Table of Contents

Chapter 1 DLDP Configuration 1-1
1.1 DLDP Overview 1-1
1.1.1 DLDP Fundamentals 1-2
1.1.2 Precautions During DLDP Configuration 1-5
1.2 DLDP Configuration 1-6
1.2.1 Configuring DLDP 1-6
1.2.2 Resetting DLDP Status 1-7
1.3 DLDP Configuration Example 1-8
Chapter 2 DLDP Configuration Commands 2-1
2.1 DLDP Configuration Commands 2-1
2.1.1 debugging dldp 2-1
2.1.2 display dldp 2-1
2.1.3 dldp 2-3
2.1.4 dldp authentication-mode 2-4
2.1.5 dldp interval 2-5
2.1.6 dldp reset 2-5
2.1.7 dldp unidirectional-shutdown 2-6
2.1.8 dldp work-mode 2-7

Chapter 1 DLDP Configuration

1.1 DLDP Overview

You may have encountered unidirectional links in networking. When a unidirectional link occurs, the local device can receive packets from the peer device through the link layer, but the peer device cannot receive packets from the local device. See Figure 1-1 and Figure 1-2. Unidirectional links can cause many problems, spanning tree topology loop for example.

Device Link Detection Protocol (DLDP) can detect the link status of the optical fiber cable or copper twisted pair (such as super category 5 twisted pair). If DLDP finds a unidirectional link, it disables the related port automatically or informs users to disable it manually depending on specific configuration, to avoid potential network problems.

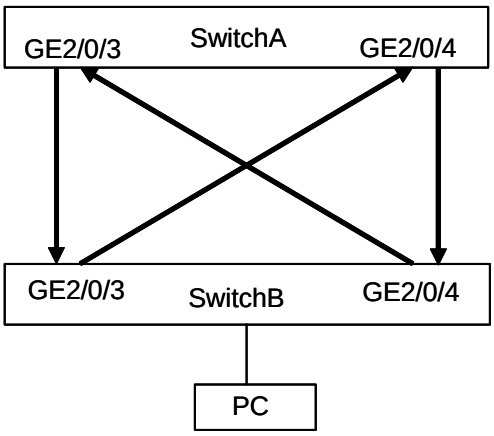

Figure 1-1 Fiber cross-connection

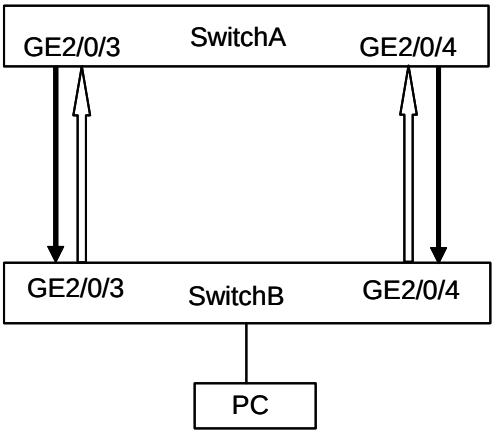

Figure 1-2 Fiber correct connection/disconnection in one direction

DLDP provides the following features:

- As a link layer protocol, it works together with the physical layer protocol to monitor the link status of a device.
- While the auto-negotiation mechanism on the physical layer detects physical signals and faults; DLDP identifies peer devices and unidirectional links, and disables unreachable ports.
- The auto-negotiation mechanism and DLDP, when enabled, work together to detect and disable physical and logical unidirectional links, and to prevent the failure of other protocols, such as STP (Spanning Tree Protocol).
- Even if the links of both ends can normally operate individually on the physical layer, DLDP can detect (at the link layer) if these links are set up correctly and packets can be exchanged normally between the two ends. This cannot be implemented by the auto-negotiation mechanism.

1.1.1 DLDP Fundamentals

I. DLDP status

DLDP may be in one of the six states: initial, inactive, active, advertisement, probe and disable.

Table 1-1 DLDP status

Status	Description
Initial	DLDP is not enabled.
Inactive	DLDP is enabled but the corresponding link is down
Active	DLDP is enabled and the link is up, or an neighbor entry is cleared
Advertisement	All neighbors communicate normally in both direction, or DLDP remains in active status for more than five seconds and enters this status. It is a stable status when no unidirectional link is found
Probe	DHCP sends packets to check if it is an unidirectional link. It enables the probe sending timer and an echo waiting timer for each target neighbor.
Disable	DLDP detects an unidirectional link, or finds (in enhanced mode) that a neighbor disappears. At this time, DLDP does not receive or send DLDP packets.

II. DLDP timers

DLDP works with the following timers:

Table 1-2 DLDP timers

Timer	Description
Advertisement sending timer	Time interval for sending advertisement packets, which can be configured with a particular command. By default, the time interval is 10 seconds.
Probe sending timer	The time interval is 1 second. In probe status, DLDP sends two probe packets every second.
Echo waiting timer	It is enabled when DLDP enters probe status. The timeout time is 10 seconds. If no echo packet is received from the neighbor when the Echo waiting timer expires, the local end is set to unidirectional communication status and the state machine turns into disable status. DLDP outputs log and tracking information, sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompt the user to disable the port manually. At the same time, DLDP deletes the neighbor entry.
Entry aging timer	When a new neighbor joins, a neighbor entry is created, and the corresponding entry aging timer is enabled. When an advertisement packet is received from a neighbor, the neighbor entry is updated, and the corresponding entry aging timer is reset. In normal mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP sends an advertisement packet with RSY tag, and deletes the neighbor entry. In enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer. The time interval set for the entry aging timer is three times of that for the advertisement timer.
Enhanced timer	In enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer for the neighbor. The timeout time for the enhanced timer is 10 seconds. The enhanced timer then sends two probe packets every one second and totally eight packets continuously to the neighbor. If no echo packet is received from the neighbor when the Echo waiting timer expires, the local end is set to unidirectional communication status and the state machine turns into disable status. DLDP outputs log and tracking information, sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompt the user to disable the port manually. DLDP deletes the neighbor entry.

III. DLDP operating mode

DLDP can operate in two modes: normal and enhanced.

Table 1-3 DLDP operating mode and neighbor entry aging

DLDP operating mode	Whether DLDP probes neighbor during neighbor entry aging	Whether entry aging timer is enabled during neighbor entry aging	Whether enhanced timer is enabled when entry aging timer expire
Normal mode	No	Yes (the neighbor entry ages after the entry aging timer expires)	No
Enhanced mode	Yes	Yes (the enhancement timer is enabled after the entry aging timer expires)	Yes (When the enhanced timer expires, the local end is set to single pass status, and the neighbor entry ages)

IV. DLDP implementation

1) If the link is up after DLDP is enabled on the port, DLDP sends DLDP packets to the peer device, and analyses and processes DLDP packets received from the peer device. DLDP in different status sends different packets.

Table 1-4 Types of packets sent by DLDP

DLDP status	Packet types
Active	Advertisement packets, including those with or without RSY tags
Advertisement	Advertisement packets
Probe	Probe packets

2) DLDP analyzes and processes received packets as follows:

- In authentication mode, DLDP authenticates the packets on the port, and discards those do not pass the authentication.
- DLDP processes the received DLDP packets as follows:

Table 1-5 Process received DLDP packets

Packet type	Processing procedure	
Advertisement packet	Extracts neighbor information	If this neighbor entry does not exist on the local device, DLDP creates the neighbor entry, enables the entry aging timer, and turns to probe status.
		If the neighbor entry already exists on the local device, DLDP resets the entry aging timer.

<table>
<tr><th>Packet type</th><th colspan="5">Processing procedure</th></tr>
<tr><td>Flush packet</td><td colspan="5">Deletes the neighbor entry from the local device</td></tr>
<tr><td rowspan="2">Probe packet</td><td colspan="2" rowspan="2">Sends echo packets containing both neighbor and its own information to the peer</td><td colspan="3">Creates the neighbor entry if this neighbor entry does not exist on the local device.</td></tr>
<tr><td colspan="3">If the neighbor entry already exists on the local device, refreshes the entry aging timer.</td></tr>
<tr><td rowspan="4">Echo packet</td><td rowspan="4">Checks whether the local device is in probe status</td><td>No</td><td colspan="3">Discards this echo packet</td></tr>
<tr><td rowspan="3">Yes</td><td rowspan="3">Checks whether neighbor information in the packet is the same as that on the local device</td><td>No</td><td>Discards this echo packet</td></tr>
<tr><td rowspan="2">Yes</td><td>Sets the neighbor flag bit to bidirectional</td></tr>
<tr><td>If all neighbors are in bidirectional communication state, DLDP turns from probe status to advertisement status, and sets the echo waiting timer to 0.</td></tr>
</table>

3) If no echo packet is received from the neighbor, DLDP performs the following processing:

Table 1-6 Processing when no echo packet received from the neighbor

No Echo packet received from the neighbor	Processing procedure
In normal mode, no echo packet is received when the echo waiting timer expires	DLDP turns into disable status. It outputs log and tracking information, sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompt the user to disable the port manually. DLDP sends the RSY message and deletes the neighbor entry.
In enhanced mode, no echo packet is received when the enhanced timer expires	

1.1.2 Precautions During DLDP Configuration

- DLDP works only when the link is up.
- To insure unidirectional links can be detected, you should make sure: DLDP is enabled on both ends, and the time interval for sending advertisement packets, authentication mode and password are set consistent on both ends.
- You can adjust the time interval for sending advertisement packets in different network circumstances, so that DLDP can respond rapidly to link failure. The time interval should be shorter than one-third of the STP convergence time, which is generally 30 seconds. If too long time interval is set, an STP loop may occur

before DLDP shut down unidirectional links. On the contrary, if too short time interval is set, network traffic increases, and port bandwidth is reduced.

- DLDP does not process any LACP event, and treats each link in the aggregation group as independent.

For the configuration of distributed products, note that:

- During hot plugging, if the interface board you insert has the same type as that you have removed, DLDP restores working automatically.
- After the SRPU board switchover, the standby board takes over unidirectional link detection. In this case, the DLDP parameters do not change and DLDP checks every port again for unidirectional links.

For the configuration of the products supporting intelligent resilient framework (IRF), note that:

- DLDP supports IRF; its processing is fully distributed. In IRF, port management is distributed to each port. Each unit completes only the DLDP tasks for its ports. DLDP commands executed on a port take effect only on the unit where the port is located.
- The global DLDP configuration must be consistent on all units. The global DLDP configuration commands take effect on all the units in the IRF.
- Stack ports do not support DLDP.

1.2 DLDP Configuration

1.2.1 Configuring DLDP

The following table describes the DLDP basic configuration tasks:

Table 1-7 DLDP configuration tasks

<table>
<tr><th colspan="3">Operation</th><th>Command</th><th>Description</th></tr>
<tr><td colspan="3">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td rowspan="3">Enable DLDP</td><td colspan="2">Enable DLDP globally</td><td>dldp enable</td><td rowspan="3">Required, by default, DLDP is disabled</td></tr>
<tr><td rowspan="2">Enable DLDP on a port</td><td>Enter Ethernet port view</td><td>interface { interface-type interface-number</td></tr>
<tr><td>Enable DLDP on a port</td><td>dldp enable</td></tr>
<tr><td colspan="3">Set the authentication mode and password</td><td>dldp authentication-mode { none | simple password | md5 password }</td><td>Optional, by default, the authentication mode is none</td></tr>
</table>

Operation	Command	Description
Set the time interval for sending DLDP packets	**dldp interval** *integer*	Optional, by default, the time interval is 10 seconds.
Set the DLDP handling mode when an unidirectional link is detected	**dldp unidirectional-shutdown** { **auto** | **manual** }	Optional, by default, the handling mode is auto.
Set the DLDP operating mode	**dldp work-mode** { **enhance** | **normal** }	Optional; by default, DLDP works in normal mode.
Display the configuration information about the ports on which DLDP is enabled	**display dldp** { *unit-id* | *interface-type interface-number* }	You can execute this command in any view.

Note:

- When you use the **dldp enable/dldp disable** command in system view to enable/disable DLDP globally on all optical ports of the switch, this command is only valid for existing optical ports on the device, it is not valid for those added subsequently.
- DLDP can operate normally only when the same authentication mode and password are set for local and peer ports.

1.2.2 Resetting DLDP Status

Note:

The command here is only valid for those ports that are DLDP down due to the detection of unidirectional link. You can use the command here to reset the DLDP status of these ports to retrieve DLDP probes.

Table 1-8 Reset DLDP status

Operation			Command	Description
Reset DLDP status	Enter system view		**system-view**	Optional
	Reset the DLDP status of the system		**dldp reset**	
	Reset the DLDP status of a port	Enter Ethernet port view	**interface** *interface-type interface-number*	
		Reset the DLDP status of a port	**dldp reset**	

Caution:

This command only applies to the ports in DLDP down status.

1.3 DLDP Configuration Example

I. Network requirements

As shown in Figure 1-3 and Figure 1-4, two switches (SwitchA and SwitchB) are connected with each other by fibers.

- The two switches are connected by two pairs of fibers.
- The cross lines in Figure 1-3 indicates the two fibers are incorrectly cross-connected, and the vacant lines in Figure 1-4 indicates the two fibers may be either correctly connected or disconnected.
- Both switches support DLDP.
- Unidirectional links due to incorrect fiber connections between the two switches (including disconnection in one direction and cross-connection) are expected to be detected and then automatically shut down by DLDP.
- Suppose a cross-connection exists between SwitchA and SwitchB, which is then corrected by a network administrator after DLDP shuts down the unidirectional links. Now the ports taken down by DLDP need to be restored.

II. Network diagram

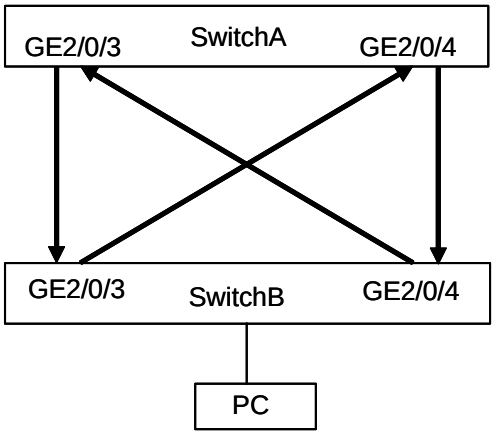

Figure 1-3 Fiber cross-connection

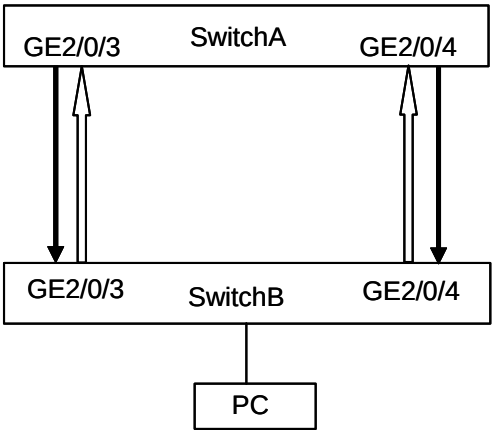

Figure 1-4 correct connection/disconnection in one direction

III. Configuration procedure

1) Configure SwitchA

Configure the ports to work in mandatory full duplex mode

```
<QuidwayA> system-view
[QuidwayA] interface gigabitethernet 2/0/3
[QuidwayA-GigabitEthernet2/0/3] duplex full
[QuidwayA-GigabitEthernet2/0/3] speed 1000
[QuidwayA-GigabitEthernet2/0/3] quit
[QuidwayA] interface gigabitethernet 2/0/4
[QuidwayA-GigabitEthernet2/0/4] duplex full
[QuidwayA-GigabitEthernet2/0/4] speed 1000
[QuidwayA-GigabitEthernet2/0/4] quit
```

Enable DLDP globally

```
[QuidwayA] dldp enable
```

Set the time interval for sending DLDP packets to 15 seconds

```
[QuidwayA] dldp interval 15
```

Configure DLDP to work in enhanced mode

```
[QuidwayA] dldp work-mode enhance
```

Set the DLDP handling mode for unidirectional links to auto

```
[QuidwayA] dldp unidirectional-shutdown auto
```

Display the DLDP status on Switch A

```
[QuidwayA] display dldp 2
```

If the fibers are correctly connected between the two switches, the system displays the connections with the neighbor as bidirectional links, or else, it displays the connections with the neighbor as unidirectional links.

Restore the ports taken down by DLDP

```
[QuidwayA] dldp reset
```

2) Configure Switch B

Configure the ports to work in mandatory full duplex mode

```
<QuidwayB> system-view
[QuidwayB] interface gigabitethernet 2/0/3
[QuidwayB-GigabitEthernet2/0/3] duplex full
[QuidwayB-GigabitEthernet2/0/3] speed 1000
[QuidwayB-GigabitEthernet2/0/3] quit
[QuidwayB] interface gigabitethernet 2/0/4
[QuidwayB-GigabitEthernet2/0/4] duplex full
[QuidwayB-GigabitEthernet2/0/4] speed 1000
[QuidwayB-GigabitEthernet2/0/4] quit
```

Enable DLDP globally

```
[QuidwayB] dldp enable
```

Set the time interval for sending DLDP packets to 15 seconds

```
[QuidwayB] dldp interval 15
```

Configure DLDP to work in enhanced mode

```
[QuidwayB] dldp work-mode enhance
[QuidwayB] dldp work-mode enhance
```

Set the DLDP handling mode for unidirectional links to auto

```
[QuidwayB] dldp unidirectional-shutdown auto
```

Display the DLDP status on SwitchB

```
[QuidwayB] display dldp 2
```

If the fibers are correctly connected between the two switches, the system displays the connections with the neighbor as bidirectional links, or else, it displays the connections with the neighbor as unidirectional links.

Restore the ports taken down by DLDP

```
[QuidwayB] dldp reset
```

Note:

- For DLDP to detect fiber disconnection in one direction, you must configure the port to work in mandatory full duplex mode.
- When a port works in mandatory full duplex mode and DLDP is enabled, DLDP considers a link as in unidirectional status if fiber in one direction is disconnected.
- When a port works in non-mandatory full duplex mode, even if DLDP is enabled, it does not take effect when fiber in one direction is disconnected, in that case, it considers that the port is down.

Chapter 2 DLDP Configuration Commands

2.1 DLDP Configuration Commands

2.1.1 debugging dldp

Syntax

debugging dldp { **error** | **neighor** | **packet** | **state** | **all** }

undo debugging dldp { **error** | **neighor** | **packet** | **state** | **all** }

View

User view

Parameter

error: Debugging for DLDP error.

neighbor: Debugging for DLDP neighbor.

packet: Debugging for DLDP packets.

state: Debugging for the DLDP status on ports

all: All DLDP debuggings.

Description

Use the **debugging dldp** command to enable specific debugging for DLDP on all ports with DLDP enabled.

Use the **undo debugging dldp** command to disable debugging for DLDP on all ports with DLDP enabled.

By default, DLDP debugging is disabled.

Related command: **display dldp**.

Example

Enable debugging for DLDP error.

```
<Qudiway> debugging dldp error
```

2.1.2 display dldp

Syntax

display dldp { *unit-id* | *interface-type interface-number* }

View

Any view

Parameter

unit-id: Unit number in intelligent resilient framework (IRF) system.

interface-type: Port type.

interface-number: Port number.

Description

Use the **display dldp** command to specify the configuration, status, and neighbor table information about one specific or all the ports in the specified unit with DLDP enabled.

The configuration information includes the following:

- The configuration information includes the time interval, authentication mode, password, DLDP operating mode, and handling mode when an unidirectional link is found.
- The status information includes the neighbor status, local port status and link status
- The neighbor table includes the MAC address, port ID, neighbor status and aging time items.

Example

Display information about all the ports with DLDP enabled on Unit 1.

```
<Quidway> display dldp 1
dldp interval 10
 dldp work-mode enhance
 dldp authentication-mode none
 dldp unidirectional-shutdown manual

 The port number of unit 1 with DLDP is 2.

 interface GigabitEthernet2/0/1
     dldp port state : inactive
     dldp link state : down
     The neighbor number of the port is 0.
 interface GigabitEthernet2/0/2
     dldp port state : advertisement
     dldp link state : up
     The neighbor number of the port is 1.
         neighbor mac address : 00e0-fc27-750d
         neighbor port index : 98
         neighbor state : two way
```

```
neighbor aged time : 24
```

2.1.3 dldp

Syntax

dldp { **enable** | **disable** }

View

System view, Ethernet port view

Parameter

None

Description

In system view:

Use the **dldp enable** command to enable DLDP globally on all optical ports of the switch.

Use the **dldp disable** command to disable DLDP globally on all optical ports of the switch.

In Ethernet port view:

Use the **dldp enable** command to enable DLDP on the current port.

Use the **dldp disable** command to disable DLDP on the current port.

The commands can apply to a non-optical port as well as an optical port.

By default, DLDP is disabled.

Note that:

- When you use the **dldp enable/dldp disable** command in system view to enable/disable DLDP globally on all optical ports of the switch, this command is only valid for the existing optical ports on the device, it is not valid for those added subsequently.

Example

Enable DLDP globally on all optical ports of the switch.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dldp enable
All fiber ports except fabric ports have enabled DLDP!
```

2.1.4 dldp authentication-mode

Syntax

dldp authentication-mode { **none** | **simple** *password* | **md5** *password* }

undo dldp authentication-mode

View

System view

Parameter

md5: Sets the authentication mode to MD5.

none: Performs no authentication.

simple: Sets the authentication mode to plain text.

password: Authentication password, which is a string in plain text consisting of 1 to 16 characters.

Description

Use the **dldp authentication-mode** command to set the DLDP authentication mode and password for the ports of the local and peer devices.

By default, authentication mode is **none**.

Note that:

When you configure the DLDP authentication mode and authentication password, make sure the same DLDP authentication mode and password are set for the ports of the local and peer devices, which are connected with the optical fiber cable or copper twisted pair. Otherwise, DLDP authentication fails. DLDP cannot work when DLDP authentication fails.

Related command: **dldp unidirectional-shutdown**.

Example

Set the DLDP authentication mode and password for the ports connected with fiber cables or copper twisted pairs, between the two devices (QuidwayA and QuidwayB) to plain text and password1 respectively.

- Configure QuidwayA:

```
<QuidwayA> system-view
System View: return to User View with Ctrl+Z.
[QuidwayA] dldp authentication-mode simple password1
```

- Configure QuidwayB:

```
<QuidwayB> system-view
System View: return to User View with Ctrl+Z.
[QuidwayB] dldp authentication-mode simple password1
```

2.1.5 dldp interval

Syntax

dldp interval *integer*

undo dldp interval

View

System view

Parameter

Integer: Time interval for sending DLDP frames, in the range of 5 seconds to 100 seconds.

Description

Use the **dldp interval** command to set the time interval for sending advertisement packets. For any port where DLDP is enabled, when DLDP is in advertisement state, it sends advertisement packets through the port at the intervals of this value..

Use the **undo dldp interval** command to restore the default time interval.

By default, the time interval for sending advertisement packets is 10 seconds.

Note that:

- The time interval you define applies to all ports with DLDP enabled.
- The time interval should be shorter than one-third of the STP convergence time, which is generally 30 seconds. If too long time interval is set, an STP loop may occur before DLDP shut down unidirectional links. On the contrary, if too short time interval is set, network traffic increases, and port bandwidth is reduced.

Example

Set the time interval for sending advertisement packets to 20 seconds.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dldp interval 20
```

2.1.6 dldp reset

Syntax

dldp reset

View

System view, Ethernet port view

Parameter

None

Description

In system view:

Use the **dldp reset** command to reset the DLDP status of all the ports disabled by DLDP.

In Ethernet port view:

Use the **dldp reset** command to reset the DLDP status of current port disabled by DLDP.

After the **dldp reset** command is executed, the DLDP status of these ports changes from disable to active and DLDP restarts to probe the link status of the fiber cables or copper twisted pairs.

Related command: **dldp**, **dldp unidirectional-shutdown**.

Example

Reset the DLDP status of all the ports disabled by DLDP.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dldp reset
```

2.1.7 dldp unidirectional-shutdown

Syntax

dldp unidirectional-shutdown { **auto** | **manual** }

undo dldp unidirectional-shutdown

View

System view

Parameter

auto: In this mode, when DLDP finds an unidirectional link or finds (in the enhanced mode) that the peer end is down , it automatically disables the corresponding port.

manual: In this mode, when DLDP finds an unidirectional link or finds (in the enhanced mode) that the peer end is down, instead of disabling the port automatically, it stops the DLDP packets sending/receiving on the port and prompts the user to disable the port manually.

Description

Use the **dldp unidirectional-shutdown** command to set DLDP handling mode when an unidirectional link is found.

Use the **dldp unidirectional-shutdown** command to restore the default setting.

By default, the handling mode when finding unidirectional link is auto.

Related command: **dldp work-mode**.

Example

Configure DLDP to automatically disable the corresponding port when an unidirectional link is found.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dldp unidirectional-shutdown auto
```

2.1.8 dldp work-mode

Syntax

dldp work-mode { **enhance** | **normal** }

undo dldp work-mode

View

System view

Parameter

enhance: Configure DLDP to work in enhanced mode. In this mode, DLDP probes actively whether neighbors exist when neighbor entries age out.

normal: Configure DLDP to work in normal mode. In this mode, DLDP does not probe actively whether neighbors exist when neighbor entries age out.

Description

Use the **dldp work-mode** command to set the DLDP operating mode.

Use the **undo dldp work-mode** command to restore the default DLDP operating mode.

By default, DLDP works in normal mode.

Example

Configure DLDP to work in enhanced mode.

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dldp work-mode enhance
```