WAP680ax Series Access Points

Reliability Configuration

Legal Notice

Warranty

This publication is subject to change.

Teldat S.A. offers no warranty whatsoever for information contained in this manual.

Teldat S.A. is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Reliability Configuration

1 Configuring RLDP

1.1 Overview

The Rapid Link Detection Protocol (RLDP) is an Ethernet link failure detection protocol, which is used to rapidly detect unidirectional link failures, bidirectional link failures, and downlink loop failures. When a failure is found, RLDP automatically shuts down relevant ports or asks users to manually shut down the ports according to the configured failure handling methods, to avoid incorrect forwarding of traffic or Ethernet L2 loops.

Protocols and Standards

- N/A

1.2 Applications

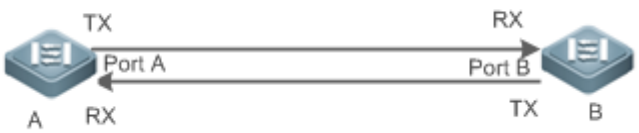
Application	Description
Configuring Unidirectional Link Detection	Detect unidirectional link failures.
Configuring Bidirectional Link Detection	Detect bidirectional link failures.
Configuring Downlink Loop Detection	Detect loop failures.

1.2.1 Configuring Unidirectional Link Detection

Scenario

As shown in Figure 1-1, device A is connected with device B through an optical fiber. The two lines are the Tx and Rx lines of the optical fiber. Unidirectional link detection of RLDP is enabled on device A and device B. If a fault occurs on either the Tx end of device A or Rx end of device B or on either the Rx end of device A or Tx end of device B, RLDP can detect the unidirectional failure and handle it. If the failure is eliminated, the administrator can manually restore the RLDP state on devices A and B and restart detection.

Figure 1-1



Remarks	A and B are layer-2 or layer-3 devices.

	The Tx end of port A on device A is connected with the Rx end of port B on device B. The Rx end of port A on device A is connected with the Tx end of port B on device B.

Deployment

- Enable RLDP globally.
- Configure unidirectional link detection of RLDP on ports and define a method for handling unidirectional failures.

1.2.2 Configuring Bidirectional Link Detection

Scenario

As shown in Figure 1-2, device A is connected with device B through an optical fiber. The two lines are the Tx and Rx lines of the optical fiber. Bidirectional link detection of RLDP is enabled on device A and device B. If a fault occurs on the Tx end of device A and Rx end of device B or on the Rx end of device A and Tx end of device B, RLDP can detect a bidirectional failure and handle it. If the failure is eliminated, the administrator can manually restore the RLDP state on devices A and B and restart detection.

Figure 1-2

Remarks	A and B are layer-2 or layer-3 devices. The Tx end of port A on device A is connected with the Rx end of port B on device B. The Rx end of port A on device A is connected with the Tx end of port B on device B.

Deployment

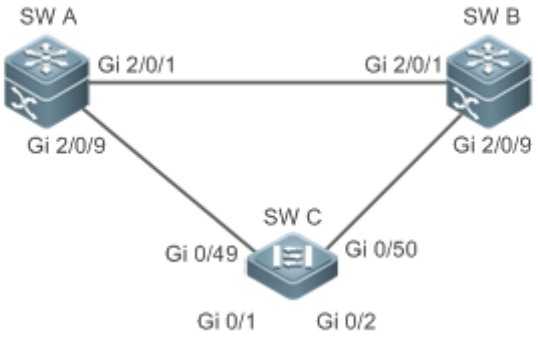
- Enable RLDP globally.
- Configure bidirectional link detection of RLDP on ports and define a method for handling bidirectional failures.

1.2.3 Configuring Downlink Loop Detection

Scenario

As shown in Figure 1-3, devices A, B, and C form a network loop. Downlink loop detection of RLDP is enabled on device A. RLDP can detect loop failures and make responses.

Figure 1-3



Remarks	A, B, and C are layer-2 or layer-3 devices. A, B, and C are interconnected through switching ports.

Deployment

- Enable global RLDP on device A.
- Configure downlink loop detection of RLDP for the ports that connect A and B and that connect A and C and define a method for handling loop failures.

1.3 Features

A typical Ethernet link detection mechanism detects physical link connectivity through auto-negotiation at the physical layer. However, this detection mechanism has limitations. In some cases, devices are connected and work normally at the physical layer but L2 link communication fails or is abnormal. RLDP recognizes a neighbor device and detects whether a link failure exists by exchanging prob packets, echo packets, or loop packets with the neighbor device.

Basic Concepts

Unidirectional Link Failure

A unidirectional link failure occurs when two optical fibers are crossly connected, one optical fiber is not connected or disconnected, one line in a twisted-pair cable is disconnected, or unidirectional disconnection occurs on an intermediate device between two devices. A unidirectional link failure can lead to incorrect forwarding of traffic or the failure of a loop protection protocol such as Spanning Tree Protocol (STP).

Bidirectional Link Failure

A bidirectional link failure occurs when two optical fibers are disconnected, two lines in a twisted-pair cable are disconnected, or bidirectional disconnection occurs on an intermediate device between two devices. A bidirectional link failure can lead to the incorrect forwarding of traffic.

Loop Failure

A loop failure occurs when a downlink port of a device is incorrectly connected with another device and a loop is formed. A loop failure can result in a broadcast storm.

RLDP Packet

RLDP packets include prob packets, echo packets, and loop packets.

- Prob packets: L2 multicast packets used for neighbor negotiation, and unidirectional or bidirectional link detection. The default packet encapsulation format is the Subnetwork Access Protocol (SNAP) type, which automatically changes to EthernetII if a neighbor sends EthernetII packets.
- Echo packets: L2 unicast packets in response to prob packets and used for unidirectional or bidirectional link detection. The default encapsulation format is of the SNAP type, which automatically changes to EthernetII if a neighbor sends EthernetII packets.
- Loop packets: L2 multicast packets for downlink loop detection. They can only be received by senders. The default encapsulation format of the packets is of the SNAP type.

RLDP Detection Interval and Maximum Detection Count

A detection interval and the maximum detection count can be configured for 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 count determine the maximum detection time (Detection interval × Maximum detection count + 1) for unidirectional or bidirectional link detection. If neither a prob nor an echo packet from a neighbor is correctly received within the maximum detection time, the handling of unidirectional or bidirectional failures is triggered.

RLDP Neighbor Negotiation

When configured with unidirectional or bidirectional link detection, a port can learn a peer device as its neighbor. One port can learn only one neighbor, which is changeable. If the negotiation function is enabled, unidirectional or bidirectional link detection starts after a port finds a neighbor through negotiation. Negotiation is considered successful if the port receives a prob packet from the neighbor. However, if RLDP is enabled on a port after a failure occurs, the port fails to learn a neighbor and detection fails to be started. In this case, you are advised to rectify the link failure first.

Handling Methods for RLDP Failed Ports

- Warning: Only the relevant system log is printed to indicate the failed port and the failure type.
- Shutdown SVI: A system log is printed. If the failed port is a physical switching port or member port of an L2 aggregate port (AP), the switch virtual interface (SVI) is queried based on the access virtual local area network (VLAN) or native VLAN of the port, and then the SVI is shut down.
- Errdisable: A system log is printed, the failed port is set to the errdisable state, and the port enters the linkdown state physically.
- Block: A system log is printed, the forwarding state of the failed port is set to Block, and the port does not forward received packets.
- isolate-vlan: A system log is printed, and the looped VLAN is isolated.

Recovery Methods for RLDP Failed Ports

- Manual reset: Manually reset all the failed ports to the initialized state to restart link detection.
- Manual or automatic execution of **errdisable recovery**: Recover all the failed ports to the initialized state manually or regularly (30s by default and configurable) and restart link detection.
- Automatic recovery: Under unidirectional or bidirectional link detection, if the handling method specified for failed ports is not entering the errdisable state, the ports can automatically recover to the initialized state based on prob packets exchanged with the neighbor and restart link detection.
- Automatic execution of **rldp error-recover interval**: Recover all the failed ports to the initialized state regularly (configurable) and restart link detection.

RLDP Port Status

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

Overview

Feature	Description
Enabling RLDP Detection	Enable unidirectional link detection, bidirectional link detection, or downlink loop detection to discover unidirectional, bidirectional, or loop failures and handle the failures.

1.3.1 Enabling RLDP Detection

RLDP provides unidirectional link detection, bidirectional link detection, downlink loop detection, and VLAN loop detection.

Working Principle

Unidirectional Link Detection

After unidirectional link detection is enabled, a port sends prob packets to and receives echo packets from a neighbor regularly. It also receives prob packets from the neighbor and replies with echo packets to the neighbor. If the port receives only prob packets but no echo packets, or none of them from the neighbor within the maximum detection time, handling of a unidirectional failure is triggered and the detection stops.

Bidirectional Link Detection

After bidirectional link detection is enabled, a port sends prob packets to and receives echo packets from a neighbor regularly. It also receives prob packets from the neighbor and replies with echo packets to the neighbor. If the port receives neither prob packets nor echo packets from the neighbor within the maximum detection time, handling of a bidirectional failure is triggered and the detection stops.

Downlink Loop Detection

After downlink loop detection is enabled on ports, the ports send loop packets regularly. A loop failure is triggered in the following scenarios: The transmission and receiving ports of the packets are the same routed port or L3 AP

member port; the transmission and receiving ports of the packets are switching ports or L2 AP member ports, the default VLANs of the ports are the same, and forwarding states of the ports are Forward. The failure is handled according to the configured method, and the detection stops.

Related Configuration

- Configure RLDP detection.

  The detection function is disabled by default.

  Run the **rldp enable** command in global configuration mode or the **rldp port** command in interface configuration mode to enable RLDP detection and specify the detection type and failure handling method.

  Based on the actual environment, run the **rldp neighbor-negotiation** command to specify neighbor negotiation, the **rldp detect-interval** command to specify the detection interval, the **rldp detect-max** command to specify the maximum detection count, the **rldp error-recover interval** command to recover failed ports regularly, and the **rldp reset** command to recover failed ports.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic RLDP Functions	(Mandatory in global configuration mode) It is used to enable RLDP detection globally.	
	rldp enable	Enables RLDP detection globally to apply RLDP detection to all ports.
	(Mandatory in interface configuration mode) It is used to specify the detection type and failure handling method on a port.	
	rldp port	Enables RLDP detection on a port and specifies the detection type and failure handling method.
	(Optional in global configuration mode) It is used to specify the detection interval, maximum detection count, and whether neighbor negotiation is required.	
	rldp detect-interval	Modifies RLDP configuration parameters globally, including the detection interval, maximum detection count, neighbor negotiation, which can take effect to RLDP detection on all ports.
	rldp detect-max	
	rldp neighbor-negotiation	

	rldp error-recover interval	Configures an interval globally for RLDP to recover failed ports. No interval is configured by default.
	(Optional in privilege EXEC mode)	
	rldp reset	Recovers failed ports in privilege EXEC mode, which can take effect to RLDP detection on all ports.

1.4.1 Configuring Basic RLDP Functions

Configuration Effect

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

Notes

- Loop detection configured on an AP member port takes effect on all the member ports of the AP. Unidirectional link detection and bidirectional link detection configured on an AP member port take effect only on the AP member port.
- The loop detection configuration of a physical port added to an AP must be the same as that of the other member ports of the AP. If loop detection is not configured on the new member port but on the existing member ports or loop detection configured on the new member port is different from that on existing member ports, the new port adopts the configuration and detection results of the existing member ports.
- When RLDP is configured on an AP member port, only the "shutdown-port" handling method can be configured. If the failure handling method is not "shutdown-port", it is modified to "shutdown-port" and takes effect.
- After the "shutdown-port" handling method is configured on a port, the port cannot resume RLDP detection in the case of a failure. After confirming that the failure is rectified, you can run the **rldp reset** or **errdisable recovery** command to restore the port and restart detection.

Configuration Steps

Enabling RLDP Detection Globally

- Mandatory.
- After RLDP detection is configured in global configuration mode, RLDP detection can be started on all ports.

Configuring Neighbor Negotiation Globally

- Optional.
- After neighbor negotiation is configured in global configuration mode, RLDP detection on a port is started after successful neighbor negotiation.

Configuring the Detection Interval Globally

- Optional.
- Configure the detection interval in global configuration mode.

Configuring the Maximum Detection Count Globally

- Optional.
- In global configuration mode,
- specify the maximum detection count.

Configuring the Interval for Recovering Failed Ports Globally

- Optional.
- Configure the interval for recovering failed ports in global configuration mode.

Enabling RLDP Detection on a Port

- Mandatory.
- Perform this configuration in interface configuration mode.
- In interface configuration mode, configure unidirectional link detection, bidirectional link detection, downlink loop detection, or VLAN loop detection of RLDP and specify a failure handling method.

Recovering All Failed Ports in Privileged EXEC Mode

- Optional.
- Perform this configuration in privileged EXEC mode to restore all the failed ports and restart detection.

Verification

- Display RLDP information on the device, including global, port, and neighbor information.

Related Commands

Enabling RLDP Globally

Command	**rldp enable**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	This command is used to enable RLDP detection globally.

Enabling RLDP Detection on a Port

Command	**rldp port { unidirection-detect | bidirection-detect | loop-detect } { warning | shutdown-svi | shutdown-port | block }**
Parameter Description	**unidirection-detect**: Enables unidirectional link detection. **bidirection-detect**: Enables bidirectional link detection. **loop-detect**: Enables downlink loop detection. **warning**: Sends a warning upon a failure. **shutdown-svi**: Disables the SVI to which a port belongs upon a failure. **shutdown-port**: Sets a port to the errdisable state upon a failure. **block**: Disables the learning and forwarding capabilities of a port upon a failure.
Command Mode	Interface configuration mode
Usage Guide	Ports include layer-2 switching ports, layer-3 routed ports, layer-2 AP member ports, and layer-3 AP member ports. The port that detects a downlink loop failure is at random. For example, if RLDP downlink loop detection is configured on downlink ports A and B, the configured failure handling method is warning on downlink port A and shutdown-port on downlink port B, and a downlink loop exists between ports A and B, port A may detect a downlink loop failure before port B. After the failure handling method on port A takes effect, port A no longer sends packets or detects the downlink loop status. Port B does not receive prob packets from port A and cannot detect downlink loop failures. As a result, the downlink loop failure still exists in the environment. To ensure that downlink loop failures in actual scenarios can be rectified, the loop failure handling method configured on downlink ports in the same loop must be the same and cannot be warning. The monitor policy can be configured in unidirectional link detection mode for association with the Ethernet Ring Protection Switching (ERPS) protocol to ensure that ERPS can detect unidirectional link connection in time.

Modifying RLDP Detection Parameters Globally

Command	**rldp** { **detect-interval** *interval* | **detect-max** *num* | **neighbor-negotiation** }
Parameter Description	**detect-interval** *interval*: Specifies the detection interval. **detect-max** *num*: Specifies the maximum detection count. **neighbor-negotiation**: Specifies whether neighbor negotiation is required.
Command Mode	Global configuration mode

Usage Guide	This command is used to modify all RLDP detection parameters for all ports when the actual environment changes.

Configuring the Interval for Recovering Failed Ports Globally

Command	**rldp error-recover interval** *interval*
Parameter Description	*interval*: Interval for recovering failed ports, in seconds. The value range is from 30 to 86400. By default, no interval is configured.
Command Mode	Global configuration mode
Usage Guide	This command is used to recover RLDP failed ports regularly. If a loop failure is rectified, the environment can be restored automatically.

Recovering RLDP Failed Ports

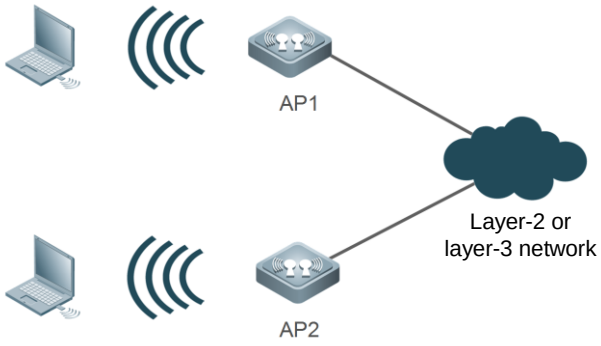
Command	**rldp reset**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to reset all RLDP failed ports and restart detection.

Displaying RLDP Status Information

Command	**show rldp** [**interface** *interface-type interface-number*]
Parameter Description	*interface-type interface-number*: Name of the interface to be queried.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	This command is used to display the status information of RLDP.

Configuration Example

Configuring RLDP Loop Detection on Wireless APs

Scenario Figure 1-4	As shown in Figure 1-5, RLDP loop detection is configured on wireless APs. 
Configuration Steps	● Enable RLDP loop detection on the AP wired ports. ● Enable RLDP on APs in global configuration mode. ● On APs, configure the recovery time for ports that are set to the errdisable state by RLDP.

AP1, AP2	`Hostname#configure terminal`
	`Hostname(config)# rldp enable`
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# errdisable recovery interval 500`
	`Hostname(config-if-GigabitEthernet 0/1)# rldp port loop-detect shutdown-port`

Verification	● On the AP, check whether the RLDP loop detection configurations take effect.

AP1, AP2	`Hostname# show run`
	`!`
	`rldp enable`
	`…`
	`interface GigabitEthernet 0/1`
	` errdisable recovery interval 500`
	` encapsulation dot1Q 1`
	` rldp port loop-detect shutdown-port`
	`!`

Common Errors

N/A

1.5 Monitoring

Displaying

Description	Command
Displays the RLDP running status.	**show rldp** [**interface** *interface-type interface-number*]