Руководство пользователя

QSR-2830

Оглавление

1 HDLC CONFIGURATION

1.1 Understanding HDLC

The RGOS supports the Cisco HDLC private protocol. Unlike the ISO HDLC, the Cisco HDLC protocol uses the SDLC frame format and supports synchronous and full-duplex operation, but does not support the traffic control like the ISO HDLC. It is an unreliable connection. After this protocol is encapsulated, the reliable connection is implemented at the upper layer. The HDLC features high efficiency and simple implementation and is a point-to-point (PTP) link protocol.

Note

Reliable connection refers to the message acknowledgement mechanism that is used during data communication. A lost packet will be retransmitted and the connection is interrupted if a packet times out. The PTP protocol means that communication parties are in one-to-one relationship. PPP and SLIP are also PTP protocols, whereas X.25 and Frame Relay are point-to-multipoint protocols.

The working principle of the HDLC is illustrated in the following phases:

- Negotiation and connection establishment: Two parties of the HDLC link send a link detection negotiation message to each other every 10 seconds. The messages are received or sent based on the sequence numbers of messages. Disorder of sequence numbers results in link disconnection. This kind of message that is used to detect whether a PTP link is active is called the keepalive message.
- Message transmission: The IP messages are encapsulated at the HDLC layer. During data transmission, the keepalive message negotiation is still working to detect whether the link is valid.
- Timeout disconnection: When the interface encapsulated with HDLC cannot receive the acknowledgement from the peer to increment the sequence number for 3 times continuous (or 6 times when the packet receiving speed is over 1000 packets/second), the link state changes from UP to Down. At this time, the link is in down state, and data communication fails.

1.2 Configuring HDLC

1.2.1 HDLC Configuration Task List

The HDLC configuration is rather simple and involves only the following tasks.

- Configuring the Interface Encapsulation Protocol
- Configuring the Keepalive Time

1.2.2 Configuring the Interface Encapsulation Protocol

The protocol encapsulated on the synchronous interface is HDLC by default.

Use the following command to change the protocol encapsulated on the interface to HDLC.

Command	Function
Qtech(config-if)#**encapsulation hdlc**	Encapsulates the HDLC protocol.

1.2.3 Configuring the Keepalive Time

For the HDLC encapsulated on a synchronous interface, only two parameters are configurable: interval at which the keepalive message is sent and the maximum timeout time of the keepalive message. The interval is 10 seconds by default.

Use the following command to set the interval and maximum timeout time of the keepalive message based on the link traffic.

Command	Function
Qtech(config-if)#**keepalive** *second*s	Sets the interval at which the keepalive message is sent and the maximum timeout time of the keepalive message. The maximum timeout time is optional. The range of the interval is from 1 to 32767. The range of the maximum timeout time is from 1 to 255.

1.3 Monitoring and Maintaining HDLC

Command	Function
Qtech#**debug hdlc events**	Turns on the HDLC link status event debugging switch.
Qtech#**debug hdlc packets**	Turns on the HDLC message receiving/transmitting debugging switch.

1) debug hdlc events

If an interface (for example, Serial1/0) is encapsulated with HDLC, the following information is printed during the keepalive message negotiation:

```
%Interface serial 1/0 : receive one HDLC keepalive packet.
%Interface serial 1/0 send one keepalive packet:
    my_seq = 21, my_seen = 20, your_seen = 16
    line protocol is UP, not in loopback state.
%Interface serial 1/0 : receive one HDLC keepalive packet.
%Interface serial 1/0 send one keepalive packet:
    my_seq = 22, my_seen = 21, your_seen = 17
    line protocol is UP, not in loopback state.
```

Where, my_seq is the sequence number of the message sent by the local router, my_seen is the sequence number of the HDLC keepalive message recognized by the peer router, and your_seen means the sequence number of the peer router recognized by the local router. The sequence numbers are incremental. See the following debug information:

```
%Interface serial 1/0 : receive one HDLC keepalive packet.
%Interface serial 1/0 send one keepalive packet:
    my_seq = 21, my_seen = 20, your_seen = 16
    line protocol is UP, not in loopback state.
%Interface serial 1/0 send one keepalive packet:
    my_seq = 22, my_seen = 20, your_seen = 16
    line protocol is UP, not in loopback state.
%Interface serial 1/0 send one keepalive packet:
    my_seq = 23, my_seen = 20, your_seen = 16
    line protocol is UP, not in loopback state.
```

The local sequence number my_seq increments according to the keepalive time, but the keepalive message of the peer router is not received. The my_seen is always 20. The local party has no way to know the acknowledgement for the increment of your_seen. This means that the message of the peer router cannot reach the local HDLC protocol layer during communication possibly because the peer router is shut down or a fault occurs during line transmission.

1) debug hdlc packets

Use this command to turn on the HDLC receiving/transmitting message debug switch to print the messages received or to be sent by the HDLC, including the message length and received message type. If the message is longer than 64 bytes, only the first 64 bytes are printed, as shown below:

```
Interface serial 1/0 HDLC input:
  packet->len = 22(0x16):
  8F 00 80 35 00 00 00 02 00 00 00 16 00 00 00 1A
  FF FF 00 5C E2 53
  packet->pkt_type = 3(PDD_RARP)
Interface serial 1/0 HDLC output:
  packet->len = 22(0x16):
  8F 00 80 35 00 00 00 02 00 00 00 1B 00 00 00 16
  FF FF 00 5F 8E D9
```

2 PPP AND MP PROTOCOL CONFIGURATION

2.1 PPP and MP Protocol Introduction

The PPP (Point-to-Point Protocol) is a kind of link layer protocol providing bearer for network data packets over point-to-point links. PPP defines a whole set of protocols, including LCP (Link Control Protocol), NCP (Network Control Protocol) and authentication protocols (PAP and CHAP). PPP is widely used for its ability of authentication, easy to expand and support of synchronization and asynchronization. For the PPP specifications, see RFC 1661.

2.1.1 PPP Working Process and Principle

- The PPP performs LCP negotiation before line setup, including operation mode (SP or MP), authentication method, and maximum transmission unit.
- The PPP enters the Line Establish phase after LCP negotiation. At this time, the LCP state is Opened, indicating that the link has been established.
- If authentication (the remote end authenticates the local end or vice versa) is enabled in the configuration, the PPP enters the Authenticate phase to start CHAP or PAP authentication.
- If authentication fails, it enters the Terminate phase to remove the link, and the LCP status turns to Closed; if the authentication succeeds, it enters the Network consultation phase (NCP), here, the LCP status is still Opened but that of IPCP and IPXCP turns from Closed to Opened.
- The support of NCP negotiation includes IPCP, IPXCP and BRIDGECP negotiation. IPCP negotiation mainly includes the IP addresses of both parties; IPXCP negotiation mainly includes network IDs and node numbers; BRIDGECP negotiation mainly includes the MAC addresses of both parties, MAC address type, spanning tree and Bridge ID. One or more network layer protocols are selected and configured through NCP negotiation. After the successful configuration of each selected network layer protocol, this network layer protocol can send messages through this link.
- This link will keep available for communication, until a definite LCP or NCP frame closes it, or some external events happen.

2.1.2 PPP Authentication Mode

The PPP supports two kinds of authentication modes: PAP and CHAP.

1. The PAP is a two-handshake authentication, and the password is in clear text.The PAP authentication process is as follows:
   1) The party to be authenticated sends the username and password to the authenticating party.
   2) The authenticating party checks whether this user name exists and whether the password is correct according to the user configuration, and then returns a response accordingly.
2. The CHAP refers to challenge handshake authentication protocol, and the password is in cipher text (key). The process of CHAP authentication is as follows:
   1) The authenticating party sends some random reports to the party to be authenticated.

2) The authenticated party encrypts the random messages using its own password and MD5 algorithm, and sends the generated cipher text back to the authenticating party.
3) The authenticating party encrypts the original random reports with the stored password of the authenticated party and the MD5 algorithm, compares the two cipher texts, and then returns the relevant response according to the comparison results.

2.1.3 MP Protocol Introduction

The Multi-Link PPP (MP) binds the PPP of multiple physical links to a single logical interface, aiming to increase link bandwidth. Any physical link that supports PPP can enable MP and be bound to the same logical interface Dialer port. The MP allows fragment of the messages on the network layers like IP. The fragments of the message are transmitted via multiple links and arrive at the same destination at the same time, resulting in summarization of the bandwidth of all links.

The operational process of the MP is as follows:

After the negotiation of general LCP parameters is completed, the PPP initiates the MP request again. If the peer link supports MP and responds properly, it is bound to the logical interface together with the other physical links for further NCP (such as IPCP) negotiation. If negotiation succeeds, all MP physical links use the network address of the same logical interface.

2.2 PPP Configuration

2.2.1 PPP Configuration Task List

This chapter describes how to configure PPP in the dedicated line mode (including synchronous interface and asynchronous interface). For the PPP configuration for the dialup connection available in the serial interface, additional configurations are needed in addition to the following ones. See Dialup Configuration Guide for details.

- Configure the interface encapsulation protocol
- Configure the PPP CHAP authenticated party
- Configure the PPP CHAP authenticating party
- Configure the PPP PAP authenticated party
- Configure the PPP PAP authenticating party
- Configure the PPP compression mode

2.2.2 Configuring the Encapsulation Protocol on the Interface

To configure the PPP, encapsulate the PPP on the interface. To encapsulate the PPP, run the following commands in the interface configuration mode:

Command	Function
Qtech(config-if)#**encapsulation ppp**	Encapsulate the PPP on the interface.
Qtech(config-if)#**no encapsulation ppp**	Remove the PPP encapsulation on the interface.

2.2.3 **Configuring the PPP CHAP Authenticated Party**

The CHAP authentication generally involves authenticating party and authenticated party. The CHAP negotiation is initiated by the authenticating party, and the authenticated party sends only the username and password for the use of the PPP authentication. By default, the authenticated party sends its own hostname as the PPP username.

To configure the PPP CHAP authenticated party, use the following command at interface configuration mode:

Command	Function
Qtech(config-if)# **ppp chap hostname** *hostnmae*	Specify the hostname for PPP CHAP authentication.
Qtech(config-if)# **ppp chap password** {**0**|**7**} *password*	Specify the password for PPP CHAP. authentication

If the hostname used by the authenticating party is known, the following configuration can be used:

Command	Function
Qtech(config-if)# **ppp chap hostname** *hostnmae*	Specify the hostname for PPP CHAP authentication.
Qtech(config)# **username** *username* password {0|7} *password*	Create user database records for the authenticating party hostname, with passwords consistent at both ends.

Note

There are clear text password and cipher text password, "0" for clear text password and 1-7 for cipher text password. The default input method is the clear text password. In this manual, all places involving password setting is suitable for the above rule. In the interconnection with other manufacturers, only the clear text password is accepted. For the configuration of bidirectional authentication, the configuration of authenticating party is also needed.

2.2.4 **Configuring the PPP CHAP Authenticating Party**

The PPP CHAP authenticating party initiates the authentication proactively. Since the username and password from the peer router shall be validated, the authenticating party shall create and maintain a local user database. To configure the PPP CHAP authenticating party, use the following command at interface configuration mode:

Command	Function
Qtech(config-if)# **ppp authentication chap [callin]**	Enable the PPP authentication and specify the PPP CHAP authentication method.
Qtech(config-if)# **no ppp authentication chap**	Disable the PPP CHAP authentication.
Qtech(config)# **username** *username* **password {0|7}** *password*	Create the user database record.

The authenticating party has the username and related password configured in the user database, where the username is the PPP hostname of the peer router (the authenticated party).

Note

The Callin is an optional command option. With it configured, the CHAP authentication is not initiated unless the peer router (authenticated party) dials to connect the network in dialup mode. For the PPP connection that is set up because the local router dials out, the CHAP authentication is not initiated. Therefore, this command does not affect the dedicated line PPP negotiation.

2.2.5 Configuring the PPP PAP Authenticated Party

The PAP authentication involves authenticating party and authenticated party. For the setting of PAP authenticated party for PPP, run the following commands:

Command	Function
Qtech(config-if)# **ppp pap sent-username** *username* **password {0|7}** *password*	Specify the username and password for PPP PAP authentication.
Qtech(config-if)# **no ppp pap sent-username**	Remove the PPP PAP authentication settings.

2.2.6 Configuring the PPP PAP Authenticating Party

The commands for setting the PPP PAP authenticating party are as follows:

Command	Function
Qtech(config-if)# **ppp authentication pap [callin]**	Configure the PPP PAP authenticating party
Qtech(config)# **username** *username* **password {0|7}** *password*	Create the user database record.

Note

The Callin is an optional command option. With it configured, the PAP authentication is not initiated unless the peer router (authenticated party) dials to connect the network via dialup mode. For the PPP connection that is set up because the local router dials out, the PAP authentication is not initiated. Therefore, this command does not affect the dedicated line PPP negotiation.

2.2.7 Configure the PPP Negotiation Parameters

During the PPP negotiation, both LCP and IPCP have timeout periods. Once the period expires, the LCP resends requests. This period can be set by using this command to coordinate the negotiation time in the interconnection with heterogeneous devices.

Command	Function
Qtech(config-if)#**ppp negotiation-timeout** *seconds*	Configure the PPP LCP negotiation time.
Qtech(config-if)#**no ppp negotiation-timeout**	Restore the PPP negotiation time to the default.

2.2.8 Configuring Sender of PPP LCP Extended Configuration Option

The sender of the PPP LCP configuration option actively adds the extended configuration option to LCP configuration request packets. The IMSI number, the serial number (SN) of the local router, or the MAC address of the local router is sent to the peer end by being carried in the extended configuration option. Run the following command in interface configuration mode to configure the sender of the PPP LCP extended configuration option:

Command	Function
Qtech(config-if)#**ppp lcp send-option {imsi|serial-number|mac-address}**	Sends the LCP extended configuration option carrying the IMSI number, the SN, or the MAC address.

Note

Run the **ppp lcp send-option imsi** command to send the LCP extended configuration option carrying the IMSI number. Run the **ppp lcp send-option serial-number** command to send the LCP extended configuration option carrying the SN. Run the **ppp lcp send-option mac-address** command to send the LCP extended configuration option carrying the MAC address.

2.2.9 Configuring Receiver of PPP LCP Extended Configuration Option

The receiver of the PPP LCP extended configuration option needs to identify the PPP LCP extended configuration option sent from the remote router and send the information in the extended configuration option to the AAA server. Run the following command in interface configuration mode to configure the receiver of the PPP LCP extended configuration option:

Command	Function
Qtech(config-if)#**ppp lcp accept-option**	Identifies the PPP LCP extended configuration option and sends the information in the extended configuration option to the AAA server.

Note

Run the **ppp lcp accept-option** command to identify the PPP LCP extended configuration option carrying IMSI number. Run the **ppp lcp accept-option** command to identify the PPP LCP extended configuration option carrying the SN. Run the **ppp lcp accpet-option** command to identify the PPP LCP extended configuration option carrying the MAC address. The preceding command can also send the information in the extended configuration option to the AAA server if the AAA function is enabled.

In addition to the **ppp lcp accept-option** command, run the **force-local-lcp** command on the LNS device to transmit the IMSI, the SN, or the MAC address via the PPP LCP extended configuration option. In addition, the functions must be normal to ensure that the IMSI/MAC/SN extended configuration option is identified.

The LAC device of the operator may not support LCP re-negotiation and the configuration of the **force-local-lcp** command will result in a PPP negotiation failure. As a result, the IMSI/MAC/SN authentication function is unavailable.

2.2.10 Configuring Function of Accepting/Rejecting/Ignoring Received ACFC Negotiation Requests

During PPP link negotiation, run the following command in interface configuration mode to determine whether to accept the Address-and-Control-Field-Compression (ACFC) negotiation request sent from the peer end:

Command	Function
Qtech(config-if)#**ppp acfc remote** {**apply**|**reject**|**ignore**}	Configures how the local router processes the PPP configuration request packet that carries the ACFC option and that is sent from the remote device.

Note

Run the **ppp acfc remote apply** command to accept ACFC negotiation from the peer end. That is, ACFC is enabled for PPP frames from the peer end, but is enabled or disabled for PPP frames from the local end based on the interface type.
Run the **ppp acfc remote reject** command to reject ACFC negotiation from the peer end.
Run the **ppp acfc remote ignore** command to ignore ACFC negotiation from the peer end . That is, ACFC can be enabled or disabled for PPP frames from the peer end, but is disabled for PPP frames from the local end.
If the **ppp acfc remote** command conflicts with the **ppp acfc local** command, the later configured command shall prevail.

2.2.11 Configuring Function of Initiating/Forbidding ACFC Option

During PPP link negotiation, run the following command in interface configuration mode to determine whether to initiate ACFC negotiation from the local end:

Command	Function
Qtech(config-if)#**ppp acfc local** {**request**|**forbid**}	Configures how the local router processes the ACFC option in the to-be-sent PPP configuration request.

Note

Run the **ppp acfc local request** command to initiate ACFC negotiation on the local end, that is, the PPP LCP configuration request packet to be sent from the local end carries the ACFC option.
Run the **ppp acfc local forbid** command to forbid ACFC negotiation on the local end, that is, the PPP LCP configuration request packet to be sent from the local end does not carry the ACFC option and the configuration request packet that carries the ACFC option and that is sent from the peer end is rejected.
If the **ppp acfc local** command conflicts with the **ppp acfc remote** command, the later configured command shall prevail.

2.2.12 Configuring Function of Accepting/Rejecting/Ignoring Received PFC Negotiation Requests

During PPP link negotiation, run the following command in interface configuration mode to determine whether to accept the protocol field compression (PFC) negotiation request sent from the peer end:

Command	Function
Qtech(config-if)#**ppp pfc remote** {**apply**|**reject**|**ignore**}	Configures how the local router processes the PPP configuration request packet that carries the PFC option and that is sent from the remote device.

Note

Run the **ppp pfc remote apply** command to accept PFC negotiation from the peer end. That is, PFC is enabled for PPP frames form the peer end, but is enabled or disabled for PPP frames from the local end based on the interface type.
Run the **ppp pfc remote reject** command to reject PFC negotiation from the peer end.
Run the **ppp pfc remote ignore** command to ignore PFC negotiation from the peer end. That is, PFC can be enabled or disabled for PPP frames from the peer end, but is disabled for PPP frames from the local end.
If the **ppp pfc remote** command conflicts with the **ppp pfc local** command, the last configured command shall prevail.

2.2.13 Configuring Function of Initiating/Forbidding PFC Option

During PPP link negotiation, run the following command in interface configuration mode to determine whether to initiate PFC negotiation from the local end:

Command	Function
Qtech(config-if)#**ppp pfc local** {**request**|**forbid**}	Configures how the local router processes the PFC option in the to-be-sent PPP configuration request.

Note

Run the **ppp pfc local request** command to initiate PFC negotiation on the local end, that is, the PPP LCP configuration request packet to be sent from the local end carries the PFC option.
Run the **ppp pfc local forbid** command to forbid PFC negotiation on the local end, that is, the PPP LCP configuration request packet to be sent from the local end does not carry the PFC option and the configuration request packet that carries the PFC option and that is sent from the peer end is rejected.
If the **ppp pfc local** command conflicts with the **ppp pfc remote** command, the last configured command shall prevail.

2.3 MP configuration

2.3.1 Configuring MP on the Dialer Interface

2.3.1.1 MP Configuration Task List

The MP can be implemented by configuring the rotary-group on the physical interface layer and binding the dialer logical interface. This chapter describes only the multilink PPP binding the dialer interface and the synchronous serial interface. For the configuration of the dialup multilink of asynchronous serial interface, see DDR Configuration Guide. The list of configuration tasks for the multilink of Dialer interface binding synchronous serial interface is as follows:

- Configuring the synchronous serial interface
- Encapsulating PPP link protocol
- Configuring dialer in-band
- Configuring rotary-group
- The configuration of the rotary-group needs the DDR. So, if the **dialer in-band** has not been configured in advance, it will be automatically configured in configuring **dialer rotary-group**.
- Creating the logical interface dialer
- When you create the logical interface dialer, the physical interface with the rotary group configured must be existent, which maintains the binding by consistency of the rotary group number and the logical interface dialer number. If the logical interface is to be deleted, it is required to delete the rotary group on the physical interface first.
- Configuring the ppp multilink
- Configuring the dialup filtering rule

2.3.1.2 Configuring the synchronous serial interface

To configure the synchronous serial interface for multilink binding:

Command	Function
Qtech(config)# **interface serial** *interface-number*	Enter the configuration mode of the specified serial interface.

2.3.1.3 Encapsulating PPP link protocol

The multilink PPP is a PPP at first. So, it is required to encapsulate the PPP link protocol first no matter whether it is on a physical interface or a logical interface.

Command	Function
Qtech(config-if)#**encapsulation ppp**	Encapsulate the PPP link protocol.
Qtech(config-if)#**no encapsulation ppp**	Cancel the encapsulation of the PPP link protocol.

2.3.1.4 Configuring dialer in-band

To configure the multilink, it is required to configure the DDR on the serial interface configuration layer at first by using the following command, which is the prerequisite for configuring rotary-group:

Command	Function
Qtech(config-if)#**dialer in-band**	Set the DDR configuration.
Qtech(config-if)#**no dialer in-band**	Cancel the DDR configuration.

2.3.1.5 Configuring rotary-group

This command binds the physical interface to the rotary group of logical interface to enable the multilink binding.

Command	Function
Qtech(config-if)#**dialer rotary-group** *group-number*	Set the number of the rotary group.
Qtech(config-if)#**no dialer rotary-group** *group-number*	Delete the rotary group.

Note

The configuration of the rotary-group needs the DDR. So, if the **dialer in-band** has not been configured in advance, it will be automatically configured in configuring **dialer rotary-group**.

2.3.1.6 Creating the logical interface dialer

When the rotary group is set, it is necessary to create the logical interface dialer that individual physical interfaces are bound to. The interface number must be the same as the number of the rotary group. After the logical interface dialer is created, it enters into the dialer logical interface configuration layer. Accordingly, it is required to encapsulate the PPP link protocol, configure the PPP multilink, configure the dialup filtering rule, and so on.

Command	Function
Qtech(config)#**interface dialer** *group-number*	Create the logical interface dialer.
Qtech(config)#**no interface dialer** *group-number*	Delete the logical interface dialer.

Note

When you create the logical interface dialer, the physical interface with the rotary group configured must be existent, which maintains the binding by consistency of the rotary group number and the logical interface dialer number. If the logical interface is to be deleted, it is required to delete the rotary group on the physical interface first.

2.3.1.7 Configuring the ppp multilink

To set the multilink PPP, it is required to configure the **PPP multilink** command on the logical interface to specify the logical interface to use the multilink negotiation mode.

Command	Function
Qtech(config-if)#**ppp multilink**	Set the multilink negotiation mode.
Qtech(config-if)#**no ppp multilink**	Cancel the setting of the PPP multilink negotiation mode.

2.3.1.8 Configuring the dialup filtering rule

On the logical interface, it is required to configure the dialup filtering rule. This rule is powerful enough to use with the ACL. Here is the simplified description for the functions of the **dialer-list**.

Command	Function
Qtech(config-if)#**dialer-group** *group-number*	Set the dialer group.
Qtech(config)#**dialer-list** *group-number* **protocol ip permit**	Set the common dialer group list allowing the access to IP packets.

2.3.2 Configuring MP on the Multilink Interface

2.3.2.1 MP Configuration Task List

The MP can be implemented by configuring the multilink group on the physical interface layer and binding the multilink logical interface. This chapter describes only the multilink PPP of the multilink interface binding the synchronous serial interface. The list of configuration tasks of multilink interface binding synchronous serial interface is as follows:

- Creating the logical interface multilink
- Configuring the synchronous serial interface
- Encapsulating PPP link protocol
- Configuring the ppp multilink
- Configuring the ppp multilink group

2.3.2.2 Creating the logical interface multilink

To configure the MP binding of the multilink interface, create the logical interface multilink binding individual physical interfaces. After the logical interface multilink is created, it enters into the multilink logical interface configuration layer, where the PPP encapsulation and MP are enabled by default.

Command	Function
Qtech(config)#**interface multilink** *group-number*	Create the logical interface multilink.
Qtech(config)#**no interface multilink** *group-number*	Delete the logical interface multilink.

⚠ Caution Up to 72 multilink interfaces are supported.

2.3.2.3 Configuring the synchronous serial interface

To configure the synchronous serial interface for multilink binding, execute the following command:

Command	Function
Qtech(config)# **interface serial** *interface-number*	Enter the specified serial interface configuration mode.

2.3.2.4 Encapsulating PPP link protocol

The multilink PPP is a PPP at first. So, it is required to encapsulate the PPP link protocol first on the synchronous serial interface.

Command	Function
Qtech(config-if)#**encapsulation ppp**	Encapsulate the PPP link protocol.
Qtech(config-if)#**no encapsulation ppp**	Remove the encapsulation of PPP link protocol.

2.3.2.5 Configuring the ppp multilink

To set the synchronous interface to use the multilink negotiation mode, execute the **PPP multilink** command on the synchronous serial interface.

Command	Function
Qtech(config-if)#**ppp multilink**	Set the multilink negotiation mode.
Qtech(config-if)#**no ppp multilink**	Remove the setting of the PPP multilink negotiation mode.

2.3.2.6 Configuring the ppp multilink group

To bind the synchronous serial interface to the group of logical interface for multilink binding, execute the following command.

Command	Function
Qtech(config-if)# **ppp multilink group** *group-number*	Set the number of the multilink group.
Qtech(config-if)#**no ppp multilink group** *group-number*	Remove the number of the multilink group.

Note

The parameter group-number configured here is the same as the multilink interface number in the creation of the multilink. When configuring the ppp multilink group, the multilink interface must exist accordingly. The physical interface uses the multilink group number and the logical interface number of multilink interface to maintain binding. If the logical interface is to be deleted, it is required to delete the multilink group on the physical interface first.

2.3.3 Configuring MP on the Virtual-Template Interface

2.3.3.1 MP Configuration Task List

The MP can be implemented by configuring the MP on the physical interface layer and binding the virtual template interface. This chapter describes only the multilink PPP of the virtual template interface binding the synchronous serial interface. For details of the virtual template, see VPN Configuration Guide. The list of configuration tasks for the virtual template interface binding synchronous serial interface is as follows:

- Creating the virtual template interface
- Creating the bounded virtual template interface
- For the Virtual-Template multilink binding, in the setup of the binding, a virtual access interface Virtual-Access is created automatically as the binding interface. This command specifies which virtual template copy configuration acts as the settings of the virtual access interface during the creation of the virtual access interface.
- Configuring the synchronous serial interface
- Encapsulating the PPP link protocol
- Configuring the ppp multilink

2.3.3.2 Creating the virtual template interface

To configure the MP in the Virtual-Template method, it is required to create the Virtual-Template interface. After the Virtual-Template interface is created, it enters into the virtual template interface configuration layer. Accordingly, it is required to encapsulate the PPP link protocol, configure the PPP multilink, configure the dialup filtering rule, and so on.

Command	Function
Qtech(config)#**interface virtual-template** *number*	Create/configure the specified virtual -template interface
Qtech(config)#**no interface virtual-template** *number*	Delete the specified virtual -template interface

2.3.3.3 Creating the bounded virtual template interface

After the virtual template interface is created, the **multilink virtual-template** command is used to specify which virtual template copy binds the interface parameters.

Command	Purpose
Qtech(config)# **multilink virtual-template** *number*	Specify the virtual template for the MP bundle interface to clone interface parameters

Command	Purpose
Qtech(config)# **no multilink virtual-template** *number*	Delete the virtual template for the MP bundle interface to clone interface parameters

Note

For the Virtual-Template multilink binding, in the setup of the binding, a virtual access interface Virtual-Access is created automatically as the binding interface. This command specifies which virtual template copy configuration acts as the settings of the virtual access interface during the creation of the virtual access interface.

2.3.3.4 Configuring the synchronous serial interface

To configure the synchronous serial interface for multilink binding:

Command	Function
Qtech(config)# **interface serial** *interface-number*	Enter the configuration mode of the specified serial interface

2.3.3.5 Encapsulating the PPP link protocol

The multilink PPP is a PPP at first. So, it is required to encapsulate the PPP link protocol first no matter whether it is on a synchronous serial interface or a virtual template interface.

Command	Function
Qtech(config-if)#**encapsulation ppp**	Encapsulate PPP link protocol
Qtech(config-if)#**no encapsulation ppp**	Cancel the encapsulation of PPP link protocol

2.3.3.6 Configuring the ppp multilink

To set the virtual template interface and physical interface to use the multilink negotiation mode, execute this command on the virtual template interface and synchronous interface.

Command	Function
Qtech(config-if)#**ppp multilink**	Set the multilink negotiation mode.
Qtech(config-if)#**no ppp multilink**	Remove the setting of the PPP multilink negotiation mode.

Note

It is not necessary to configure multilink group or rotary-group on the physical interface for virtual template-based binding. It only the **ppp multilink** command is configured on the physical interface but no configuration for which link group or dialup rotary group to belong to, the physical interface will belong to the multilink binding in virtual template mode.

2.4 PPP Monitoring and Maintenance

2.4.1 Showing the Protocol Interface Information

Run the following command to show the PPP protocol interface information, which is the first step to debug PPP:

Command	Function
Qtech#**show interface serial** *interface-number*	Show the information of the serial interface.

Take Serial1/0 as an example. The following information in printed after the command is entered:

```
serial 1/0 is UP  , line protocol is UP
Hardware is Infineon DSCC4 PEB20534 H-10 serial
Interface address is: 100.100.100.1/24
 MTU 1500 bytes, BW 2000 Kbit
 Encapsulation protocol is PPP, loopback not set
 Keepalive interval is 10 sec , set
 Carrier delay is 2 sec
 RXload is 1 ,Txload is 1
 LCP Open
 Open: ipcp
 Queueing strategy: WFQ
 5 minutes input rate 30 bits/sec, 0 packets/sec
 5 minutes output rate 30 bits/sec, 0 packets/sec
 49 packets input, 786 bytes, 0 no buffer
 Received 1 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
 47 packets output, 768 bytes, 0 underruns
 0 output errors, 0 collisions, 1 interface resets
 1 carrier transitions
    V35 DTE cable
 DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

First check the link status from the physical layer. The five signals (DCD, DSR, DTR, RTS, CTS) in the last row determine whether the serial is UP or not. This is the prerequisite for PPP Line Protocol UP.

Then, check whether the PPP negotiation is successful by checking whether the LCP status is UP and whether the IPCP status is UP. If yes for both, the line protocol is in the up status, and the link layer shall be available for communication.

Last, refer to the data receiving/transmitting conditions at the bottom layer. Packet Input and Output indicate the number of messages received and transmitted. If there is no interface reset, the message transmission is successful. If there is no number of drops in the Input Queue, it means all messages are received successfully.

2.4.2 PPP Debugging Information

In case of problem with the PPP link layer negotiation, run the following command to debug the PPP:

Command	Function
Qtech# **debug ppp packet**	Print message debug information during PPP communication
Qtech# **debug ppp negotiation**	Print negotiation debug information during PPP communication
Qtech# **debug ppp authentication**	Print authorization debug information during PPP communication

2.4.2.1 Packet debugging

In the privileged command layer, enter the **PPP Packet** debug command:

```
Qtech#debug ppp packet
PPP: serial 1/0 [S] LCP CONFREQ id 3 len 10
   MAGICNUMBER (6) 0x0 0x2b 0x39 0x1b
%LINK CHANGED: Interface serial 1/0, changed state to up
PPP: serial 1/0 [R] LCP CONFREQ id 6 len 10
   MAGICNUMBER (6) 0x29 0xbd 0xea 0xeb
PPP: serial 1/0 [S] LCP CONFACK id 6 len 10
   MAGICNUMBER (6) 0x29 0xbd 0xea 0xeb
PPP: serial 1/0 [R] LCP CONFACK id 3 len 10
   MAGICNUMBER (6) 0x0 0x2b 0x39 0x1b
PPP: serial 1/0 LCP up
PPP: serial 1/0 PPP up.
PPP: serial 1/0 [S] IPCP CONFREQ(2) id 10 len 2
   Address (6) 0x64 0x64 0x64 0x1
PPP: serial 1/0 [R] IPCP CONFREQ(3) id 10 len 2
   Address (6) 0x64 0x64 0x64 0x2
PPP: serial 1/0 [S] IPCP CONFACK(3) id 10 len 2
   Address (6) 0x64 0x64 0x64 0x2
PPP: serial 1/0 [S] LCP PROTREJ id 4 len 10 protocol = 0x82070103
PPP: serial 1/0 [R] IPCP CONFACK(2) id 10 len 2
   Address (6) 0x64 0x64 0x64 0x1
%LINE PROTOCOL CHANGE: Interface serial 1/0, changed state to UP
Qtech#
PPP: serial 1/0 [S] LCP ECHOREQ id 1 len 12 magic 0x2b391b
```

The above debugging information is for all messages from the start of the PPP negotiation to the Line Protocol Up, without authentication. Pay attention to the bolded debug information: Both routers send the LCP CONFREQ to each other and then respond with the LCP CONFACK. Then it enters into the IPCP negotiation. Also pay attention to the bolded contents. Both routers send IPCP CONFREQ to each other and attach their own IP addresses, and then send the IPCP CONFACK response with the peer IP address attached after the IPCP CONFREQ request is received. Now the PPP negotiation of the interface succeeds.

2.4.2.2 PPP negotiation debugging information

The negotiation debugging information is used for the debugging trace purpose in negotiating the PPP parameters. For example, in the CHAP authentication of PPP, the **debug ppp negotiation** command can trace the following parameter negotiation information:

```
Qtech#
PPP: serial 1/0 reset lcp options
PPP: serial 1/0 sending OPCODE_CONFREQ, type = 5 (LCP_MAGICNUMBER), value =
0x10a5df
%LINK CHANGED: Interface serial 1/0, changed state to up
LCP: received config , type = 5 (MAGICNUMBER) value = 0x29cbca60 acked
PPP: serial 1/0 OPCODE_CONFACK received, type = 5 (LCP_MAGICNUMBER), value =
0x10a5df
PPP: serial 1/0 state = Acksent ppp_recv_confack(0xc021): rcvd id 5
PPP: serial 1/0 reset ipcp options
IPCP: serial 1/0 sending OPCODE_CONFREQ, type = 3 (IPCP_ADDRESS), Address =
100.100.100.1
IPCP: serial 1/0 received ADDR : her address 100.100.100.2 (ACK)
IPCP: ipcp_do_req_cb: returning OPCODE_CONFACK.
IPCP: serial 1/0 OPCODE_CONFACK received, type = 3 (IPCP_ADDRESS), Address =
100.100.100.1
PPP: serial 1/0 state = Acksent ppp_recv_confack(0x8021): rcvd id 3
IPCP: serial 1/0 install route to 100.100.100.2
%LINE PROTOCOL CHANGE: Interface serial 1/0, changed state to UP
```

Pay attention to the bolded contents, which are the options for the LCP and IPCP negotiation parameters.

2.4.2.3 PPP authentication debugging information

The debug of the authentication information is used to trace the PPP authentication. With PAP as an example, the PAP authenticating party prints the following debugging information:

```
PPP: serial 1/0 PAP authenticating peer DRO36
PPP: serial 1/0 Remote passed PAP authentication sending Auth-Ack to peer.
PPP: serial 1/0 lcp authentication OK#
```

The CHAP authentication party prints the following information when the sent CHAP password is wrong:

```
PPP: serial 1/0 recv CHAP challenge from Router
PPP: serial 1/0 remote router failed CHAP authentication
PPP: serial 1/0 Remote msg is: Authentication failure
```

2.5 Typical PPP Configuration Examples

2.5.1 **PPP PAP Authentication Example**

The example below shows a PAP configuration, username Qtech, password Router, authenticating party IP address 1.1.1.1/24, authenticated party IP address 1.1.1.2/24, username and password configured same as the authentication method. Router A is the authenticated party and Router B is the authenticating party.

Router A:

```
Qtech#config terminal
Qtech(config)#interface Serial1/0
```

# Configure the IP address

```
Qtech(config-if)#ip address 1.1.1.2 255.255.255.0
```

# Encapsulate PPP protocol

```
Qtech(config-if)#encapsulation ppp
```

# Configure the username and password for PAP authentication.

```
Qtech(config-if)#ppp pap sent-username Qtech password 0 Router
```

Router B:

```
Qtech#config terminal
Qtech(config)#username Qtech password 0 Router
Qtech(config)#interface Serial1/0
```

# Configure the IP address

```
Qtech(config-if)#ip address 1.1.1.1 255.255.255.0
```

# Encapsulate PPP protocol

```
Qtech(config-if)#encapsulation ppp
```

# Specify the PPP authentication mode

```
Qtech(config-if)#ppp authentication pap
```

2.5.2 PPP CHAP Authentication Example

The example below shows a PPP CHAP authentication configuration, where the Router A is the authenticating party, IP address is 1.1.1.1/24, hostname is RouterA, password is Router, and the user list contains the hostname RouterB; the Router B is the authenticating party, IP address is 1.1.1.2/24, hostname is RouterB and the password sent is Router.

Router A:

```
Qtech#config terminal
```

# Set the hostname

```
Qtech(config)#hostname RouterA
```

# Set the username and password list

```
RouterA(config)#username RouterB password 0 Router
RouterA(config)#username RouterC password 0 Router
RouterA(config)#interface serial1/0
```

# Encapsulate protocol

```
RouterA(config-if)#encap ppp
```

# Set IP address

```
RouterA(config-if)#ip address 1.1.1.1 255.255.255.0
```

# Specify the PPP chap authentication mode

```
RouterA(config-if)#ppp authentication chap
```

Router B:

```
Qtech#config terminal
```

# Set the hostname

```
Qtech(config)#hostname RouterB
```

# Use the peer hostname as the username, and the password is the same as that configured on the peer router.

```
RouterB(config)#username RouterA password 0 Router
RouterB(config)#interface serial1/0
```

# Encapsulate protocol

```
RouterB(config-if)#encap ppp
```

# Set IP address

```
RouterB(config-if)#ip address 1.1.1.2 255.255.255.0
```

To keep the administration hostname, the hostname configured for the CHAP authentication can be configured by using the **chap hostname *hostname*** command. In the above example, the Router B as the authenticated party uses the default hostname, and the host for the CHAP authentication is RouterB.

Router B:

```
Qtech#config terminal
Qtech(config)#
```

# Use the peer hostname as the username, and the password is the same as that configured on the peer router.

```
R(config)#username RouterA password 0 Router
Qtech(config)#interface serial1/0
```

# Encapsulate protocol

```
Qtech(config-if)#encap ppp
```

# Set IP address

```
Qtech(config-if)#ip address 1.1.1.2 255.255.255.0
```

# Set the local CHAP authentication hostname

```
Qtech(config-if)#ppp chap hostname RouterB
```

2.5.3 PPP MS-CHAP Authentication

The following example describes the PPP MS-CHAP authentication configuration. Router A is the authentication party, with the IP address being 1.1.1.1/24, host name being RouterA, and password being Router. The user list of Router A includes the host name of Router B. Router B is the authenticated party, with IP address being 1.1.1.2/24, host name being RouterB, and password being Router.

Router A:

```
Qtech# config terminal
```

#Set a host name.

```
Qtech(config)# hostname RouterA
```

#Set a username and password list.

```
RouterA(config)#username RouterB password 0 Router
RouterA(config)#username RouterC password 0 Router
RouterA(config)#interface serial 1/0
```

#Set the encapsulation protocol.

```
RouterA(config-if)# encap ppp
```

#Set an IP address.

```
RouterA(config-if)# ip address 1.1.1.1 255.255.255.0
```

#Set the PPP MS-CHAP authentication mode.

```
RouterA(config-if)# ppp authentication ms-chap
```

Router B:

```
Qtech# config terminal
```

#Set a host name.

```
Qtech(config)# hostname RouterB
```

#Set the host name of Router A as the username, and set the password to be the same as that of Router A.

```
RouterB(config)# username RouterA password 0 Router
RouterB(config)# interface serial 1/0
```

#Set the encapsulation protocol.

```
RouterB(config-if)# encap ppp
```

#Set an IP address.

```
RouterB(config-if)# ip address 1.1.1.2 255.255.255.0
```

To reserve the host name, run the **ppp chap hostname** *hostname* command to specify the local host name used for MS-CHAP authentication. In the preceding example, the authenticated party Router B uses the default host name RouterB, which is used for MS-CHAP authentication.

Router B:

```
Qtech# config terminal
Qtech(config)#
```

#Set the host name of Router A as the username, and set the password to be the same as that of Router A.

```
Qtech  (config)# username RouterA password 0 Router
Qtech(config)# interface serial 1/0
```

#Set the encapsulation protocol.

```
Qtech(config-if)# encap ppp
```

#Set an IP address.

```
Qtech(config-if)# ip address 1.1.1.2 255.255.255.0
```

#Set the host name for local MS-CHAP authentication.

```
Qtech(config-if)# ppp chap hostname RouterB
```

2.5.4 PPP MS-CHAP-V2 Authentication

The following example describes the PPP MS-CHAP-V2 authentication configuration. Router A is the authentication party, with the IP address being 1.1.1.1/24, host name being RouterA, and password being Router. The user list of Router A includes the host name of Router B. Router B is the authenticated party, with IP address being 1.1.1.2/24, host name being RouterB, and password being Router.

Router A:

```
Qtech# config terminal
```

#Set a host name.

```
Qtech(config)# hostname RouterA
```

#Set a username and password list.

```
RouterA(config)#username RouterB password 0 Router
RouterA(config)#username RouterC password 0 Router
RouterA(config)#interface serial 1/0
```

#Set the encapsulation protocol.

```
RouterA(config-if)# encap ppp
```

#Set an IP address.

```
RouterA(config-if)# ip address 1.1.1.1 255.255.255.0
```

#Set the PPP MS-CHAP-V2 authentication mode.

```
RouterA(config-if)# ppp authentication ms-chap-v2
```

Router B:

```
Qtech# config terminal
```

#Set a host name.

```
Qtech(config)# hostname RouterB
```

#Set the host name of Router A as the username, and set the password to be the same as that of Router A.

```
RouterB(config)# username RouterA password 0 Router
RouterB(config)# interface serial 1/0
```

#Set the encapsulation protocol.

```
RouterB(config-if)# encap ppp
```

#Set an IP address.

```
RouterB(config-if)# ip address 1.1.1.2 255.255.255.0
```

To reserve the host name, run the **ppp chap hostname** *hostname* command to specify the local host name used for MS-CHAP-V2 authentication. In the preceding example, the authenticated party Router B uses the default host name RouterB, which is used for MS-CHAP-V2 authentication.

Router B:

```
Qtech# config terminal
Qtech(config)#
```

#Set the host name of Router A as the username, and set the password to be the same as that of Router A.

```
Qtech (config)# username RouterA password 0 Router
Qtech(config)# interface serial 1/0
```

#Set the encapsulation protocol.

```
Qtech(config-if)# encap ppp
```

#Set an IP address.

```
Qtech(config-if)# ip address 1.1.1.2 255.255.255.0
```

#Set the host name for local MS-CHAP-V2 authentication.

```
Qtech(config-if)# ppp chap hostname RouterB
```

2.5.5 MP Configuration Example

The example below shows a multilink configuration, where two synchronous interfaces serial1/0 and serial1/1 are bound to the logical interface dialer 1 to implement the Multilink PPP.

# Create the loopback interface and use its IP address as the IP address of the dialer logical interface

```
interface Loopback0
ip address 192.168.20.2 255.255.255.0
```

# Configure DDR on the physical interfaces serial1/0 and serial1/1, and specify the rotary group number (1 in this example)

```
interface Serial1/0
no ip address
encapsulation ppp
dialer in-band
dialer rotary-group 1
#
interface Serial1/1
no ip address
encapsulation ppp
dialer in-band
dialer rotary-group 1
```

# Create the dialer 1 logical interface and borrow the IP address of loopback0, set the dialer group, and specify the multilink ppp negotiation method.

```
interface Dialer1
ip unnumbered Loopback0
encapsulation ppp
dialer-group 1
ppp multilink
#
dialer-list 1 protocol ip permit
```

The example below uses two synchronous interfaces serial1/0 and serial1/1 are bound to the logical interface multilink 1 to implement the Multilink PPP.

# Create the loopback interface and use its IP address as the IP address of the multilink logical interface

```
interface Loopback0
  ip address 192.168.20.1 255.255.255.0
```

# Configure ppp multilink on the physical interfaces serial1/0 and serial1/1, and specify the multilink group number 1.

```
interface Serial 1/0
  no ip address
  encapsulation ppp
  ppp multilink
  multilink-group 1
interface Serial 1/1
  no ip address
  encapsulation ppp
  ppp multilink
  multilink-group 1
```

# Create the multilink 1 logical interface and borrow the IP address of loopback0.

```
interface multilink 1
  ip unnumbered Loopback0
  encapsulation ppp
  ppp multilink
```

The example below uses two synchronous interfaces serial1/0 and serial1/1 are bound to the virtual template interface to implement the Multilink PPP.

# Create the loopback interface and use its IP address as the IP address of the virtual template interface

```
interface Loopback0
  ip address 192.168.20.1 255.255.255.0
```

# Configure the PPP multilink on physical interfaces serial1/0 and serial1/1

```
interface Serial 1/0
  no ip address
  encapsulation ppp
  ppp multilink
interface Serial 1/1
```

```
  no ip address
  encapsulation ppp
  ppp multilink
```

# Create the virtual-template 1 interface and borrow the IP address of loopback0.

```
interface virtual-template 1
  ip unnumbered Loopback0
  encapsulation ppp
  ppp multilink
multilink virtual-template 1
```

# Specify copying parameters from virtual-template 1, to establish the binding from virtual-access interface to synchronous interface.

2.5.6 Configuration of Sender/Receiver of LCP Extended Configuration Option

In the following example, Router A is configured as the sender of the PPP LCP extended configuration option, so as to send the SN of router A to Router B through the LCP extended configuration option; Router B is configured as the receiver of the PPP LCP extended configuration option, identifies the LCP extended configuration option that carries the SN and that is sent from Router A, and then sends the information in the extended configuration option to the AAA server for authentication.

Router A:

```
Qtech# config terminal
```

#Set a host name.

```
Qtech(config)# hostname RouterA
```

#Set the encapsulation protocol.

```
RouterA(config-if)# encap ppp
```

#Set an IP address.

```
RouterA(config-if)# ip address 1.1.1.1 255.255.255.0
```

#Set the sender of the PPP LCP extended configuration option.

```
RouterA(config-if)#ppp lcp send-option serial-number
```

Router B:

```
Qtech# config terminal
```

#Set a host name.

```
Qtech(config)# hostname RouterB
```

#Set the encapsulation protocol.

```
RouterB(config-if)# encap ppp
```

#Set an IP address.

```
RouterB(config-if)# ip address 1.1.1.2 255.255.255.0
```

#Set the receiver of the PPP LCP extended configuration option.

```
RouterB(config-if)#ppp lcp accept-option
```

2.5.7 ACFC Option Processing

In the following example, the interface Serial 1/3 of Router A is configured to actively send the ACFC option during PPP LCP negotiation, enable ACFC, and reply with an ACK response to the PPP LCP configuration request packet that carries the ACFC option and that is sent from the peer end.

Router A:

```
Qtech# config terminal
```

#Set a host name.

```
Qtech(config)# hostname RouterA
```

#Enter the interface configuration mode.

```
Qtech(config)# interface Serial 1/3
```

#Set the encapsulation protocol.

```
RouterA(config-if)# encap ppp
```

#Set an IP address.

```
RouterA(config-if)# ip address 1.1.1.1 255.255.255.0
```

#Configure the function of actively sending the ACFC option.

```
RouterA(config-if)#ppp acfc local request
```

#Configure the function of accepting the PPP LCP configuration request packet that carries the ACFC option.

```
RouterA(config-if)#ppp acfc remote apply
```

2.5.8 PFC Option Processing

In the following example, the interface Serial 1/3 of Router A is configured to actively send the PFC option during PPP LCP negotiation, enable PFC, and reply with an ACK response to the PPP LCP configuration request packet that carries the PFC option and that is sent from the peer end.

Router A:

```
Qtech# config terminal
```

#Set a host name.

```
Qtech(config)# hostname RouterA
```

#Enter the interface configuration mode.

```
Qtech(config)# interface Serial 1/3
```

#Set the encapsulation protocol.

```
RouterA(config-if)# encap ppp
```

#Set an IP address.

```
RouterA(config-if)# ip address 1.1.1.1 255.255.255.0
```

#Configure the function of actively sending the PFC option.

```
RouterA(config-if)#ppp pfc local request
```

#Configure the function of accepting the PPP LCP configuration request packet that carries the PFC option.

```
RouterA(config-if)#ppp pfc remote apply
```

2.6 PPP Troubleshooting

First, use the **show interface serial** *slot-number/interface-number* command to check the interface status. A synchronous interface may have four statuses. Take the serial 1/0 as an example;

Status display	Fault description
serial 1/0 is administratively down, line protocol is down	The interface is shut down by someone.
serial 1/0 is down, line protocol is down	The interface is not activated, or the physical interface has not turned Up
Serial 1/0 is up, line protocol is up	The interface is available for data transmission.
serial 1/0 is up, line protocol is down	The interface has been activated but the link negotiation fails.

2.6.1 Interface Cannot be Up

Firstly: Remove the fault of manual shutdown of the interface.

Secondly: Check the physical layer causes. Run the show interface serial1/0 command to check the interface status. All the physical layer parameters (DCD, DTR, DSR, CTS, RTS) shall be up. If some one is down, verify whether the related V.35 or V.24 cable has problem or not.

Finally: If the cable of the interface is DTE (the connector connected with the line device is a fame-end cable) but the DCD is down, verify whether the line handshake of the Modem connected with the cable is successfully. If so, the DCD or LINE indicator on the Modem shall be always on.

2.6.2 Link Protocol Cannot be Up

The interface is up is the prerequisite for Line Protocol Up. Therefore, first remove the interface down fault in troubleshooting the fault of the link protocol cannot be up. Then, verify the data receiving/transmitting of the link layer: Run the **show interface serial** ***slot-number/interface-number*** command to note the numbers of Packet Input and Packet Output. If there is no Input message, the peer router may be shut down or the transmission of the peer router has problem.

Run the **Clear Count serial** ***slot-number/interface-number*** command for a period and note the number of Interface reset. If any, it indicates the local router transmission has problem.

To prevent the loopback problem with the line: Run the **show interface serial** ***slot-number/interface-number*** command to check whether there is the prompt "Loopback is set". Use the **debug PPP packet** command to check whether the PPP negotiation matches the reply of the peer router Magic Number. If yes, the line may be in the loopback status, causing the link cannot be up. It may also possible that the link is up but the peer cannot be pinged through.

If the data transmission/receiving of the line is normal but the protocol settings of the line do not match, such as HDLC protocol set for the peer router, run the **debug PPP packet** command to view the prompt for protocol type. If so, the line protocol cannot be up.

The fault that the link protocol cannot be up is related with the negotiation parameters. If the line negotiation needs the CHAP or PAP authentication, it is necessary to ensure correct username and password, which can be verified by using the **debug ppp packet** or **debug ppp negotiation** command.

2.6.3 Link is Up but Ping Failed

The status of link up is based on the successful LCP negotiation. If the interface has been configured with an IP address, the Line protocol may also be up but there is no prompt "IPCP Open". As a result, if the IP address of the peer WAN interface cannot be pinged through, remove the fault of the IPCP negotiation failure. If the peer WAN interface can be pinged through but the IP addresses inside the peer LAN cannot be pinged through, troubleshoot from the routing table first. For the related routing configuration, see IP Routing Protocol Configuration Guide.

3 DLDP CONFIGURATION

3.1 Overview

Based on the SDH platform, the MSTP supports access, processing, and transmission of multiple services such as TDM, ATM, and Ethernet and provides multi-service nodes with a the unified network management system. The Ethernet access mode is commonly used at user access points. However, link keep-alive protocols are not available on Ethernet, causing exceptions where the link protocol status is normal whereas lines are disonnected when MSTP networks are accessed in Ethernet access mode. In this case, route convergence is slow and faults are more difficult to locate.

The major procedure for device link detection falls into the following stages:

2) Initialization

When DLDP is enabled on the interface, the status of DLDP changes to the initialization state, and then an ARP request is sent to obtain the MAC address of the peer device. If DLDP cannot obtain the MAC address of the peer device, DLDP remains in the initialization stage. In this case, if the DLDP function is disabled, the DLDP status changes to deleted. After the MAC address of the peer device is obtained, the DLDP status changes to link succeeded.

3) Link succeeded status

In this state, a DLDP link detection request can be sent to detect line connectivity. If a DLDP response is received, the corresponding interface is marked as UP. If no response is received, requests are sent until the number of requests exceeds the maximum allowed number of requests. In this case, the link is marked as failed and the DLDP status changes to initialization. If this function is deleted during this process, the DLDP status changes to deleted.

4) Deleted status

In the deleted state, the interface status is not analyzed by the link detection function and remains consistent with the physical channel status.

3.2 Configuring Device Link Detection

3.2.1.1 Task List

3.2.1.2 Configuring the Ethernet Link Detection Function

This command can be configured on the Ethernet port only. By default, this function is disabled. To activate this function, run the following command:

Command	Function
Qtech(config-if)#**dldp** *ip [nexthopip]*	Activates the link detection protocol.

Note

1. This function is implemented using ICMP ECHO packets. The ICMP response function needs to be enabled on the peer device.
2. The precondition for enabling this function is that the interface is in the UP state.
3. After this function is enabled, the IP address of the interface cannot be modified when the interface is in the down state .
4. In the case of detection across network segments, the next-hop IP address needs to be configured. For example, If the local interface IP address is 10.1.1.1 and 30.1.1.1 needs to be detected through the 20.1.1.2 gateway, the next-hop IP address 20.1.1.2 needs to be configured.

3.2.1.3 Configuring the Interval

Setting heartbeat intervals can change the frequency of handshake packet sending for link detection.

Command	Function

Qtech(config-if)# **dldp** ip **interval** *val*	Sets the interval for device link detection.

3.2.1.4 Configuring Retry Times

Command	Function
Qtech(config-if)# **dldp** ip **retry** *val*	Sets the threshold of error times during device link detection.

3.2.1.5 Configuring Resume Times

Command	Function
Qtech(config-if)# **dldp** ip **resume** *val*	Sets the resumption threshold of the device link. The threshold indicates the times for receiving continuous DLDP detection packet responses before the link status changes from DOWN to UP. The resumption time is related to the interval for sending link detection packets set by running the **dldp ip interval** command. The line resumption time can be calculated using the following formula: Line resumption time = Resume times x Time configured by using the **dldp ip interval** command.

Note

This function is used to avoid oscillation of device links. For example, if link status changes between connnected and disonnected during the link status detection using the **ping** command, continuous oscillation occurs on the link (Link status changes continuously between UP and DOWN or ARP is continuously switched.). This problem can be avoided by setting a greater resume value. Link status changes from DOWN to UP only when the number of detection packet responses received by the link reached the threshold set by using the **resume** command.

3.2.1.6 Clearing the Records of the Times When DLDP Status Changes Between UP and DOWN

Command	Function
Qtech(config-if)# **clear-dldp***[all] [ip [nexthopip]]*	Qtech routers can record the times when DLDP protocol status changes between UP and DOWN. The **clear-dldp** command can be used to clear the recorded times and start the new recording.

Note

1. The **clear-dldp all** command can be used to clear the recorded times when DLDP status changes between UP and DOWN on an interface within a period of time and to start the new recording from 0.
2. The **clear-dldp ip [nexthopip]** command can be used to clear the recorded times when link status changes between UP and DOWN on a specified interface within a period of time and to start the new recording from 0.

3.2.1.7 Checking the Times When DLDP Status Changes Between UP and DOWN Within a Period of Time

Command	Function
Qtech(config-if)# **show dldp** interface *[ ] [FastEthernet/GigabitEthernet number]*	Displays the times when DLDP status changes between UP and DOWN within a period of time.

Note

1. The **show dldp interface** command can be used to check the times when DLDP status changes between UP and DOWN on all interfaces and view the time when the recording starts.
2. The **show dldp interface FastEthernet/GigabitEthernet number** command can be used to check the recorded times when protocol status changes between UP and DOWN on an Ethernet interface and view the time when the recording starts.

4 BFD CONFIGURATION

4.1 Understanding BFD

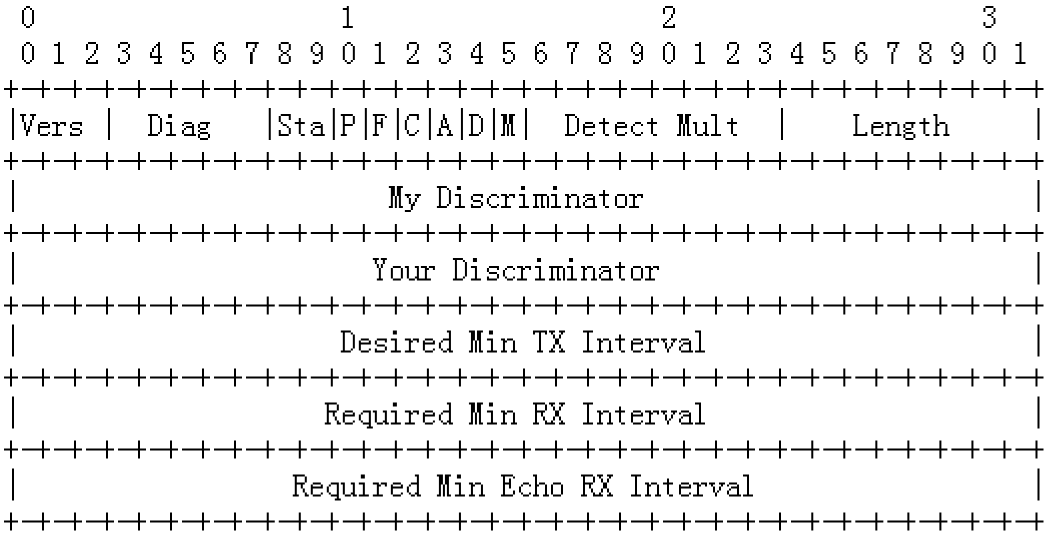
4.1.1 Overview

Bidirectional forwarding detection (BFD) provides low-overhead, short-duration detection of the connectivity in the forwarding path between adjacent routers. The fast detection of failures in the forwarding path speeds up enabling the backup forwarding path and improves the network performance.

4.1.2 BFD Packet Format

The two types of BFD packets are control packets and echo packets. The local end sends echo packets to the peer, which returns the received echo packets back without processing. Therefore, no BFD echo packet format is defined. Only BFD control packet format is defined. There are two versions for the BFD control packet: version 0 and version 1. By default, the BFD session establishment adopts the version 1. However, if one end receives the version 0 control packets from the peer, the default version 1 automatically switches to version 0 to establish the BFD session. You can use the **show bfd neighbors** command to view the version member. The format of the version 1 packet is shown as follows:

Figure 1 Format of BFD control packets (version 1)



```
 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	BFD protocol version. Currently, the value is **1**.
Diag	The following are causes of the latest switchover from the UP state to other states: **0**: indicates no diagnosis. **1**: indicates the control timeout detection. **2**: indicates the echo function failure. **3**: indicates that the neighbor advertising session is down. **4**: indicates that the forwarding plane is reset. **5**: indicates that the channel is invalid. **6**: indicates that the connection channel is invalid. **7**: indicates that administration is down.
Sta	Local status of the BFD. Including: **0**: AdminDown **1**: agent down **2**: agent Init **3**: agent UP
P	When a parameter changes, the sender places this flag in a BFD packet. The receiver must

Field	Description
	immediately respond the packet.
F	The packet must have the F flag set for responding to the packet with the P flag set.
C	Forward/control separation flag. Once this flag is set, the change of the control plane does not affect the BFD. For example, if the control plane deploys OSPF, the BFD continues with link status detection when OSPF restarts or performs a graceful restart (GR).
A	Authentication flag. If this flag is set, sessions need to be authenticated.
M	Used in point-to-multipoint in the future. Currently, the value must be set to **0**.
Detect Mult	Detection timeout multiples. This flag is used by the detector to compute the timeout duration.
Length	Packet length
My Discriminator	Discriminator used by the BFD session to connect to the local end
Your Discriminator	Discriminator used by the BFD session to connect to the remote end
Desired Min Tx Interval	Minimum BFD packet sending interval supported by the local end
Required Min RX Interval	Minimum BFD packet receiving interval supported by the local end
Required Min Echo RX Interval	Minimum echo packet receiving interval supported by the local end. If the local end does not support the echo function, set the value to 0.
Auth Type	Authentication types (optical), including: Simple Password Keyed MD5 Meticulous Keyed MD5 Keyed SHA1 Meticulous Keyed SHA1
Auth Length	Authentication data length
Authentication Data	Authentication data area

Note

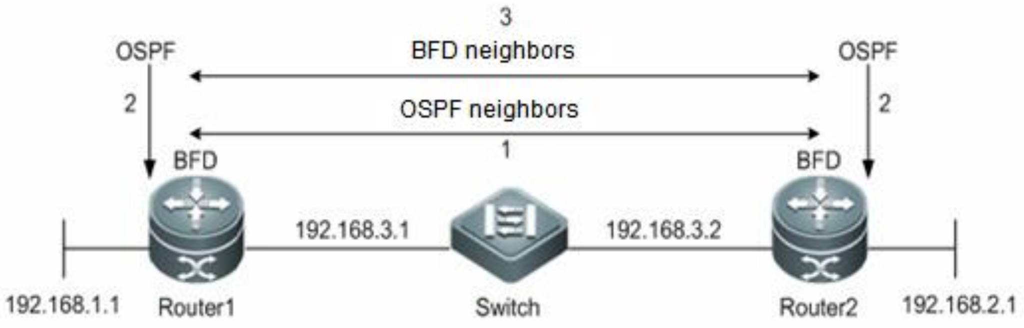
From version 10.3(4b3), the RGOS supports version 1 and version 0 packets. By default, session initiation packets adopt version 1. If one end receives version 0 control packets from the peer, the default version 1 automatically switches to version 0 to establish the session.

4.1.3 BFD Operation Mechanism

The BFD detection mechanism is independent from the applied interface media type, encapsulation format mad, associated upper-layer protocols such as OSPF, BGP, and RIP. The BFD establishes a session between adjacent routers enables the route protocols to re-calculate the route table by rapidly sending the detection fault to the running route protocols and decreases the network convergence time sharply. The BFD cannot discover the neighbors, so it needs the upper-layer protocols to notify the neighbors of which the session is established.

The following figure shows that two routers are connected through a L2 switch. The two routers runs OSPF and BFD.

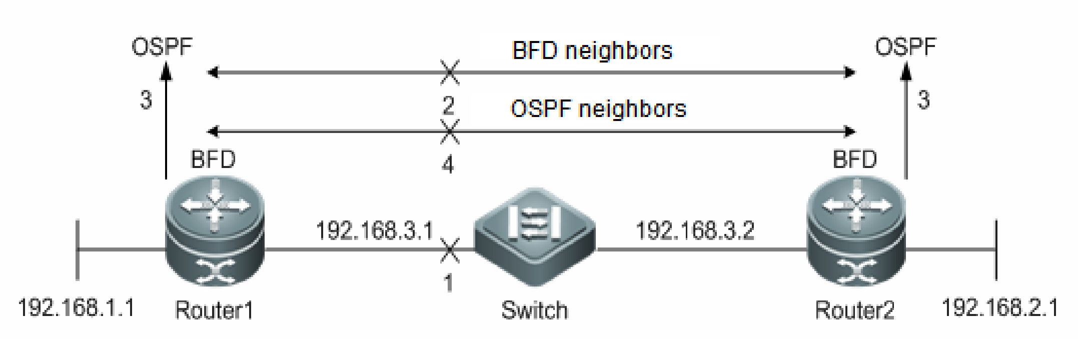
Figure 2 BFD session establishment



The BFD session establishment process is as follows:

5) OSPF discovers neighbors and establishes neighbor relationships.
6) OSPF notifies BFD of establishing the session with the neighbors.
7) BFD establishes the session with the neighbors.

Figure 3 BFD fault detection process



The BFD fault detection process is as follows:

8) Step 1: A link communication failure between Router1 and Router2 occurs.
9) Step 2: BFD session between the Router1 and Router2 detects the fault.
10) Step 3: BFD notifies the fault of the OSPF reachability to the forwarding path of the neighbor.
11) Step 4: OSPF deals with the process of the neighbor Down. If the backup forwarding path exists, and the protocol convergence is performed and the backup forwarding path is enabled.

4.1.4 Related Protocols and Regulations

The related BFD protocols and regulations are:

- draft-ietf-bfd-base-09: Bidirectional Forwarding Detection
- draft-ietf-bfd-generic-05: Generic Application of BFD
- draft-ietf-bfd-mib-06: Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-v4v6-1hop-09: BFD for IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-07: BFD for IPv4 and IPv6 (Multihop)
- draft-ietf-bfd-mpls-07: BFD For MPLS LSPs

☑ Currently, no version supports draft-ietf-bfd-mib-06.

4.2 BFD Features

This section describes the BFD features.

4.2.1 BFD Session Establishment Mode

The BFD session is established in the following modes:

- Active Mode: Before a session is established, BFD actively sends the BFD control packets regardless of whether any BFD control packet is received from the peer.

4.2.2 BFD Detection Mode

Asynchronous Mode

In the asynchronous mode, the BFD control packets are sent periodically among the systems. If one system receives no BFD control packet from the peer within the BFD interval, the BFD session will be down.

Echo Mode

The local system sends the BFD echo packet periodically. The peer system loops back the echo packet via the forwarding channel. The BFD session will be down if the continuous echo packets are not received within the detection interval. The echo mode can be co-used with the above-mentioned two detection modes. In the echo mode, the packets are forwarded back via the forwarding panel of the peer system rather than the control panel, reducing the delay and speeding up the fault detection in comparison to the control packet sending. In the asynchronous mode, the control packet sending will be decreased with the echo function enabled, for the echo function processes the detection. The echo function must be enabled in the BFD session; otherwise the echo function will be invalid.

☑ Only BFD session version 1 supports the BFD echo function

⚠ Caution

The **no ip redirects** command must be executed to disable the redirect function of the IP packets and the **no ip deny land** command must be executed to disable the function of anti-attack of the Land-based DDOS before configuring the echo mode.

4.2.3 BFD Session parameters

- BFD session parameters (including Desired Min Tx Interval, Required Min RX Interval, and Detect Mult) must be configured on interfaces at both ends. Otherwise, BFD sessions cannot be created.
- During BFD session creation, interfaces at both ends will negotiate BFD session parameters and accordingly detect the session.
- If BFD session parameters are revised after BFD session creation, interfaces at both ends re-initiate the negotiation. During revision, the BFD session remains in the UP state.

4.2.4 BFD for Dynamic Route Protocols

Configuring BFD for the route protocols improves the convergence performance of the protocol by taking advantages of the faster fault detection of the BFD in comparison to the HELLO mechanism of the protocol. Generally, the fault detection time can be decreased to less than 1s.

Make sure that the BFD for corresponding protocol is enabled on all BFD session neighbors, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for this protocol is established.

4.2.5 BFD for Static Route

Configuring BFD for static route prevents the static route from being the forwarding path when the router selects the routing under the circumstances that the configured static route is unreachable. It can rapidly switch to the backup forwarding path if the backup forwarding path exists.

Being different from the dynamic route protocol, the static route protocol has no mechanism of discovering the neighbor. Therefore, when configuring the BFD for static route, the reachability of the next-hop of the static route is dependent on the BFD session state. If the BFD session detects the fault, which means that next-hop of the static route is unreachable; the static route cannot be installed into the RIB. Make sure that the BFD for static route is enabled on all BFD session neighbors, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for static route is enabled..

If the BFD session is removed from the peer in the process of the BFD session establishment, the BFD session is down. Under this circumstance, the static route forwarding shall be ensured.

4.2.6 BFD for PBR

Configuring BFD for PBR prevents the PBR from being the forwarding path when the router selects the routing under the circumstances that the configured PBR is unreachable. It can rapidly switch to the backup forwarding path if the backup forwarding path exists.

The method of BFD for PBR is similar to the BFD for static route. If the BFD session detects the fault by following the forwarding path of the specified neighbor, the PBR will be notified of the unreachability to the corresponding next-hop. The PBR reaching the next-hop is ineffective.

Make sure that the BFD for PBR is enabled on all BFD session neighbors, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for PBR will be enabled automatically.

If the BFD session is removed from the peer in the process of the BFD session establishment, the BFD session will be down. And under this circumstance, the PBR forwarding shall be ensured.

4.2.7 BFD for VRRP

BFD for VRRP configuration can replace the HELLO mechanism of VRRP itself to realize the fast detection of running state of the master and backup routers and improve the network performance. Generally, the time of failure detection can be shortened to less than 1s.

Make sure that the BFD for VRRP is enabled on the router at both ends, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for VRRP will also be configured.

VRRP can also use BFD to follow the specified neighbor. If the BFD session detects the fault of the forwarding path to the neighbor, it will reduce the VRRP priority automatically and trigger the switchover between the master and backup routers. The BFD can be established only when the dynamic route protocol or other applications notify BFD of establishing the session with corresponding neighbor.

4.2.8 BFD Supports to Change the State of Layer3 Interfaces

The BFD supports the function of changing the L3 interface status. In the configuration mode, you can run the **bfd bind peer-ip** command to detect the direct connection address of a specified L3 interface. BFD session status established through this command will generate the corresponding interface BFD status, such as BFD-DOWN/BFD-

UP. With this function commonly used in various FRRs, the BFD is used to detect the interface status and perform FRR.

4.2.9 BFD for MPLS-LSP

The BFD for MPLS indicates that the Label Switched Path (LSP) performs fast detection for neighbors through the BFD. The following detection modes are supported:

- Configuring the BFD for static LSP
- Configuring the BFD for LSPs generated by LDP
- Configuring the BFD for LSP reverse links by using IP addresses

4.2.10 BFD for VRF

The BFD supports VPN Routing and Forwarding (VRF) and detects the connectivity of the forwarding path between the Provider Edge (PE) and the Customer Edge (CE).

4.2.11 BFD for Interfaces

Switches: BFD configuration is allowed only on Routed Port and SVI, not on a L3 AP. If the SVI member interface is a L2 AP, BFD session creation fails on the member interface.

Routers: BFD configuration is allowed on synchronous interfaces, asynchronous interfaces, ATM, serial interfaces, frame relay, POS, CPOS, Ethernet interfaces and child interfaces, E1, channelized ATM, and channelized CPOS.

4.3 Configuring BFD

4.3.1 Default configurations for the BFD

Function	**Defaults**
BFD session creation mode	Active mode. It cannot be set.
BFD detection mode	Asynchronous mode. The echo function is enabled by default.
BFD session parameter	No default value. It must be set.
BFD authentication method	Disabled. It cannot be set.
BFD for dynamic route protocol	Disabled
BFD for the static route	Disabled
BFD for PBR	Disabled
BFD for VRRP	Disabled
BFD for VRF	Disabled
BFD for MPLS-LSP	Disabled

4.3.2 Configuring BFD Session Parameters

The BFD session parameter has no default value and must be configured. To configure BFD session parameters, run the following command in turn.

Command	**Function**
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global mode.
Qtech(config)# **interface** *type number*	Enters interface configuration mode.
Qtech(config-if)# **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*	Configures BFD session parameters for a specified interface. **interval** *milliseconds*: indicates the minimum sending interval. The unit is millisecond. **min_rx** *milliseconds*: indicates the minimum receiving

Command	Function
	interval. The unit is millisecond. **multiplier** *interval-multiplier*: indicates the detection timeout multiples.
Qtech(config-if)# **end**	Exits interface configuration mode and restores privileged mode.

To delete BFD session parameter configurations, run the **no bfd interval** command in interface configuration mode.

The following example shows how to configure BFD session parameters on the Routed Port FastEthernet 0/2.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface fastEthernet 0/2
Qtech(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

⚠ Caution

The difference of the bandwidth transmitted on different interfaces must be considered when configuring the parameters. If the minimum sending and receiving intervals are too low, it may result in the oversized bandwidth of the BFD and affect data transmission.
Switches cannot be configured on the L3 AP interface.

4.3.3 Configuring the BFD Echo Function

The session status is not affected if the echo function is enabled after the BFD session is created. After the echo function is disabled, no echo packet is sent and the forwarding plane ceases to receive echo packets. To configure the BFD echo function, run the following commands in turn.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global mode.
Qtech(config)# **interface** *type number*	Enters interface configuration mode.
Qtech(config-if)# **bfd echo**	Enables the BFD echo function.
Qtech(config-if)# **end**	Exits interface mode and returns to privileged mode.

To disable the BFD echo function, run the **no bfd echo** command in interface mode.

The following example shows how to configure the BFD echo function on the Routed Port FastEthernet 0/2:

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface fastEthernet 0/2
Qtech(config-if)# bfd echo
```

To enable the BFD control packet to be sent in a slower frequency after the echo function is enabled in the BFD asynchronous mode, run the following commands in turn.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global mode.
Qtech(config)# **bfd slow-timer** milliseconds	Configures the slow-timer. The default value is 1 second. The value range is from 1000 to 30000 and the unit is millisecond.
Qtech(config)# **end**	Enters global configuration mode.

To restore the default value of the slow-timer, run the **no bfd slow-time** mode in global mode.

The following example shows how to configure the time of the slow-timer to 1400 milliseconds:

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# bfd slow-timer 1400
```

Caution

The local end sends the BFD echo packet to the peer, which returns the received packets with processing on the forwarding panel. In this process, the BFD session detection may fail for the peer has been congested resulting in the loss of the echo packets. Under these circumstances, the corresponding QoS policy is necessary to be configured to make sure that the echo packets take the precedence to be processed or the echo function is disabled.

4.3.4 Configuring the BFD UP-Dampening Time

The BFD up-dampening time configuration solves the problem that the BFD session status frequent switches between DOWN and UP due to the line instability, which results in the frequent forwarding path switchover of the associated application (for example, the static route) and the abnormal operation. This feature allows you to configure the required up-dampening time before advertising the session UP state to a related application. To configure the BFD UP-Dampening function, run the following commands in turn.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global mode.
Qtech(config)# **interface** *type number*	Enters interface configuration mode.
Qtech(config)# **bfd up-dampening** *milliseconds*	Configures the up-dampening time.
Qtech(config)#**end**	Exits global mode

To restore the default value, run the **no bfd up-dampening** command in interface configuration mode.

The following example shows how to configure the BFD up-dampening time as 60,000ms:

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface fastEthernet 0/2
Qtech(config-if)# bfd up-dampening 60000
```

Caution

In the configuration process, the parameter configurations for two ends of the BFD session must be consistent. This ensures that applications and protocols associated with the BFD take effect simultaneously, and avoid that unidirectional communication occurs on the forwarding path due to different up-dampening time on the two ends.

The dampening function does not take effect in the BFD for OSPFv3.

4.3.5 Configuring the BFD CPP

The BFD protocol is a sensitive protocol. When the device with BFD function enabled suffers from attack (for example, a large amount of Ping packets attack the device), which lead to the BFD session turbulence, the device can be protected by enabling the BFD protection policy. However, if the BFD function and the BFD protection policy are enabled at the same time, the loss of BFD packets on the attacked device occurs when the packets sent from the last-hop device go through this device, influencing the BFD session establishment between the last-hop device and other devices. This function takes effect only for the switches.

To configure the BFD CPP, run the following commands in turn.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global mode.
Qtech(config)# **bfd cpp**	Enables the BFD CPP.
Qtech(config)# **end**	Exits global configuration mode.

By default, the BFD CPP is enabled. To disable the BFD CPP, run the **no bfd cpp** command in global mode.

The following example shows how to enable the BFD CPP.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# bfd cpp
```

4.3.6 Configuring the BFD for RIP

RIP sends the route updating information periodically. A route is invalid and RIP cannot rapidly respond to the link failure when no route updating information is received within the specified time.

After enabling the BFD for RIP, the BFD session will be established for the RIP route information source (the source address for RIP route updating packet). Once BFD detects that a neighbor is invalid, RIP route information will directly be in the invalid state and not join in the route forwarding no longer. The convergence time can be decreased from 180s (the default RIP timer) to less than 1s.

Run the **bfd all-interfaces** command to enable BFD for RIP applications on all interfaces. Or run the **ip rip bfd** [**disable**] command in interface configuration mode to enable or disable to allow BFD for RIP applications on specified interfaces.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **router rip**	Enters router configuration mode.
Qtech(config-router)# **bfd all-interfaces**	Allows the BFD for RIP on all interfaces.
Qtech(config-router)# **exit**	Exits router configuration mode and returns to global configuration mode. (Optional)
Qtech(config)# **interface** *type number*	Enters interface configuration mode. (Optional)
Qtech(config-if)#**ip rip bfd** [**disable**]	Allows or prohibits the BFD for RIP on specified interfaces. (Optional)
Qtech(config-if)#**end**	Exits interface configuration mode. (Optional)
Qtech#**show bfd neighbors** [**details**]	Displays the BFD session establishment information and whether RIP is for the specified session. (Optional)

To disable to allow the BFD for RIP applications, run the **no bfd all-interfaces** in Router mode.

The following example shows how to enable the BFD for RIP on all interfaces excluding the FastEthernet 0/2:

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# router rip
Qtech(config-router)# bfd all-interfaces
Qtech(config-router)# exit
Qtech(config)# interface FastEthernet 0/2
Qtech(config-if)# ip rip bfd disable
Qtech(config-if)#end
```

Caution

The route information sources (source address for RIP route updating packet) of two devices with RIP enabled must be in the same network segment to establish the BFD session between adjacent routers.
BFD session parameters must have been configured. Otherwise, BFD session creation fails.
For the non-unnumbered interface, if the neighbor end and the local end are not connected directly, the BFD for IPv4 PBR fails to be enabled.
BFD session creation fails if an interface specified during BFD session creation is different from the actual BFD packet egress or ingress interface due to IP routing.
BFD session creation fails if an interface specified during BFD session creation is different from the actual BFD packet egress or ingress interface.

4.3.7 Configuring the BFD for OSPF

The OSPF protocol dynamically discovers the neighbors by the Hello packets. With BFD for OSPF configured, the BFD session for the neighbors in FULL relationship will be established and the neighbor state will be detected by the BFD mechanism. Once BFD neighbor is invalid, OSPF processes the network convergence. The convergence time could be from 120s(by default, the sending interval of the OSPF Hello packet in non-broadcast network is 30s, which is a quarter of the invalid time for the adjacency router, namely, 120s) to less than 1s.

Run the **bfd all-interfaces** command to enable BFD for RIP applications on all interfaces. Or run the **ip ospf bfd** [**disable**] command in interface configuration mode to enable or disable to allow the BFD for RIP applications on specified interfaces.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **router ospf** *process-id*	Enters router configuration mode.
Qtech(config-router)# **bfd all-interfaces**	Allows the BFD for RIP on all interfaces. Prohibits the BFD for RIP on all interfaces by running the **no** command.
Qtech(config-router)# **exit**	Exits router configuration mode and returns to global configuration mode. (Optional)
Qtech(config)# **interface** *type number*	Enters interface configuration mode. (Optional)
Qtech(config-if)#**ip ospf bfd** [**disable**]	Allows or prohibits the BFD for RIP on specified interfaces. (Optional)
Qtech(config-if)#**end**	Exits interface configuration mode. (Optional)
Qtech#**show bfd neighbors** [**details**]	Displays the BFD session establishment information and whether OSPF is for the specified session. (Optional)
Qtech#**show ip ospf**	Displays whether OSPF is for the specified session. (Optional)

To disable to allow the BFD for RIP applications, run the **no bfd all-interfaces** in Router mode.

The following example shows how to enable the BFD for OSPF on all interfaces excluding the FastEthernet 0/2:

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# router ospf 123
Qtech(config-router)# bfd all-interfaces
Qtech(config-router)# exit
Qtech(config)# interface FastEthernet 0/2
Qtech(config-if)# ip rip bfd disable
Qtech(config-if)#end
```

☑ 10.3(4b3) or 10.3(5) do not support the BFD for OSPFv3.

Caution

BFD session parameters must have been configured. Otherwise, BFD session creation fails.
BFD session creation fails if an interface specified during BFD session creation is different from the actual BFD packet egress or ingress interface due to IP routing.
BFD session creation fails if an interface specified during BFD session creation is different from the actual BFD packet egress or ingress interface.
The OSPFv2/OSPFv3 virtual link does not support the BFD monitoring.

4.3.8 Configuring Association Between IS-IS and BFD

The Intermediate System to Intermediate System (IS-IS) protocol dynamically discovers a neighbor via hello packets. When the BFD function is enabled, the device running the IS-IS protocol establishes a BFD session for a neighbor in the UP state, and detects the status of the neighbor via the BFD mechanism. Once the BFD neighbor fails, the device running the IS-IS protocol immediately performs network convergence. The network convergence period can be reduced from 30s to 1s. By default, the transmission interval of point-to-point hello packets is 10s, and the failure period of the neighbor device is 30s (3 times the transmission interval).

Run the **bfd all-interfaces** command to enable association between IS-IS and BFD on all interfaces. Run the **isis bfd [disable]** command in interface configuration mode to enable or disable association between IS-IS and BFD on a specified interface.

Command	Function
Qtech>**enable**	Enters the privileged EXEC mode.

Qtech# **configure terminal**	Enters the global configuration mode.
Qtech(config)# **router isis**	Enters the router configuration mode.
Qtech(config-router)# **bfd all-interfaces**	Enables association between IS-IS and BFD on all interfaces. Runs the **no** form of this command to disable association between IS-IS and BFD on all interfaces.
Qtech(config-router)# **exit**	(Optical) Exits the router configuration mode and returns to the global configuration mode.
Qtech(config)# **interface** *type number*	(Optical) Enters the interface configuration mode.
Qtech(config-if)#**isis bfd** [**disable**]	(Optical) Enables or disables association between IS-IS and BFD on a specified interface.
Qtech(config-if)#**end**	(Optical) Exits the interface configuration mode.
Qtech#**show bfd neighbors** [**details**]	(Optical) Displays BFD session information and checks whether IS-IS is associated with a specified session.
Qtech# **show isis neighbors detail**	(Optical) Displays information about whether IS-IS is associated with a specified session.

Run the **no bfd all-interfaces** command in router configuration mode to disable association between IS-IS and BFD on all interfaces.

Configuration example:

#Enable association between IS-IS and BFD on interfaces except FastEthernet 0/2.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# router isis
Qtech(config-router)# bfd all-interfaces
Qtech(config-router)# exit
Qtech(config)# interface FastEthernet 0/2
Qtech(config-if)# isis bfd disable
Qtech(config-if)#end
```

⚠ Caution

BFD session parameters must be configured before enabling association between IS-IS and BFD.
IP routing may cause inconsistency between the interface specified by the BDF session neighbor and

the actual BDF packet outbound interface. In this case, BDF sessions cannot be established.
If the interface specified for BFD session establishment is inconsistent with the BFD packet inbound interface, BDF sessions cannot be established.

4.3.9 Configuring the BFD for BGP

Being similar to OSPF, by configuring the BFD for BGP, the BGP protocol rapidly detects the faults, realizes the rapid detection of the neighbor relationship and fastens the protocol convergence. By default, the BGP keepalive interval is 60s and the holdtime is 180s. The minimum value of the keepalive interval and holdtime are 1s and 3s respectively. It is slow to detect the neighbor relationship.

A large amount of the packets will be lost on the interface that receives and sends the packets at the fast speed. With the BFD enabled, the holdtime can decrease to less than 1 second.

Run the **neighbor** *ip-address* **fall-over bfd** command to enable the BFD for BGP.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **router bgp** *as-tag*	Enters router configuration mode.
Qtech(config-router)#**neighbor** *ip-address* **fall-over bfd**	Selects BFD keywords to indicate the BFD for BGP to detect the faults of specified neighbors.
Qtech(config-router)#**end**	Exits router configuration mode. (Optional)
Qtech#**show bfd neighbors** [**details**]	Displays the BFD session establishment information and whether the BGP is associated to the specified session. (Optional)
Qtech#**show ip bgp neighbors**	Displays whether the BGP is associated to the specified session. (Optional)

To disable the BFD for BGP applications, run the **no neighbor** *ip-address* **fall-over bfd** in Router mode.

The following example shows how to enable the BFD for BGP, and detect the forwarding path with the neighbor 172.16.0.2:

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface FastEthernet 0/1
Qtech(config-if)# no switchport
Qtech(config-if)# ip address 172.16.0.1 255.255.255.0
Qtech(config-if)# bfd interval 50 min_rx 50 multiplier 3
Qtech(config-if)# exit
Qtech(config)# router bgp 44000
Qtech(config-router)# bgp log-neighbors-changes
Qtech(config-router)# neighbor 172.16.0.2 remote-as 45000
Qtech(config-router)# neighbor 172.16.0.2 fall-over bfd
Qtech(config-router)# end
```

☑ 10.3(4b3) and 10.3(5) support the BFD for BGP only when BGP works in IPv4 address families.

⚠ Caution

If BGP establishes the session using the loopback address and enables BFD to detect the neighbors, the outbound interface for the BFD packets will be specified according to the result of IP routing. In this situation, before configuring the BFD for BGP, the **bfd interval** command is necessary to be used to configure the BFD session parameter on the possible outbound interface. Otherwise, it may fail to establish the session.
The BFD session cannot be established if the specified interface and the actual incoming interface for the BFD packets are inconsistent.

4.3.10 Configuring the BFD for Static Route

To configure the BFD for Static Route, run the following commands in turn.

Command	Function

Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **ip route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* [**souce** *ip-address*]	Configures the BFD for the static route. The parameters *interface-type*, *interface-number* and *gateway* indicate the interface and IP address of a neighbor. For multi-hops, **souce** *ip-addess* needs to be configured as the session source IP address. BFD session parameters must be configured before the configuration.
Qtech(config)#{ **ip route** *prefix mask* {*ip-address* | *interface-type interface-number [ip-address*]}	Ensures the parameters *interface-type*, *interface-number* and *gateway* are consistent with that configured in Step 3 before configuring the BFD for the static route.
Qtech(config)# **end**	Exits global configuration mode.
Qtech#**show bfd neighbors** [**details**]	Displays the BFD session establishment information and whether the static route is associated to the specified session. (Optional).

To disable the BFD for the static route, run the **no ip route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* command in interface mode.

The following example shows how to enable the BFD for static route, and detect the forwarding path with the neighbor 172.16.0.2:

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface FastEthernet 0/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 172.16.0.1 255.255.255.0
Qtech(config-if)# bfd interval 50 min_rx 50 multiplier 3
Qtech(config-if)# ip route static bfd FastEthernet 0/1 172.16.0.2
Qtech(config-if)# ip route 10.0.0.0 255.0.0.0 FastEthernet 0/1 172.16.0.2
Qtech(config-if)# end
```

4.3.11 Configuring the BFD for PBR

To configure the BFD for PBR, run the following commands in turn.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	Configures the defined route map to enter route map configuration mode.
Qtech(config-route-map)#**match ip address** *access-list-number*	Configures the matching access list.
Qtech(config-route-map)#**set ip next-hop verify-availability** *next-hop-address* { **track** *number* **| bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* }	Configure the BFD for PBR. The parameters *interface-type*, *interface-number* and *gateway* indicate the interface and IP address of a neighbor. BFD session parameters must be configured before the configuration. The next hop specified by the parameter *next-hop-address* is unreachable if the BFD session detects faults. Run the **no** command to cancel the configuration.
Qtech(config-route-map)#**exit**	Exits route map configuration mode.
Qtech(config)# **interface** *type number*	Enters interface configuration mode.
Qtech(config-if)#**ip policy route-map** *route-map*	Enables the PBR on interfaces.
Qtech(config-if)#**end**	Exits interface configuration mode.
Qtech#**show bfd neighbors** [**details**]	Displays the BFD session establishment information and whether the PBR is associated with the specified session. (Optional)
Qtech#**show route-map**	Displays whether the PBR is associated with the specified session. (Optional)

To disable the BFD for PBR applications, run the **no set ip next-hop verify-availability** [*next-hop-address* [**track** *number*|**bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway*]] command in router-map mode.

The following example shows how to enable the BFD for PBR, and detect the forwarding path with the neighbor 172.16.0.2:

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# route-map Example1 permit 10
Qtech(config-route-map)# match ip address 1
Qtech(config-route-map)#set ip next-hop verify-availability 172.16.0.2 bfd
FastEthernet 0/1 172.16.0.2
Qtech(config-route-map)#end
Qtech(config)#interface FastEthernet 0/1
Qtech(config-if)#no switchport (This configuration is unnecessary for routers)
Qtech(config-if)#ip address 172.16.0.1 255.255.255.0
Qtech(config-if)#bfd interval 50 min_rx 50 multiplier 3
Qtech(config-if)#ip policy route-map Example1
Qtech(config-if)#exit
```

☑ The BFD for PBRv6 is not supported in v10.3(4b3) and v10.3(5).

4.3.12 Configuring the BFD for VRRP

To enable the BFD for VRRP groups to detect the master and backup routers, run the following commands in turn.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **interface** *type number*	Enters interface mode.
Qtech(config-if)#**vrrp** *group-number* **ip** [*ip-address*[**secondary**]]	Creates VRRP groups and virtual IP addresses. *ip-address* indicates the IP address of the specified neighbor.
Qtech(config-if)# **vrrp** *group-number* **bfd** *ip-address*	Configures the BFD for all VRRP groups. *ip-addess* indicates the neighbor IP address.
Qtech(config-if)# **end**	Exits interface configuration mode.
Qtech#**show bfd neighbors** [**details**]	Displays the BFD session establishment information and whether the VRRP is associated with the specified session. (Optional).
Qtech#**show vrrp**	Displays whether the VRRP is associated with the specified session. (Optional)

To disable the BFD for VRRP groups to detect the master and backup routers, run the **no vrrp** *group-number* **bfd** command in interface mode.

The following example shows how to enable the BFD for VRRP, and detect the forwarding path between the master and slave routers:

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#interface FastEthernet 0/1
Qtech(config-if)#no switchport (This configuration is unnecessary for routers)
Qtech(config-if)#ip address 192.168.201.11 255.255.255.0
Qtech(config-if)#bfd interval 50 min_rx 50 multiplier 3
Qtech(config-if)#vrrp 1 priority 120
Qtech(config-if)#vrrp 1 ip 192.168.201.1
Qtech(config-if)#vrrp 1 bfd 192.168.201.12
Qtech(config-if)#end
```

To enable the specified VRRP group to track the IP address of the specified neighbor through the BFD, run the following commands in turn.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **interface** *type number*	Enters interface configuration mode.
Qtech(config-if)#**vrrp** *group-number* **ip** [*ip-address*[**secondary**]]	Creates VRRP groups and virtual IP addresses on specified interfaces.

Qtech(config-if)# **vrrp** *group-number* **track bfd** *interface-type interface-number ip-address* [*priority*]	Configures the specified VRRP group to track the IP address of the specified neighbor through the BFD. Run the **no** command to cancel the configuration.
Qtech(config-if)# **end**	Exits interface configuration mode.
Qtech#**show bfd neighbors** [**details**]	Displays the BFD session establishment information and whether the VRRP is associated with the specified session. (Optional).
Qtech#**show vrrp**	Displays whether the BFD is for VRRP is enabled to track the IP address of the specified neighbor. (Optional).

To disable the specified VRRP group to track the IP address of the specified neighbor through the BFD, run the no **vrrp** *group-number* **track bfd** *interface-type interface-number ip-addess* command in interface mode.

The following example shows how to specify the VRRP to track the specified neighbor 192.168.1.3:.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#interface FastEthernet 0/1
Qtech(config-if)#no switchport (This configuration is unnecessary for routers)
Qtech(config-if)#ip address 192.168.1.1 255.255.255.0
Qtech(config-if)#bfd interval 50 min_rx 50 multiplier 3
Qtech(config)#interface FastEthernet 0/2
Qtech(config-if)#no switchport (This configuration is unnecessary for routers)
Qtech(config-if)#ip address 192.168.201.17 255.255.255.0
Qtech(config-if)#vrrp 1 priority 120
Qtech(config-if)#vrrp 1 ip 192.168.201.1
Qtech(config-if)#vrrp 1 track bfd FastEthernet 0/1 192.168.1.3 30
Qtech(config-if)#end
```

4.3.13 Configuring BFD for Changing the State of Layer 3 Interfaces

Generally, it takes a long time for link communication failure or link failure to change the interface state. For various FRRs relying on interface state, high-performance switchover cannot be achieved. Therefore, BFD is generally associated with the layer-3 interface state to realize fast detection of interface state. Execute the following configurations to associate BFD and layer 3 interface states.

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **interface** *type number*	Enters an L3 interface.
Qtech(config-if)# **bfd bind peer-ip** *ip-address* [**source-ip** *ip-adress*] **process-pst**	Configure the BFD for L3 interfaces. Source-ip specifies the source IP address of a BFD packet for avoiding that the packet is discarded due to uRPF check failure when the uRPF is also used. Process-pst indicates the BFD status of the BFD session generation interface.
Qtech(config-if)#**end**	Exits interface configuration mode. (Optional).
Qtech#**show bfd neighbors** [**details**]	Displays the BFD session establishment information and whether the interface is associated with the specified session. (Optional).

To disable the BFD for interfaces, run the **no bfd bind peer-ip** *ip-address* in configuration mode.

The following example shows how to enable the BFD for FastEthernet 0/2.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface FastEthernet 0/2
Qtech(config-if)#no sw (This configuration is unnecessary for routers)
Qtech(config-if)#ip address 1.1.1.1 255.255.255.0
Qtech(config-if)#bfd bind peer-ip 1.1.1.2 source-ip 1.1.1.1 process-pst
Qtech(config-if)#end
```

4.3.14 Configuring the BFD for MPLS

The BFD for MPLS indicates that the BFD performs rapid detection on the LSP on the MPLS network to improve MPLS network reliability.

4.3.14.1 Configuring the BFD Detection for the Static LSP

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **bfd bind static-lsp peer-ip** *ip-address* **source-ip** *ip-address* [**local-discriminator** *discr-value* **remote-discriminator** *discr-value*] [**process-state**]	Configures the BFD for static LSP. You can configure the homing address, next-hop address, and egress interface of the LSP. If no local discriminator is configured, the system automatically elects the local discriminator. If no remote discriminator is configured, the system learns of the remote discriminator in automatic configuration mode.

4.3.14.2 Configuring the BFD detection for the Dynamic LSP

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech#**mpls router ldp**	Enters LDP configuration mode.
Qtech(config-mpls-router)# **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**]	Configures the BFD for dynamic LSP. You can configure the homing address, next-hop address, and egress interface of the LSP. If no local discriminator is configured, the system automatically elects the local discriminator. If no remote discriminator is configured, the system learns of the remote discriminator in automatic configuration mode.

4.3.14.3 Configuring the IP Address Mode for Reverse Link Detection in BFD for the LSP

Command	Function
Qtech>**enable**	Enters privileged mode.
Qtech# **configure terminal**	Enters global configuration mode.
Qtech(config)# **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*}	Configures the IP address mode for reverse link detection in BFD for the LSP. You can configure the source addresses, homing address, and egress interface of the LSP. Both the local and remote discriminators must be manually configured.

For details about enabling the BFD for MPLS-LSP, see the documents *MPLS-CREF* and *MPLS-SCG*.

4.3.15 Displaying BFD Configuration and Status

BFD provides following display commands for checking various configuration and running information. The following table describes functions of commands.

Command	Function
show bfd neighbors [**vrf** *vrf-name*] [**ipv4** *ip-address* [**details**]| **ipv6** *ipv6-address* [**details**] |**client** {**bgp**|**ospf**|**rip**|**vrrp**|**vrrp-balance** |**ldp-lsp**|**static-lsp**|**backward-lsp-with-ip**|**static-route**|**pbr**|**pst**} [**ipv4** *ip-address* [**details**] | **ipv6** *ipv6-address* [**details**]| **details**]]	Displays the BFD session information. For details, see the description about session display fields in Figure 4.
show vrrp	Displays information about enabling the BFD for VRRP.
show route-map	Displays information about enabling the BFD for PBR.
show ip route static bfd	Displays information about enabling the BFD for static route.
show ip bgp neighbors	Displays information about enabling the BFD for BGP.

Command	Function
show ip ospf neighbor	Displays information about enabling the BFD for OSPF.
show ip rip peer	Displays information about enabling the BFD for RIP.

Note The preceding display commands can be configured in any mode except for user mode.

☑ 10.3(4b3), 10.4(1), and later versions support the preceding configurations.

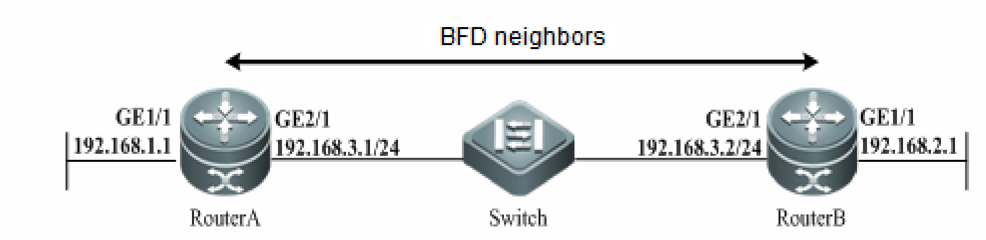
4.4 Example of Configuring BFD for RIP

4.4.1 Networking Requirement

Router A and Router B are interconnected through a L2 switch. Both routers run the RIP protocol and enable the BFD for RIP on the interface. After a link failure between Router B and L2 switch occurs, BFD detects the failure and notifies the RIP of the failure, triggering the rapid convergence.

4.4.2 Networking Topology

Figure 4 Topology of configuring BFD for RIP



4.4.3 Configuration Tips

- Router A Configuration

# Configure the Routed Port GE 2/1, the IP address, and the BFD session parameter for Router A.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.3.1 255.255.255.0
Qtech(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

Configure the Routed Port GE1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config)# ip address 192.168.1.1 255.255.255.0
```

# Enable RIP and configure the BFD for RIP to detect the neighbor 192.168.3.2.

```
Qtech(config-if)# exit
Qtech(config)# router rip
Qtech(config-router)# version 2
Qtech(config-router)# network 192.168.3.0
Qtech(config-router)# network 192.168.1.0
Qtech(config-router)# passive-interface GigabitEthernet 2/1
Qtech(config-router)# bfd all-interfaces
```

- Router B Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router B.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet 2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.3.2 255.255.255.0
Qtech(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.2.1 255.255.255.0
```

# Enable RIP and configure the BFD for RIP to detect the neighbor 192.168.3.1.

```
Qtech(config-if)# exit
Qtech(config-router)# router rip
Qtech(config-router)# version 2
Qtech(config-router)# network 192.168.3.0
Qtech(config-router)# network 192.168.2.0
Qtech(config-router)# passive-interface GigabitEthernet 2/1
Qtech(config-router)# bfd all-interfaces
Qtech(config-router)# end
Qtech#
```

4.4.4 Verification

- View the BFD session of Router A

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr          LD/RD  RH     Holdown(mult)       State  Int
192.168.3.1  192.168.3.2  1/2          1             532  (3 )           Up
       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: RIP
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
```

Field	Description
OurAddr	IP address for the session on the local end
NeighAddr	IP address for the adjacent session
LD/RD	Session ID on the local and remote end
RH/RS	Current status of the session peer end
Holdown(mult)	Time of not receiving the Hello packets on the local end of the session
State	Current session status
Int	Interface number for the session

Field	Description
Session state is UP and using echo function with 50 ms interval	Whether the session is in echo mode and the interval of sending frames. This information is shown only in echo mode.
Local Diag	Diagnosis information of the session
Poll bit	Whether the session configuration is modified.
MinTxInt	Minimum sending interval of the session on the local end
MinRxInt	Minimum receiving interval of the session on the local end
Multiplier	Timeout times detected on the local end
Received MinRxInt	Minimum sending interval of the session on the remote end
Received Multiplier	Timeout times detected on the remote end
Holdown (hits)	Session detection time and the detected timeout times
Hello (hits)	Minimum interval of receiving the Hello packet after the session negotiation
Rx Count	Number of BFD packets received on the local end
Rx Interval (ms) min/max/avg	Minimum/maximum/average interval of receiving the session on the local end
Tx Count	Number of BFD packets sent from the local end
Tx Interval (ms) min/max/avg	Minimum/maximum/average interval of sending the session from the local end
Registered protocols	Type of protocol registered to the session
Uptime	Time of keeping the session UP
Last packet	Last BFD packet received by the local end

- View the BFD session of Router B

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr          LD/RD  RH     Holdown (mult)      State  Int
192.168.3.2  192.168.3.1   2/1          1           532  (5 )             Up
       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
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197
Registered protocols: RIP
Uptime: 02:18:49
Last packet: Version: 1                          - Diagnostic: 0
I Hear You bit: 1          - Demand bit: 0
Poll bit: 0                       - Final bit: 0
Multiplier: 5                            - Length: 24
My Discr.: 1               - Your Discr.: 2
Min tx interval: 200000    - Min rx interval: 200000
Min Echo interval: 0
```

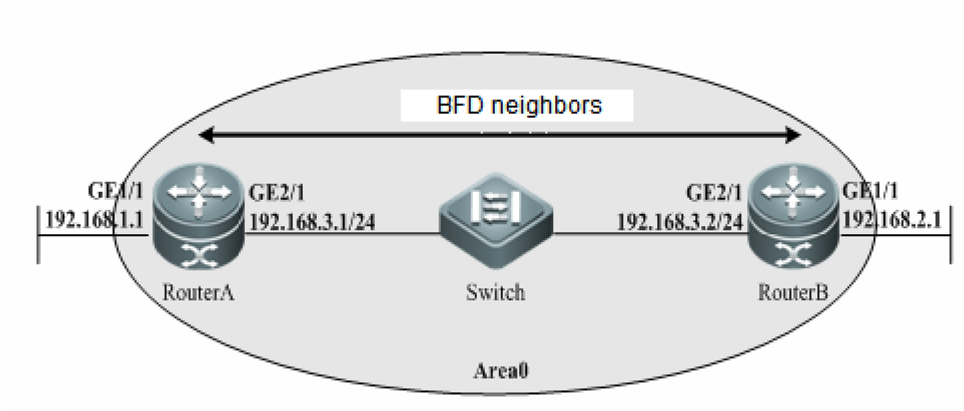
4.5 Example of Configuring BFD for OSPF

4.5.1 Networking Requirement

Router A and Router B are interconnected through a L2 switch. Both routers run the OSPF protocol and enable the BFD for OSPF on the interface. After a link failure between Router B and L2 switch occurs, BFD detects the failure and notifies the OSPF of the failure, triggering the rapid convergence.

4.5.2 Networking Topology

Figure 5 Topology of Configuring BFD for OSPF



4.5.3 Configuration Steps

- Router A Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router A.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.3.1 255.255.255.0
Qtech(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config)# ip address 192.168.1.1 255.255.255.0
```

# Enable OSPF and configure the BFD for OSPF to detect the neighbor 192.168.3.2.

```
Qtech(config-if)# exit
Qtech(config-router)# router ospf 123
Qtech(config-router)# log-adj-changes detail
Qtech(config-router)# network 192.168.3.0 0.0.0.255 area 0
Qtech(config-router)# network 192.168.1.0 0.0.0.255 area 0
Qtech(config-router)# bfd all-interfaces
Qtech(config-router)# end
Qtech#
```

- Router B Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router B.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet 2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.3.2 255.255.255.0
Qtech(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.2.1 255.255.255.0
```

# Enable OSPF and configure the BFD for OSPF to detect the neighbor 192.168.3.1.

```
Qtech(config-if)# exit
Qtech(config-router)# router ospf 123
Qtech(config-router)# log-adj-changes detail
Qtech(config-router)# network 192.168.3.0 0.0.0.255 area 0
Qtech(config-router)# network 192.168.2.0 0.0.0.255 area 0
Qtech(config-router)# bfd all-interfaces
Qtech(config-router)# end
Qtech#
```

4.5.4 Verification

- View the BFD session of Router A

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr          LD/RD  RH     Holdown(mult)       State  Int
192.168.3.1  192.168.3.2  1/2          1             532  (3 )           Up
       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: OSPF
Uptime: 02:18:49
Last packet: Version: 1                       - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0                      - Final bit: 0
Multiplier: 3                          - Length: 24
My Discr.: 2              - Your Discr.: 1
Min tx interval: 50000    - Min rx interval: 50000
Min Echo interval: 0
```

- View the BFD session of Router B

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr          LD/RD  RH     Holdown(mult)       State  Int
192.168.3.2  192.168.3.1  2/1          1             532  (5 )           Up
       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
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
```

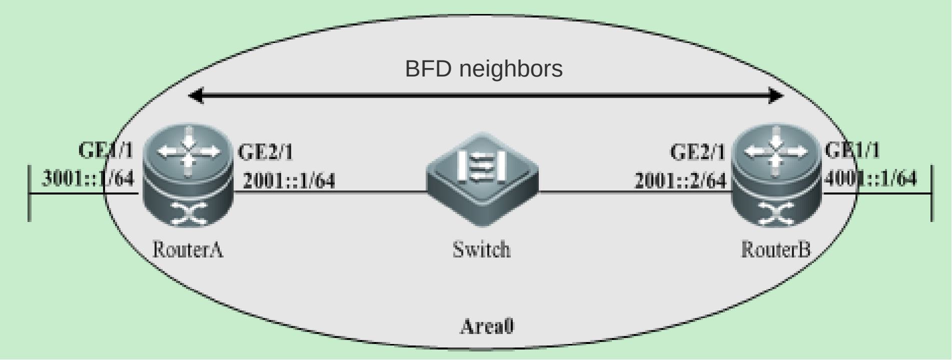
4.6 Example of Configuring BFD for OSPFv3

4.6.1 Networking Requirement

Router A and Router B are interconnected through the layer-2 switch. By running the Open Shortest Path First version 3 (OSPFv3) protocol on the switch, routes can be created and association between OSPFv3 and BFD can be enabled on interfaces of both routers. When the link between Router B and the layer-2 switch fails, the BFD function can quickly detect the failure and notify the switch running the OSPFv3 protocol to trigger fast convergence.

4.6.2 Network Topology

Figure 6 Association Between OSPFv3 and BFD



4.6.3 Configuration Tips

- Configure Router A

#Configure an interface (routed port), interface IP address, and BFD session parameters of the interface on Router A.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if)# ipv6 ospf 123 area 0
Qtech(config-if)# ipv6 address 2001::1/64
Qtech(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

#Configure the interface GE1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config)# ipv6 ospf 123 area 0
Qtech(config-if)# ipv6 address 3001::1/64
```

#Enable the OSPFv3 protocol and enable the association between OSPFv3 and BFD to detect neighbors of Router B.

```
Qtech(config-if)# exit
Qtech(config-router)# router ospf 123
Qtech(config-router)# log-adj-changes detail
Qtech(config-router)# bfd all-interfaces
Qtech(config-router)# end
Qtech#
```

- Configure Router B

#Configure an interface (routed port), interface IP address, and BFD session parameters of the interface on Router B.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet 2/1
Qtech(config-if)# ipv6 ospf 123 area 0
Qtech(config-if)# ipv6 address 2001::1/64
Qtech(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

#Configure the interface GE1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config)# ipv6 ospf 123 area 0
Qtech(config-if)# ipv6 address 4001::1/64
```

#Enable the OSPFv3 protocol and enable the association between OSPFv3 and BFD to detect neighbors of Router A.

```
Qtech(config-if)# exit
Qtech(config-router)# ipv6 router ospf 123
Qtech(config-router)# log-adj-changes detail
Qtech(config-router)# bfd all-interfaces
Qtech(config-router)# end
Qtech#
```

4.6.4 Verification

- Display BFD session establishment information on Router A.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr          LD/RD  RH/RS  Holdown(mult)      State  Int
fe80::200:12ff:fe34:5678 fe80::21a:a9ff:fe41:a124    1/2          Up           532
(3 )         Up           Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: OSPFv3
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
```

- Display BFD session establishment information on Router B.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr          LD/RD  RH/RS  Holdown(mult)      State  Int
fe80::200:12ff:fe34:5678 fe80::21a:a9ff:fe41:a124    2/1          Up           532
(5 )         Up           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: OSPFv3
Uptime: 02:18:49
Last packet: Version: 1                       - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0                     - Final bit: 0
Multiplier: 5                         - Length: 24
```

```
My Discr.: 1                - Your Discr.: 2
Min tx interval: 200000     - Min rx interval: 200000
Min Echo interval: 0
```

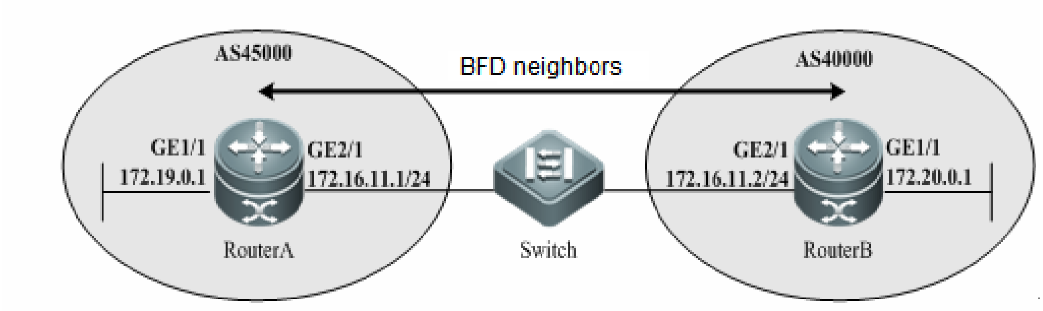
4.7 Example of Configuring BFD for BGP

4.7.1 Networking Requirement

Router A and Router B are interconnected through a L2 switch. Both routers run the BGP protocol and enable the BFD for BGP on the interface. After a link failure between Router B and L2 switch occurs, BFD detects the failure and notifies the BGP of the failure, triggering the rapid convergence.

4.7.2 Networking Topology

Figure 7 Topology of configuring BFD for BGP



4.7.3 Configuration Tips

- Router A Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router A.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 172.16.11.1 255.255.255.0
Qtech(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config)# ip address 172.19.0.1 255.255.255.0
```

# Enable BGP and configure the BFD for BGP to detect the neighbor 172.16.11.2.

```
Qtech(config-if)# exit
Qtech(config)# router bgp 45000
Qtech(config-router)# bgp log-neighbor-changes
Qtech(config-router)# neighbor 172.16.11.2 remote-as 40000
Qtech(config-router)# neighbor 172.16.11.2 fall-over bfd
Qtech(config-router)# address-family ipv4
Qtech(config-router-af)# neighbor 172.16.11.2 activate
Qtech(config-router-af)# no auto-summary
Qtech(config-router-af)# no synchronization
Qtech(config-router-af)# network 172.19.0.0 mask 255.255.255.0
Qtech(config-router-af)# exit-address-family
Qtech(config-router)# end
Qtech#
```

- Router B Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router B.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 172.16.11.2 255.255.255.0
Qtech(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config)# ip address 172.20.0.1 255.255.255.0
```

# Enable BGP and configure the BFD for BGP to detect the neighbor 172.16.11.1.

```
Qtech(config-if)# exit
Qtech(config-router)# router bgp 40000
Qtech(config-router)# bgp log-neighbor-changes
Qtech(config-router)# neighbor 172.16.11.1 remote-as 45000
Qtech(config-router)# neighbor 172.16.11.1 fall-over bfd
Qtech(config-router)# address-family ipv4
Qtech(config-router-af)# neighbor 172.16.11.1 activate
Qtech(config-router-af)# no auto-summary
Qtech(config-router-af)# no synchronization
Qtech(config-router-af)# network 172.20.0.0 mask 255.255.255.0
Qtech(config-router-af)# exit-address-family
Qtech(config-router)# end
Qtech#
```

4.7.4 Verification

- View the BFD session of Router A.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr    LD/RD  RH/RS  Holdown(mult)       State  Int
172.16.11.1  172.16.11.2  1/2          Up            532  (3 )                 Up
       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: BGP
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
```

- View the BFD session of Router B.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr    LD/RD  RH/RS  Holdown(mult)       State  Int
172.16.11.2  172.16.11.1  2/1          Up            532  (5 )                 Up
       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: BGP
Uptime: 02:18:49
Last packet: Version: 1    - Diagnostic: 0
I Hear You bit: 1                - Demand bit: 0
Poll bit: 0                      - Final bit: 0
Multiplier: 5                    - Length: 24
My Discr.: 1                     - Your Discr.: 2
Min tx interval: 200000    - Min rx interval: 200000
Min Echo interval: 0
```

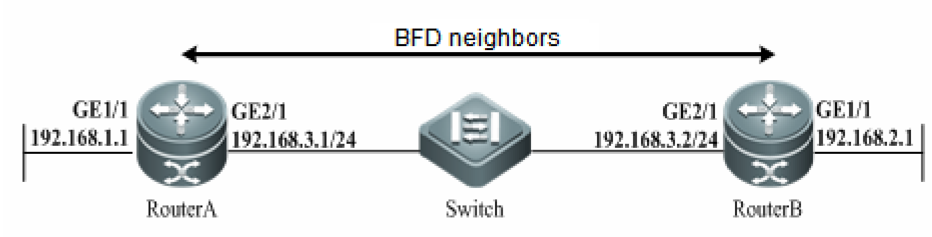
4.8 Example of Configuring BFD for Static Route

4.8.1 Networking Requirement

Router A and Router B are interconnected through a L2 switch. Both routers run the static route protocol and enable the BFD for static route on the interface. After a link failure between Router B and L2 switch occurs, BFD detects the failure and notifies the static route of the failure, triggering the static route removal from RIB and preventing the routing error.

4.8.2 Networking Topology

Figure 8 Topology of configuring BFD for Static Route



4.8.3 Configuration Tips

- Router A Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router A.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.3.1 255.255.255.0
Qtech(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config)# ip address 192.168.1.1 255.255.255.0
```

# Configure the BFD for static route to detect the neighbor 192.168.3.2.

```
Qtech(config-if)# exit
Qtech(config)# ip route static bfd GigabitEthernet 2/1 192.168.3.2
Qtech(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 2/1 192.168.3.2
Qtech(config)# end
Qtech#
```

- Router B Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router B.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet 2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.3.2 255.255.255.0
Qtech(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.2.1 255.255.255.0
```

# Configure the BFD for static route to detect the neighbor 192.168.3.1.

```
Qtech(config-if)# exit
Qtech(config)# ip route static bfd GigabitEthernet 2/1 192.168.3.1
Qtech(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 2/1 192.168.3.1
Qtech(config)# end
Qtech#
```

4.8.4 Verification

- View the BFD session of Router A.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr          LD/RD  RH     Holdown(mult)      State  Int
192.168.3.1  192.168.3.2  1/2          1             532  (3 )          Up
       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: STATIC ROUTE
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
```

- View the BFD session of Router B.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr          LD/RD  RH     Holdown(mult)      State  Int
192.168.3.2  192.168.3.1  2/1          1             532  (5 )          Up
       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: STATIC ROUTE
Uptime: 02:18:49
Last packet: Version: 1                       - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0                      - Final bit: 0
Multiplier: 5                          - Length: 24
My Discr.: 1              - Your Discr.: 2
Min tx interval: 200000   - Min rx interval: 200000
Min Echo interval: 0
```

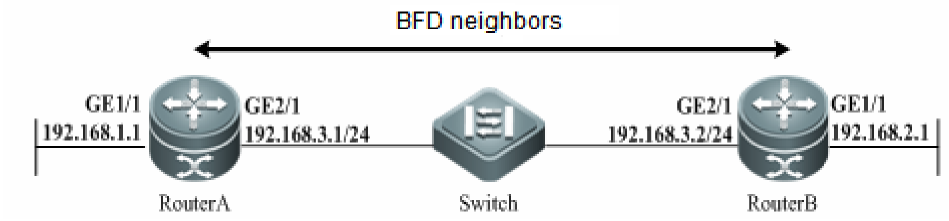
4.9 Example of Configuring BFD for PBR

4.9.1 Networking Requirement

Router A and Router B are interconnected through a L2 switch. Both routers run the PBR protocol and enable the BFD for PBR on the interface. After a link failure between Router B and L2 switch occurs, BFD detects the failure and notifies the PBR of the failure, triggering the PBR removal and preventing the routing error.

4.9.2 Networking Topology

Figure 9 Topology of configuring BFD for PBR



4.9.3 Configuration Tips

- Router A Configuration

# Configure the Routed Port GE2/1, the interface IP address, and the BFD session parameter of the interface for Router A.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.3.1 255.255.255.0
Qtech(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config)# ip address 192.168.1.1 255.255.255.0
```

# Configure the BFD for PBR to detect the neighbor 192.168.3.2.

```
Qtech(config)# ip access-list extended 100
Qtech(config-ext-nacl)# permit ip any 192.168.2.0 0.0.0.255
Qtech(config-ext-nacl)# deny ip any any
Qtech(config-ext-nacl)# exit
Qtech(config)# route-map Example1 permit 10
Qtech(config-route-map)# match ip address 100
Qtech(config-route-map)# set ip precedence priority
Qtech(config-route-map)#set ip next-hop verify-availability 192.168.3.2 bfd
GigabitEthernet 0/1 192.168.3.2
Qtech(config)# end
Qtech#
```

- Router B Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router B.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet 2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.3.2 255.255.255.0
Qtech(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 192.168.2.1 255.255.255.0
```

# Configure the BFD for PBR to detect the neighbor 192.168.3.1.

```
Qtech(config)# ip access-list extended 100
Qtech(config-ext-nacl)# permit ip any 192.168.1.0 0.0.0.255
Qtech(config-ext-nacl)# deny ip any any
Qtech(config-ext-nacl)# exit
Qtech(config)# route-map Example1 permit 10
Qtech(config-route-map)# match ip address 100
Qtech(config-route-map)# set ip precedence priority
Qtech(config-route-map)#set ip next-hop verify-availability 192.168.3.1 bfd
GigabitEthernet 2/1 192.168.3.1
Qtech(config)# end
Qtech#
```

4.9.4 Verification

- View the BFD session of Router A.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr           LD/RD  RH    Holdown(mult)       State  Int
192.168.3.1  192.168.3.2   1/2          1            532  (3 )           Up
       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: PBR
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
```

- View the BFD session of Router B.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr           LD/RD  RH    Holdown(mult)       State  Int
192.168.3.2  192.168.3.1   2/1          1            532  (5 )           Up
       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: PBR
Uptime: 02:18:49
Last packet: Version: 1                        - Diagnostic: 0
I Hear You bit: 1          - Demand bit: 0
Poll bit: 0                      - Final bit: 0
Multiplier: 5                          - Length: 24
My Discr.: 1               - Your Discr.: 2
Min tx interval: 200000    - Min rx interval: 200000
Min Echo interval: 0
```

4.10 Example of Configuring BFD for VRRP

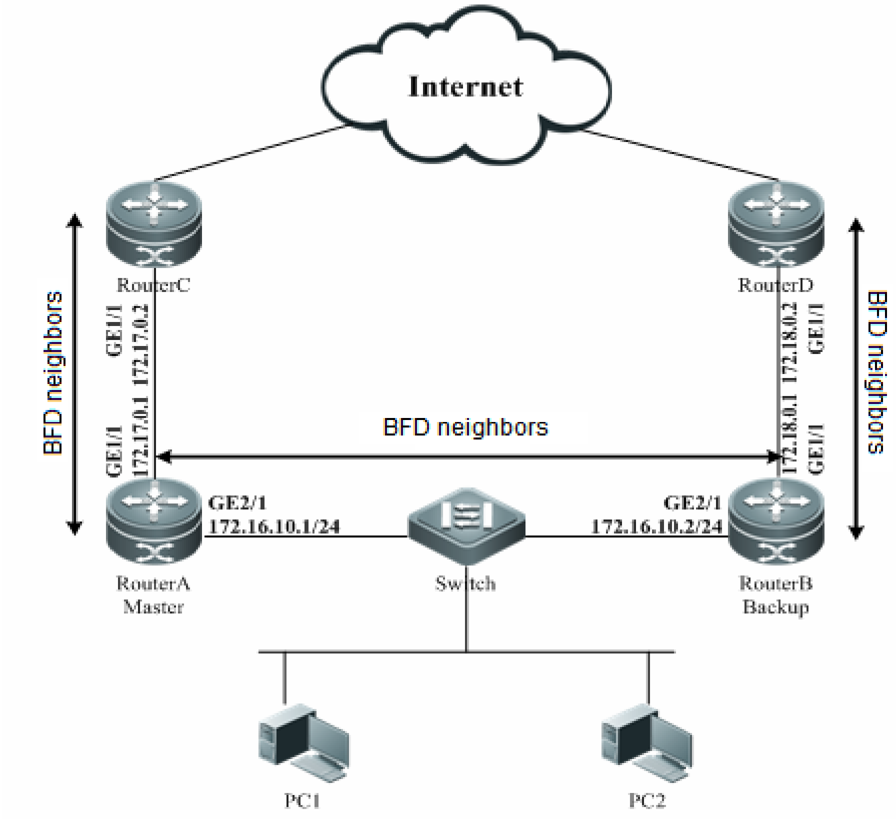
4.10.1 Networking Requirement

Router A and Router B are interconnected through a L2 switch. Both routers run the VRRP protocol and enable the BFD for PBR on the interface to detect the master and backup routers. After a link failure between Router A and L2 switch occurs, BFD detects the failure, notifies VRRP of the failure, and triggers the decrease of the priority of the VRRP master router. As a result, the switchover between the master and backup routers, which enables the backup router rapidly.

Router A and Router B access the Internet through Router C and Router D respectively. Configure the static routes to establish the forwarding path between Router A and Router C, Router B and Router D and enable the BFD to detect the neighbor. At the same time, Router A and Router B are configured the BFD for VRRP to detect the forwarding path between the Router A and Router C, Router B and Router D. The detection failure triggers the decrease of the priority for VRRP master router and switchover between the master and backup routers, which enables the backup router rapidly.

4.10.2 Networking Topology

Figure 10 Topology of configuring BFD for VRRP



4.10.3 Configuration Tips

- Router A Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router A.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 172.16.10.1 255.255.255.0
Qtech(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 172.17.0.1 255.255.255.0
Qtech(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

# Enable VRRP and configure the BFD for VRRP to detect the neighbor 172.16.10.2 and 172.17.0.2 at the same time.

```
Qtech(config-if)# interface GigabitEthernet2/1
Qtech(config-if)# vrrp 1 timers advertise 3
Qtech(config-if)# vrrp 1 ip 172.16.10.3
Qtech(config-if)# vrrp 1 priority 120
Qtech(config-if)# vrrp 1 bfd 172.16.10.2
Qtech(config-if)# vrrp 1 track bfd GigabitEthernet 1/1 172.17.0.2 30
```

# Configure the static route and associate the BFD to detect the neighbor 172.17.0.2:

```
Qtech(config-if)# exit
Qtech(config)# ip route static bfd GigabitEthernet 1/1 172.17.0.2
Qtech(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 1/1 172.17.0.2
Qtech(config)# end
Qtech#
```

- Router B Configuration

# Configure the Routed Port, the IP address, and the BFD session parameter for Router B.

```
Qtech# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 172.16.10.2 255.255.255.0
Qtech(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

# Configure the Routed Port GE 1/1.

```
Qtech(config-if)# exit
Qtech(config)# interface GigabitEthernet1/1
Qtech(config-if)# no switchport (This configuration is unnecessary for routers)
Qtech(config-if)# ip address 172.18.0.1 255.255.255.0
Qtech(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

# Enable VRRP and configure the BFD for VRRP to detect the neighbor 172.16.10.1 and 172.18.0.2 at the same time.

```
Qtech(config-if)# interface GigabitEthernet2/1
Qtech(config-if)# vrrp 1 timers advertise 3
Qtech(config-if)# vrrp 1 ip 172.16.10.3
Qtech(config-if)# vrrp 1 priority 120
Qtech(config-if)# vrrp 1 bfd 172.16.10.1
Qtech(config-if)# vrrp 1 track bfd GigabitEthernet 1/1 172.18.0.2 30
```

# Configure the static route and associate the BFD to detect the neighbor 172.18.0.2.

```
Qtech(config-if)# exit
Qtech(config)# ip route static bfd GigabitEthernet 1/1 172.18.0.2
Qtech(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 1/1 172.18.0.2
Qtech(config)# end
Qtech#
```

4.10.4 Verification

- View the BFD session of Router A.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr           LD/RD  RH    Holdown(mult)       State  Int
172.16.10.1  172.16.10.2   1/2          1            532  (3 )           Up
       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: VRRP
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
```

```
OurAddr             NeighAddr           LD/RD  RH    Holdown(mult)       State  Int
172.17.0.1   172.17.0.2                 2/3          1            532  (3 )
       Up            Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: VRRP,STATIC ROUTE
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
```

View the BFD session of Router B.

```
Qtech# show bfd neighbors details
OurAddr             NeighAddr          LD/RD  RH     Holdown(mult)       State  Int
172.16.10.2  172.16.10.1   2/1          1             532  (3 )             Up
       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: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: VRRP
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.: 1               - Your Discr.: 2
Min tx interval: 200000    - Min rx interval: 200000
Min Echo interval: 0

OurAddr             NeighAddr          LD/RD  RH     Holdown(mult)       State  Int
172.18.0.1          172.18.0.2         1/3           1             532  (3 )
       Up           Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: VRRP,STATIC ROUTE
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
```

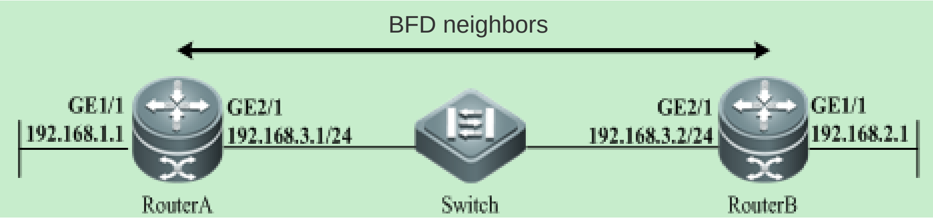
4.11 Example of Configuring QoS Policy in ECHO Mode for Guaranteeing Priority

4.11.1 Networking Requirement

Router A and Router B are interconnected through the layer-2 switch. A traffic pumping device of IXIA is used to pump traffic from Router A to Router B. A QoS policy is configured on Router A to guarantee the forwarding priority of echo packets sent from Router B.

4.11.2 Network Topology

Figure 11 QoS Policy Configuration in ECHO Mode



4.11.3 Configuration Tips

- Configuring Router A

#Configure packets of Port 3785 as BFD echo packets in the ACL.

```
Qtech#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Qtech(config)#ip access-list extended 100
Qtech(config-ext-nacl)#10 permit udp any any eq 3785
Qtech(config-ext-nacl)#
```

#Configure the port queue template.

```
Qtech(config)#port-queue 1
```

#Configure the user queue.

```
Qtech(config)#user-queue uq1 outbound
Qtech(config-user-queue)# cir 1000000 pir 1000000
Qtech(config-user-queue)#
Qtech#
```

#Configure the traffic classifier.

```
Qtech(config)#traffic classifier tc1 or
Qtech(config-traffic-classifier)# if-match acl 100
Qtech(config-traffic-classifier)#
Qtech#
```

#Configure the traffic behavior.

```
Qtech(config)#traffic behavior tb1
Qtech(config-traffic-behavior)# user-queue uq1 outbound
Qtech(config-traffic-behavior)# service-class cs7 color green
Qtech(config-traffic-behavior)#
```

#Configure the traffic policy.

```
Qtech(config)#traffic policy tp1
Qtech(config-traffic-policy)# classifier tcl behavior tb1 precedence 1
Qtech(config-traffic-policy)#
```

#Apply the policy to traffic from the interface to application.

```
Qtech(config)# interface GigabitEthernet2/1
Qtech(config-if- GigabitEthernet2/1)#traffic-policy tp1 outbound
Qtech(config-if- GigabitEthernet2/1)#
```

4.12 Example of Configuring BFD for the L3 Interface

Because the configuration of BFD for the L3 interface is usually used in FRR application and independent usage is not recommended. For details, see description in *MPLS-SCG.doc*.

4.13 Example of Configuring BFD for MPLS

For details, see description in *MPLS-SCG.doc*.

4.14 Example of Configuring BFD for VRRP

For details, see description in *VRRP-PLUS-SCG.doc*.