UniDirectional Link Detection (UDLD) Protocol

The UniDirectional Link Detection protocol is a Layer 2 protocol that detects and disables one-way connections before they create undesired situation such as Spanning Tree loops.

Information About the UDLD Protocol

UDLD Overview

The Cisco-proprietary UDLD protocol allows the devices connected through fiber optic or copper (for example, Category 5 cabling) Ethernet cables that are connected to the LAN ports to monitor the physical configuration of the cables and detect whether a unidirectional link exists. When a unidirectional link is detected, the UDLD shuts down the affected LAN port and alerts the corresponding user, because unidirectional links cause a variety of problems, including spanning tree topology loops.

UDLD is a Layer 2 protocol that works with the Layer 1 protocols to determine the physical status of a link. In Layer 1, auto negotiation takes care of physical signaling and fault detection. UDLD performs tasks that auto negotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected LAN ports. When you enable both auto negotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever the traffic transmitted by a local device over a link is received by a neighbor, but traffic transmitted from the neighbor is not received by the local device. If one of the fiber strands in a pair is disconnected, the link does not stay up as long as the auto negotiation is active. In such a scenario, the logical link is undetermined, and the UDLD does not take any action. If both the fibers are working normally in Layer 1, the UDLD in Layer 2 determines whether those fibers are connected correctly and whether the traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by auto negotiation because auto negotiation operates in Layer 1.

The router periodically transmits the UDLD packets to the neighbor devices on LAN ports where UDLD is enabled. If the packets are echoed back within a specific timeframe and they are lacking a specific acknowledgment (echo), the link is flagged as unidirectional and the LAN port is shut down. Devices on both ends of the link must support UDLD for the protocol to successfully identify and disable the unidirectional links.

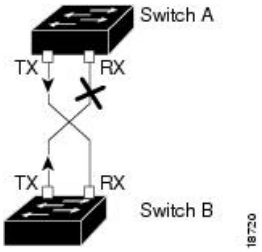
UDLD detects and disables unidirectional links on Ethernet fiber and copper interfaces due to miswiring or malfunctioning of the interfaces.

Note UDLD is disabled by default on all ports to avoid sending unnecessary traffic.

To configure fibre-optic interfaces, enable the **udld** command at the global level. For copper interfaces, enable the **udld port** command at the interface level.

The figure displays the UDLD mechanism.

Figure 1: Unidirectional Link



UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected interfaces on fiber-optic links.

UDLD Normal Mode

In normal mode, UDLD detects the unidirectional link when fiber strands in a fiber-optic interface are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the interfaces are connected correctly, but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In case, the logical link is considered undetermined, and UDLD does not disable the interface. If one of the fiber strands in a pair is disconnected and autonegotiation is active, the link does not stay up because the Layer 1 mechanisms did not detect a physical problem with the link. In this case, UDLD does not take any action, and the logical link is considered undetermined.

UDLD Aggressive Mode

The UDLD aggressive mode is configured only on the point-to-point link between the network devices that support the UDLD aggressive mode. With UDLD aggressive mode enabled, a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving the UDLD packets. The UDLD tries to re-establish the connection with the neighbor; the port is disabled after eight failed retries.

To prevent spanning tree loops, nonaggressive UDLD with the default interval of 15 seconds is fast enough to shut down a unidirectional link before a blocking port transitions to the forwarding state (with default spanning tree parameters).

When the UDLD aggressive mode is enabled, the UDLD can error disable the ports on the link to prevent the traffic from being discarded under the following scenarios:

- One side of a link has a port (either Tx and Rx) stuck.

- One side of a link remains up while the other side of the link has gone down.

UDLD Functions

UDLD performs the following functions

- Sends a probe packet on every active interface on which UDLD is configured to keep each device informed about its neighbors.
- Learns about the neighbors and keeps the updated neighbor information in a cache table
- Sends several echo messages whenever it detects a new neighbor sending UDLD packets or whenever a neighbor requests a resynchronization of the caches
- Shuts down the affected port and notifies the user when one-way connection is detected. Devices on both ends of the link must support UDLD in order for the protocol to successfully identify and disable unidirectional links
- Reestablishes the connection with the neighbor when a port on a bidirectional link stops receiving UDLD packets if aggressive mode is enabled. After eight failed retries, the port goes into disabled state

Detecting Unidirectional Links

UDLD operates by using two mechanisms:

Neighbor database maintenance

UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active interface to keep each device informed about its neighbors. When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one. Whenever an interface is disabled and UDLD is running, whenever UDLD is disabled on an interface, or whenever the switch is reset, UDLD clears all existing cache entries for the interfaces affected by the configuration change. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.

Event-driven detection and echoing

UDLD relies on echoing as its detection mechanism. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply. If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the interface is shut down. If UDLD in normal mode is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors. If you enable aggressive mode when all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the port if, after the fast train of messages, the link state is still undetermined.

How to Configure UDLD Protocol

Enabling UDLD Protocol

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **udld** {**enable** | **aggressive**}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**udld** {**enable**	**aggressive**} **Example:** `Router(config)# udld enable`	Enables UDLD protocol on the router.
Step 4	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Enabling UDLD Protocol at Interface Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **udld port** [**aggressive**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet0/0/1`	Enter interface configuration mode. Valid interfaces are physical ports.
Step 4	**udld port** [**aggressive**] **Example:** `Router(config)# udld port aggressive`	Enables UDLD on a specific port. Enter the aggressive keyword to enable the aggressive mode. On a fiber-optic LAN port, this command overrides the udld enable global configuration command setting. Use the **no** form of this command to disable the UDLD on a non fiber-optic LAN port.
Step 5	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Enabling UDLD Probe Message Interval

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **udld message time** *interval*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**udld message time** *interval* **Example:** `Router(config)# udld message time 90`	Set the time in seconds between UDLD probe messages. The valid range is from 7 to 90 seconds. The default is 15 seconds
Step 4	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Recovering the UDLD Protocol

UDLD recovery when enabled, attempts to bring an UDLD error-disabled port out of reset. Tthe default recovery timer is 300 seconds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **udld recovery** *inteval*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**udld recovery** *inteval* **Example:** `Router(config)# udld recovery`	Enables UDLD recovery on the router. • *inteval*—Sets the recovery time interval. The valid range is from 30 to 86400 seconds. The default value is 300 seconds.
Step 4	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Resetting Ports

SUMMARY STEPS

1. enable
2. udld reset
3. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**udld reset** **Example:** `Router(config)# udld reset`	Resets ports that are shut down by UDLD.
Step 3	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Configuration Examples

Example: Configuring UDLD Protocol

This example shows UDLD on the router.

```
show running-config | i udld
udld enable
udld message time 7
udld recovery
udld recovery interval 30
```

Verifying UDLD Protocol

Example: Verifying UDLD Protocol

Use the **show udld** command to view the status of the UDLD protocol on the ports.

- This example shows UDLD protocol on all ports the router.

```
Router# show udld
 Interface Te0/0/0
---
```

```
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 40
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOX1736P0JP
    Port ID: Te0/1/0
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Te0/0/0

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1B

Interface Gi0/2/0
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 33
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOC1528V27K
    Port ID: Gi0/2
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Gi0/2/0

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1A

Interface Gi0/2/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 33
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOC1639V1Z4
    Port ID: Gi0/4
    Neighbor echo 1 device: FOX1709P3D0
    Neighbor echo 1 port: Gi0/2/1

    Message interval: 15
```

```
    Time out interval: 5
    CDP Device name: RSP1A

Interface Gi0/2/2
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Advertisement
Message interval: 15
Time out interval: 5
No neighbor cache information stored

Interface Gi0/2/3
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Link down
Message interval: 15
Time out interval: 5
No neighbor cache information stored

Interface Gi0/2/4
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Gi0/2/5
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface Gi0/2/6
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown
.
.
.
```

- This example shows UDLD protocol on the Ten Gigabit Ethernet interface.

```
Router# show udld interface tengigabitethernet 0/0/0

Interface Te0/0/0
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 15
Time out interval: 5

    Entry 1
    ---
    Expiration time: 43
    Cache Device index: 1
    Current neighbor state: Bidirectional
    Device ID: FOX1736P0JP
    Port ID: Te0/1/0
    Neighbor echo 1 device: FOX1709P3D0
```

```
    Neighbor echo 1 port: Te0/0/0

    Message interval: 15
    Time out interval: 5
    CDP Device name: RSP1B

Router# show running-config | i udld
udld enable
udld message time 15
udld recovery
udld recovery interval 30
```

- This example shows the UDLD protocol neighbors.

```
Router# show udld neighbors

Port          Device Name     Device ID     Port ID        Neighbor State
------------ ------------- ------------ ------------ ----------------
Te0/0/0         FOX1736P0JP     1            Te0/1/0         Bidirectional
Gi0/2/0         FOC1528V27K     1            Gi0/2           Bidirectional
Gi0/2/1         FOC1639V1Z4     1            Gi0/4           Bidirectional
```