP address, 192.168.1.10.
40. The IP packet reaches the layer-3 switch through routing.
41. After reaching the layer-3 switch through Gi 2/1, the IP packet is sent to the reflector port and then forwarded to the destination ports Gi 1/1 and Gi 1/2 by the reflector port.
42. The active and standby servers in the NLB Group receive the IP packet.

Related Configuration

Enabling NLB Group

- ❖ By default, NLB Group is disabled.
- ❖ After NLB Group attributes are configured, the NLB Group service is automatically enabled.



Configuring NLB Group Attributes

- ❖ By default, no NLB Group attribute is configured.
- ❖ Run the **nlb-group group-number [vrf vrf-name] ip nlb-address reflector-port interface-name** command to configure NLB Group attributes. The value of **group-number** ranges from 1 to 100. If **vrf** is not specified, a global VRF is used.

Configuring the NLB Group Destination Port

- ❖ By default, no NLB Group destination port is configured.
- ❖ Run the **nlb-group** *group-number* **destination-port** *interface-name* command to configure the NLB Group destination port. A maximum of 32 destination ports can be configured.

9.4 Configuration

Configuration	Description and Command
Configuring NLB Group Attributes	 (Mandatory) It is used to enable NLB Group.
	nlb-group <i>group-number</i> [vrf <i>vrf-name</i>] ip <i>nlb-address</i> reflector-port <i>interface-name</i> Configures NLB Group attributes.
Configuring the NLB Group Destination Port	 (Optional) By default, all ports in the VLAN where the NLB Group resides are used as the NLB Group destination ports.
	nlb-group <i>group-number</i> destination-port <i>interface-name</i> Configures the NLB Group destination port.

9.4.1 Configuring NLB Group Attributes

Configuration Effect

- ❖ Enable NLB Group to send IP packets sent to the NLB Group to all member hosts in the NLB Group.

Notes

- ❖ NLB Group does not support dynamic switching of the operation mode in the NLB Group.
- ❖ When the NLB cluster server works in IGMP multicast mode, layer-3 multicast cannot be enabled on the layer-3 switch; otherwise, NLB Group may be abnormal. If layer-3 multicast must be enabled, configure the NLB Group server to work in non-IGMP multicast mode, that is, unicast mode or multicast mode.

Configuration Steps

Configuring NLB Group Attributes

- ❖ Mandatory.
- ❖ Configure the attributes on the switch.

Verification

Use a client to access the NLB Group and send a service request.

- ❖ Check whether a response is received to the request.
- ❖ Check whether all member hosts receive the request.

Related Commands

Configuring NLB Group Attributes

Command	<code>nlb-group group-number [vrf vrf-name] ip nlb-address reflector-port interface-name</code>
Parameter Description	<i>group-number</i> : Specifies the NLB Group number. <i>vrf-name</i> : Specifies the VRF. <i>nlb-address</i> : Specifies the NLB Group IP address. <i>interface-name</i> : Specifies the interface name.
Command Mode	Global configuration mode
Usage Guide	To remove NLB group attributes, run the no nlb-group group-number [vrf vrf-name] ip nlb-address reflector-port interface-name or no nlb-group group-number command. To delete all NLB groups, run no nlb-group all .

Common Errors

- ❖ A layer-3 port is configured as the reflector port.

9.4.2 Configuring the NLB Group Destination Port

Configuration Effect

- ❖ Configure NLB Group so that IP packets sent to the NLB Group are sent to the NLB Group server through specified ports.

Notes

- ❖ When the NLB Group server works in NLB IGMP multicast mode, you can configure NLB Group attributes as well as selecting whether to enable IGMP Snooping. If IGMP Snooping is enabled, the switch automatically learns the NLB Group destination port through IGMP Snooping and users do not need to manually configure the port. If the NLB Group destination port is configured and IGMP Snooping is enabled, only the destination ports receiving IGMP Report messages can receive the packet to access NLB Group, that is, the ports not only configured by users but also learned through IGMP Snooping. If IGMP Snooping is disabled, the switch cannot automatically learn the NLB Group destination port, which is the same as that when NLB Group works in unicast mode.

Configuration Steps

Configuring the NLB Group Destination Port

- ❖ Optional.
- ❖ When the NLB Group server works in unicast or multicast mode, it is advised to configure the ports directly connected to member hosts as NLB Group destination ports.

- ❖ Destination ports are configured on the switch.

Verification

- ❖ Check whether the configurations are successful.

Related Commands

Configuring the NLB Group Destination Port

Command	nlb-group <i>group-number</i> destination-port <i>interface-name</i>
Parameter Description	<i>group-number</i> : Specifies the NLB Group number. <i>interface-name</i> : Specifies the interface name.
Command Mode	Global configuration mode
Usage Guide	To delete NLB Group destination ports, run the no nlb-group <i>group-number</i> destination-port <i>interface-name</i> or no nlb-group <i>group-number</i> command.

Configuration Example

Configuring NLB Group Attributes and Specifying Connection Ports

Scenario Figure 9-2	<p>The diagram illustrates an NLB Cluster configuration. A dashed box labeled 'NLB Cluster' contains two member hosts: 'Member Host 1/2' with IP 192.168.1.8 and 'Member Host 2/2' with IP 192.168.1.9. A dotted line between them is labeled 'NLB Interaction'. The cluster IP is 192.168.1.10. Both member hosts are connected to a 'Core Switch' at interfaces Gi 1/1 and Gi 1/2 respectively. The Core Switch is also connected to a 'User' at interface Gi 2/1.</p>
Configuration Steps	<ul style="list-style-type: none"> ❖ Configure VLAN 10 and add Gi 1/1 and Gi 1/2 to VLAN 10. ❖ Configure SVI 10 and assign IP address 192.168.1.1 to SVI 10. ❖ Configure the routing port Gi 2/1 and assign IP address 192.168.2.1 to Gi 2/1. ❖ Configure NLB Group attributes and specify connection ports.

A	<pre>QTECH#configure Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#interface range gigabitEthernet 1/1-2 QTECH(config-if-range)#switchport access vlan 10 QTECH(config-if-range)#exit</pre>
B	<pre>QTECH(config)#interface vlan 10 QTECH(config-if-VLAN 10)#ip address 192.168.1.1/24 QTECH(config-if-VLAN 10)#end</pre>
C	<pre>QTECH(config)#interface gigabitEthernet 2/1 QTECH(config-if-GigabitEthernet 2/1)#no switchport QTECH(config-if-GigabitEthernet 2/1)#ip address 192.168.2.1/24 QTECH(config-if-GigabitEthernet 2/1)#exit</pre>
D	<pre>QTECH(config)#nlb-group 1 ip 192.168.1.10 reflector-port gigabitEthernet 1/3 QTECH(config)#nlb-group 1 destination-port gigabitEthernet 1/1-2</pre>
Verification	<ul style="list-style-type: none"> ❖ Send a packet from user 192.168.2.2 to NLB Group 192.168.1.10 and check whether all member hosts receive the request packet. ❖ In privileged mode, run the show nlb-group command to display the current status of NLB Group 1.

Common Errors

- ❖ The reflector port is configured as the NLB Group destination port.

9.5 Monitoring

Displaying

Description	Command
Displays NLB Group service status.	show nlb-group [<i>group-number</i>]