Contents

1 Configuring DLDP

The Data Link Detection Protocol (DLDP) achieves rapid detection of Ethernet link failures. A typical Ethernet link detection mechanism detects physical link connectivity through auto-negotiation at the physical layer. However, such a mechanism has limitations in L3 data connectivity detection, for example, the physical connection is normal but L3 data communication is abnormal. DLDP provides reliable L3 link detection information. After detecting a faulty link, DLDP disables the logical function of L3 ports to realize fast L3 protocol convergence.

1.1 Introduction

1.1.1 Basic Concepts

1. Detection Mode

Active mode and passive mode are two DLDP detection modes.

- Active mode (default): In this mode, Internet Control Message Protocol (ICMP) detection packets are sent actively.
- Passive mode: In this mode, ICMP detection packets are received passively. Namely, DLDP returns an ICMP reply packet upon receiving an ICMP echo packet, instead of actively sending ICMP echo packets to the peer end. It judges whether an ICMP echo packet is received within a specified period to determine whether the link to the peer port is faulty. This mode not only implements the function of detecting link connectivity for the both devices, but also saves the bandwidth resources and device CPU resources.

2. Inter-Network Segment Detection

If DLDP needs to detect reachability to an IP address in a non-directly connected network segment, you need to configure the next-hop IP address for the local port so that DLDP can obtain the next-hop MAC address through an Address Resolution Protocol (ARP) packet, encapsulate an ICMP packet correctly, and send it out. In this situation, however, you need to avoid receiving an ICMP reply packet from another link; otherwise, DLDP misjudges that the port does not receive an ICMP reply.

3. Detection Time

When a network device does not receive a reply packet from the peer end within the period of the detection interval multiplied by the number of retransmission times, the device determines that an L link failure occurs and actively shuts down the logical function of its L3 port (despite the physical link reachable). Once the L3 link connectivity recovers, the device restores the logical function of the L3 port.

- Detection interval: Indicates the interval at which DLDP detection packets (ICMP echo) are transmitted.
- Retransmission times: Indicates the maximum number of times that DLDP detection packets can be retransmitted after a DLDP detection failure occurs.

4. Recovery Times

A detected link may be unstable, for example, the link can be pinged through only intermittently. The results of single DLDP detection are that the link is up/ down multiple times, which further destabilizes the ring network.

The term recovery times indicates the number of times that DLDP needs to receive reply packets consecutively before a link switches from the down state to up state. The default number of recovery times is 3, that is, a link can be pinged successfully three times before it is set to up. The recovery times configuration reduces link detection sensitivity but increases stability. Related parameters can be adjusted according to the network condition.

1.1.2 DLDP Detection

When detecting that an L3 link is abnormal, DLDP actively shuts down the L3 port. After the DLDP function is enabled, DLDP sends an ARP packet to obtain the MAC address and outbound port of the detected device or the next-hop device reachable to the detected device. Then DLDP periodically sends IPv4 ICMP echo packets to the MAC address and outbound port to detect link connectivity. If DLDP does not receive an IPv4 ICMP reply packet from the detected device within a specified period, DLDP determines that the link is abnormal and sets the L3 port to down. You can configure the next-hop IP address, MAC address of the detected device, transmission interval, number of retransmission times, and number of recovery times based on the actual environment to enable the DLDP detection function.

1.1.3 MAC Address Binding

In a complex network environment, DLDP may obtain an invalid MAC address if abnormal ARP packets are transmitted (due to ARP spoofing) in the detected link. As a result, DLDP fails to conduct detection normally. To address this problem, you can bind the to-be-detected IP address (or the next-hop IP address) to the MAC address of the device to avoid a DLDP failure caused by ARP spoofing. After binding, DLDP sends ARP packets and ICMP packets with a fixed destination IP address and a fixed destination MAC address during detection. If the source IP address and MAC address in a received packet do not match the bound IP address and MAC address, DLDP does not process the packet.

1.2 Configuring DLDP Detection

1.2.1 Overview

DLDP detects L3 link connectivity. When an L3 link is abnormal, DLDP shuts down the related L3 port.

1.2.2 Restrictions and Guidelines

- To configure the DLDP function, configure the next-hop IP address, MAC address, transmission interval, retransmission times, and recovery times based on the actual environment. You are not advised to set the number of retransmission times and the number of recovery times to 1. You are advised to use the default value for the transmission interval. The number of DLDP sessions and the configured CPU protect policy (CPP) bandwidth must be considered when you adjust the value. Otherwise, the device performance consumption increases and misjudgment and flapping can be caused easily. In the case of more than 10 sessions, the recommended interval is not smaller than 100 ticks.
- DLDP can detect multiple IP addresses configured on an L3 port. DLDP sets the port to down when none of the IP addresses returns an ICMP reply. If one of the IP addresses resumes communication, DLDP sets the

port to up.

- DLDP uses the first IP address of the L3 port as the source IP address of detection packets.

1.2.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable DLDP detection.

dldp *ipv4-address* [*next-hop-ipv4-address*] [**mac-address** *mac-address*] [**interval** *tick-interval* | **resume** *resume-number* | **retry** *retry-number*]

By default, the number of retransmission times of DLDP detection is **4**, the number of recovery times is **3**, and the detection interval is **1** second.

(5) (Optional) Configure a DLDP detection mode.

dldp passive

The default DLDP detection mode is active mode.

(6) (Optional) Configure a global detection interval for DLDP detection.

dldp interval *tick-interval*

The default global detection interval of DLDP detection is **1** second.

The configuration of this command takes effect immediately for all DLDP detection operations.

(7) (Optional) Configure the number of global retransmission times for DLDP detection.

dldp retry *retry-number*

The default number of global retransmission times of DLDP detection is **4**.

The configuration of this command takes effect immediately for all DLDP detection operations.

(8) (Optional) Configure the number of link recovery times for all DLDP detection operations.

dldp resume *resume-number*

The default number of link recovery times of all DLDP detection operations is **3**.

The configuration of this command takes effect immediately for all DLDP detection operations.

1.3 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

⚠ **Caution**

Running the **clear** command during operation of the device may lose vital information and interrupt services.

Table 1-1 DLDP Monitoring

Command	Purpose
clear dldp [**interface** *interface-type* *interface-number* [*ipv4-address*]]	Clears the statistics on link up/down counts of a DLDP monitoring point.
show dldp [**interface** *interface-type* *interface-number*]	Displays the configuration of a DLDP monitoring point.
show dldp [**interface** *interface-type* *interface-number*] [**statistic**]	Displays the statistics of a DLDP monitoring point.

1.4 Configuration Examples

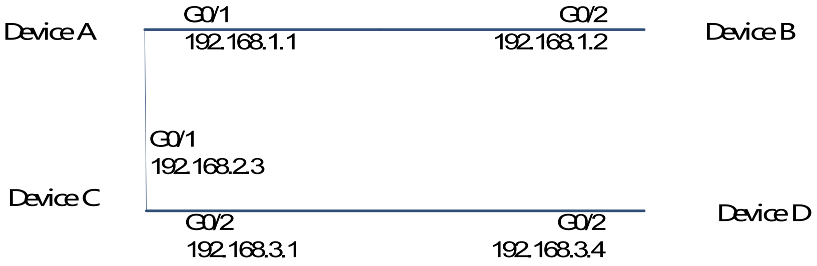
1.4.1 Configuring DLDP Detection

1. Requirements

DLDP detection needs to be enabled on an L3 network to control the L3 ports of devices A and B.

2. Topology

Figure 1-1 DLDP Topology



3. Notes

- Enable DLDP detection on the routed ports (GigabitEthernet 0/1 and GigabitEthernet 0/2) on device A to detect the L3 network connectivity from device A to device B and from device A to device D.
- To control the routed port (GigabitEthernet 0/2) of device B, enable DLDP detection and configure passive mode on the port.

4. Procedure

Perform the following configuration on device A.

```
Device A> enable
Device A# configure terminal
Device A(config)# interface gigabitethernet 0/1
Device A(config-if-GigabitEthernet 0/1)# dldp 192.168.1.2
Device A(config-if-GigabitEthernet 0/1)# exit
Device A(config)# interface gigabitethernet 0/2
Device A(config-if-GigabitEthernet 0/2)# dldp 192.168.3.4 192.168.2.3
```

Perform the following configuration on device B.

```
Device B> enable
Device B# configure terminal
Device B(config)# interface gigabitethernet 0/2
Device B(config-if-GigabitEthernet 0/2)# dldp 192.168.1.1
Device B(config-if-GigabitEthernet 0/2)# dldp passive
```

5. Verification

Run the **show dldp** command to check the DLDP state information on devices A and B and check whether DLDP detection is enabled and works normally.

```
Device A# show dldp
Interface  Type         Ip         Next-hop    Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------  ------
Gi0/1      Active   192.168.1.2               100       4      3       Up
Gi0/1      Active   192.168.3.4  192.168.2.3  100       4      3       Up
```

```
Device B# show dldp
Interface  Type         Ip         Next-hop    Interval  Retry  Resume  State
---------  -------  -----------  -----------  --------  -----  ------  ------
Gi0/2      Passive  192.168.1.1               100       4      3       Up
```

6. Common Errors

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