

2 Configuring RLDP

2.1 Overview

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

2.2 Applications

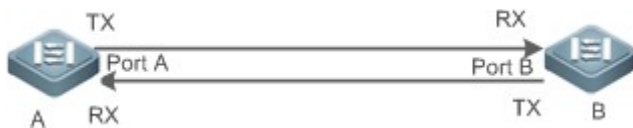
Application	Description
Unidirectional Link Detection	Detect a unidirectional link failure.
Bidirectional Forwarding Detection	Detect a bidirectional link failure.
Downlink Loop Detection	Detect a link loop.

2.2.1 Unidirectional Link Detection

Scenario

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

Figure 2-1



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

Deployment

- Global RLDP is enabled.

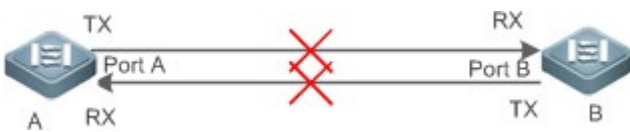
- Configure unidirectional link detection under Port A and Port B and define a method for failure treatment.

2.2.2 Bidirectional Forwarding Detection

Scenario

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

Figure 2-2



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

Deployment

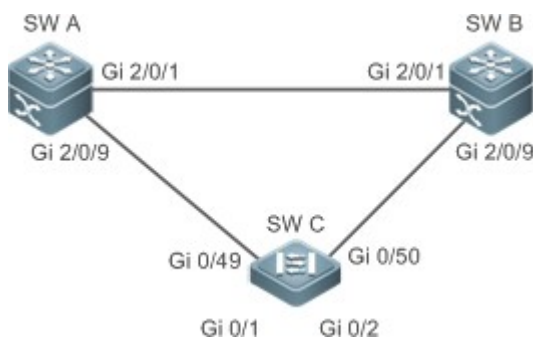
- Global RLDP is enabled.
- Configure BFD under Port A and Port B and define a method for failure treatment.

2.2.3 Downlink Loop Detection

Scenario

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

Figure 2-3



Remarks	A, B and C are layer-2 or layer-3 switches.
----------------	---

A, B and C are interconnected via exchange ports.

Deployment

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

2.3 Features

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

Basic Concepts

↘ Unidirectional Link Failure

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

↘ Bidirectional Link Failure

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

↘ Loop Failure

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

↘ RLDP Packet

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

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

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

↘ **RLDP Detection Interval and Maximum Detection Times**

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

↘ **RLDP Neighbor Negotiation**

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

↘ **Treatment for Failed Port under RLDP**

- Warning: Only print Syslog to indicate a failed port and a failure type.
- Shutdown SVI: Print Syslog, and then inquire an SVI according to the Access VLAN or Native VLAN of a port and shut down the SVI if the port is a physical exchange port or layer-2 AP member port.
- Port violation: Print Syslog, and configure a failed port as in violation state, and the port will enter Linkdown state physically.
- Block: Print Syslog, and configure the forward state of a port as Block, and the port will not forward packets.

↘ **Recovery of Failed Port under RLDP**

- Manual reset: Manually reset all failed ports to initialized state and restart link detection.
- Manual or automatic errdisable recovery: Recover all failed ports to initialized state manually or regularly (30s by default and configurable) and restart link detection.
- Automatic recovery: Under unidirectional or bidirectional link detection, if the treatment for failed ports is not specified as port violation, recover ports to initialized state based on Prob packets and restart link detection.

↘ **Port State under RLDP**

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

↘ **Overview**

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

2.3.1 Deploying RLDP Detection

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

Working Principle

↘ Unidirectional Link Detection

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

↘ Bidirectional Forwarding Detection

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

↘ Downlink Loop Detection

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

Related Configuration

- [Configuring RLDP Detection](#)





By default, RLDP detection is disabled.

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

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

2.4 Configuration

Configuration	Description and Command
---------------	-------------------------

Configuring Basic RLDP Functions	 (Mandatory) It is used to enable RLDP detection under global configuration mode.	
	rldp enable	Enables global RLDP detection on all ports.
	 (Mandatory) It is used to specify under interface configuration mode a detection type and failure treatment for an interface.	
	rldp port	Enables RLDP detection on a port and specifies a detection type and failure treatment.
	 (Optional) It is used to configure a detection interval, detection times and neighbor negotiation under global configuration mode.	
	rldp detect-interval	Modifies global RLDP parameters on all ports, such as the detection interval, maximum detection times and neighbor negotiation.
	rldp detect-max	
	rldp neighbor-negotiation	
	rldp error-recover interval	Configures the global time interval for recovering the state of the failed port.
	 (Optional) It is used under privileged mode.	
rldp reset	Recovers all ports.	

2.4.1 Configuring Basic RLDP Functions

Configuration Effect

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

Notes

- Loop detection is effective to all member ports of an AP when configured on one of the ports. Unidirectional link detection and bidirectional forwarding detection are effective only on an AP member port.
- The loop detection on a physical port added to an AP shall be configured the same as that of the other member ports. There are three cases. First, if loop detection is not configured on a newly-added port but on the existing member ports, the new port adopts the configuration and detection results of the existing ports. Second, if a newly-added port and the existing member ports have different loop detection configuration, the new port adopts the configuration and detection results of the existing ports.
- When configuring the RLDP on an AP port, you may configure failure treatment only as "shutdown-port", to which other configurations will be modified.

- When "shutdown-port" is configured on a port, RLDP detection cannot be restored in case of a failure. After troubleshooting, you may run the **rldp reset** or **errdisable recovery** command to restore the port and resume detection. For configuration of the **errdisable recovery** command, please refer to the *Configuring Interface*.
- The VLAN-based loop detection function (configured by the **rldp port vlan-loop-detect** command) can be configured only on multi-VLAN ports such as trunk and hybrid ports. It is recommended not to configure this function on access or routed ports. This function does not take effect when configured on routed ports.
- It is recommended not to configure the **rldp port vlan-loop-detect** command and the **rldp port loop-detect** command on the same port. The **rldp port loop-detect** command is mainly configured on access ports to detect downlink loops.
- The VLAN list for the VLAN-based loop detection function needs to be configured in consideration of performance, and should include only VLANs that possibly encounter loops to reduce invalid detection and improve detection performance.
- The VLAN-based loop detection function can be configured only on AP member ports. It is recommended to configure the same detection VLAN on all member ports of an AP to ensure normal loop detection.

Configuration Steps

▾ Enabling RLDP

- Mandatory.
- Enable RLDP detection on all ports under global configuration mode.

▾ Enabling Neighbor Negotiation

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

▾ Configuring Detection Interval

- Optional.
- Configure a detection interval under global configuration mode.

▾ Configuring Maximum Detection Times

- Optional.
- Specify the maximum detection times under global configuration mode.

▾ Configuring a Time Interval for Recovering State of the Failed Port

- Optional.
- Configure the time interval for recovering the state of the failed port under global configuration mode.

↘ **Configuring Detection under Port**

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

↘ **Restoring All Failed Ports**

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

Verification

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

Related Commands

↘ **Enabling Global RLDP Detection**

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

↘ **Enabling RLDP Detection on Interface**

Command	<code>rldp port { unidirection-detect bidirection-detect loop-detect } { warning shutdown-svi shutdown-port block }</code> <code>rldp port vlan-loop-detect { warning isolate-vlan} vlan <i>vlan-list</i></code>
Parameter Description	<p>unidirection-detect: Indicates unidirectional link detection.</p> <p>bidirection-detect: Indicates bidirectional forwarding detection.</p> <p>loop-detect: Indicates downlink loop detection.</p> <p>vlan-loop-detect: Indicates VLAN-based loop detection.</p> <p>warning: Indicate the failure treatment is warning.</p> <p>shutdown-svi: Indicate the failure treatment is closing the SVI that the interface is on.</p> <p>shutdown-port: Indicates the failure treatment is port violation.</p> <p>block: Indicates the failure treatment is disabling learning and forwarding of a port.</p> <p>isolate-vlan: Indicates that the failure treatment is isolation for the faulty VLAN.</p> <p>vlan-list: Indicates the VLANs to be detected.</p>
Command	Interface configuration mode

Mode	
Usage Guide	The interfaces include layer-2 switch ports, layer-3 routed ports, layer-2 AP member ports, and layer-3 AP member ports.

✚ Modifying Global RLDP Detection Parameters

Command	rldp {detect-interval <i>interval</i> detect-max <i>num</i> neighbor-negotiation }
Parameter Description	detect-interval <i>interval</i> : Indicates a detection interval. detect-max <i>num</i> : Indicates detection times. neighbor-negotiation : Indicates neighbor negotiation.
Command Mode	Global configuration mode
Usage Guide	Modify all RLDP parameters on all ports when necessary.

✚ Recovering Failed Port

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

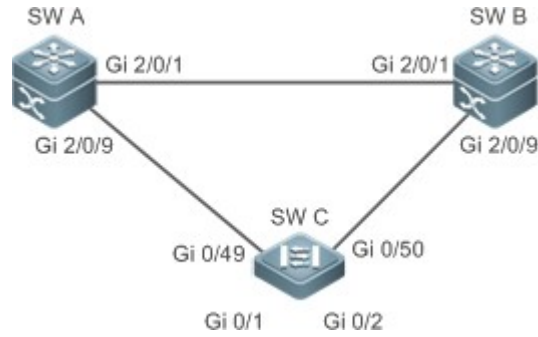
✚ Displaying RLDP State Information

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

Configuration Example

✚ Enabling RLDP Detection in Ring Topology

Scenario Figure 2-4	As shown in the following figure, the aggregation and access sections are in a ring topology. The STP is enabled on all devices to prevent loop and provide redundancy protection. To avoid a unidirectional or bidirectional link failure resulting in STP failure, RLDP unidirectional and bidirectional link detection is enabled between aggregation devices as well as between an aggregation device and the access device. To avoid loop due to wrong downlink connection of the aggregation devices, enable RLDP downlink loop detection on the downlink ports of the aggregation devices and of the access device. To avoid loop due to wrong downlink connection of the access device, enable RLDP downlink loop detection on the downlink ports of the access device.
--------------------------------------	---



Configuration Steps

- ✘ SW A and SW B are aggregation devices, and SW C is an access device. Users connected to SW C. SW A, SW B and SW C are structured in a ring topology, and the STP is enabled on each of them. For STP configuration, refer to relevant configuration guide.
- ✘ Enable the RLDP on SW A, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port.
- ✘ Enable the RLDP on SW B, enable unidirectional and bidirectional link detection on the two ports, and enable loop detection on the downlink port.
- ✘ Enable the RLDP on SW C, enable unidirectional and bidirectional link detection on the two uplink ports, and enable loop detection on the two downlink ports.

A

```
A#configure terminal
A(config)#rldp enable
A(config)#interface GigabitEthernet 2/0/1
A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)# exit
A(config)#interface GigabitEthernet 2/0/9
A(config-if-GigabitEthernet 2/0/1)#rldp port unidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port bidirection-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#rldp port loop-detect shutdown-port
A(config-if-GigabitEthernet 2/0/1)#exit
```

B

Apply the configuration on SW A.

C

```
C#configure terminal
C(config)#rldp enable
C(config)#interface GigabitEthernet 0/49
C(config-if-GigabitEthernet 0/49)#rldp port unidirection-detect shutdown-port
```

	<pre> C(config-if-GigabitEthernet 0/49)#rldp port bidirection-detect shutdown-port C(config-if-GigabitEthernet 0/49)# exit C(config)#interface GigabitEthernet 0/50 C(config-if-GigabitEthernet 0/50)#rldp port unidirection-detect shutdown-port C(config-if-GigabitEthernet 0/50)#rldp port bidirection-detect shutdown-port C(config-if-GigabitEthernet 0/50)#exit C(config)#interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port C(config-if-GigabitEthernet 0/1)#exit C(config)#interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)# rldp port loop-detect shutdown-port C(config-if-GigabitEthernet 0/2)#exit </pre>
Verification	<p>✎ Check the RLDP information on SW A, SW B and SW C. Take SW A for example.</p>
A	<pre> A#show rldp rldp state : enable rldp hello interval: 3 rldp max hello : 2 rldp local bridge : 08c6.b315.0122 Interface GigabitEthernet 2/0/1 port state : normal neighbor bridge : 08c6.b315.0121 neighbor port : GigabitEthernet 2/0/1 unidirection detect information: action: shutdown-port state : normal bidirection detect information: action: shutdown-port state : normal Interface GigabitEthernet 2/0/9 </pre>

```

port state      : normal

neighbor bridge : 08c6.b315.0123

neighbor port   : GigabitEthernet 0/49

unidirection detect information:

    action: shutdown-port

    state : normal

bidirection detect information:

    action: shutdown-port

    state : normal

loop detect information:

    action: shutdown-port

    state : normal

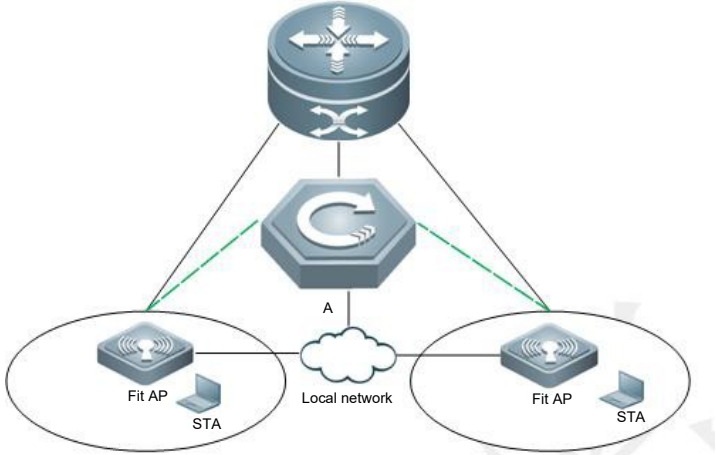
```

Common Errors

- RLDP functions and private multicast address authentication or TPP are enabled at the same time.
- Neighbor negotiation is not enabled when configuring unidirectional or bidirectional link detection. The RLDP should be enabled on a neighbor device, or otherwise a unidirectional or bidirectional failure will be detected.
- If RLDP detection is configured to be implemented after neighbor negotiation while configuring unidirectional or bidirectional link detection, detection cannot be implemented as no neighbor can be learned due to a link failure. In this situation, you are suggested to recover the link state first.
- You are suggested not to specify the failure treatment as Shutdown SVI under a routed port.
- You are suggested not to specify the failure treatment as Block for a port, on which a loop protection protocol is enabled, for example, the STP.

📌 Configuring RLDP Loop Detection on Wireless APs

Scenario Figure 2-5	As shown in the following figure, a large number of APs exist in the wireless AP scenario. If the RLDP loop detection function is configured and modified on APs one by one, the workload is heavy. The RLDP loop detection configurations can be pushed from the AC device to all online APs (or an independent AP).
--------------------------------------	---

	
<p>Configuration Steps</p>	<ul style="list-style-type: none"> ✎ Log in to the AC device and enter the AP configuration mode. ✎ Enable the RLDP loop detection function on the wired ports of the corresponding AP. ✎ Enable the RLDP function on corresponding APs in global configuration mode. ✎ On corresponding APs, configure the recovery time for the RLDP violated port.
<p>A</p>	<pre>A#configure terminal A(config)#ap-config all A(config-ap)#exec-cmd mode "int gi 0/1" cmd "rldp port loop-detect shutdown-port" A(config-ap)#exec-cmd mode configure cmd "rldp enable" A(config-ap)#exec-cmd mode configure cmd "errdisable recovery interval 600"</pre>
<p>Verification</p>	<ul style="list-style-type: none"> ✎ On the AC device, check the RLDP loop detection configurations.
<p>A</p>	<pre>A# show run ! ap-config all exec-cmd mode "int gi 0/1" cmd "rldp port loop-detect shutdown-port" exec-cmd mode configure cmd "rldp enable" exec-cmd mode configure cmd "errdisable recovery interval 600" !</pre>

Common Errors

- When the **exec-cmd** command is executed for interface configuration, the input of the corresponding AP wired port is incorrect.
- When the RLDP loop detection configurations are modified, the **no exec-cmd** command is not executed to delete the original configurations or the **exec-cmd** command is not re-executed to cancel the configurations.

2.5 Monitoring

Displaying

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