Configure UDLD

Feature History for UDLD

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 17.18.1	UniDirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Overview of UniDirectional Link Detection

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that:

- Enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables,
- Detects when a unidirectional link exists, and
- Alerts and disables the affected port upon detection.

UDLD prevents issues such as spanning-tree topology loops by identifying unidirectional links. Devices in the network must support UDLD to function effectively.

Restrictions for Configuring UniDirectional Link Detection

The following restrictions apply to configuring UniDirectional Link Detection (UDLD):

- A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port on another device.
- When configuring the UDLD mode (normal or aggressive), ensure that the same mode is configured on both sides of the link.
- Fast UDLD can only be enabled on up to 32 ports initially. If this limit is reached, Fast UDLD will not be enabled on additional ports, and an error message will be displayed on the console.

UDLD: hundredGigE<> not enabled for fast hello, maximum number of fast hello ports (32) reached.

- If UDLD is disabled when Fast UDLD is configured, the entire UDLD configuration is removed.
- The "Alert" option for UDLD ports is supported.
- During manual reloads, switches with UDLD aggressive mode enabled (and lower-value timers) may enter an error-disabled state. This is because the system requires time to gracefully restart while CPU resources prioritize higher-priority processes.

Mitigation: To prevent this, either increase the hello interval value or shut down all active interfaces before reloading.

Fast UniDirectional Link Detection Capabilities

Fast UDLD capability is a feature of network devices that:

- Supports timers in the few-hundred milliseconds range,
- Enables subsecond unidirectional link detection, and
- Facilitates transition between different modes based on configuration.

Fast UniDirectional Link Detection (Fast UDLD) allows detection of unidirectional links in less than a second, with links status messages exchanged every 200 milliseconds. A link’s transition from slow mode to fast mode occurs when both sides of a link have Fast UDLD configured and negotiated successfully to move into fast mode. Conversely, a transition from fast mode to slow mode happens when one of the configured ports has its Fast UDLD configuration removed. Fast UDLD supports a wide range of devices.

Modes of operation for UDLD

UDLD and Fast UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports 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 ports on fiber-optic links.

In normal and aggressive modes, UDLD works with the Layer 1 mechanisms to learn the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both autonegotiation 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 traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

Normal mode of operation for UDLD

A UDLD normal mode is an operational mode of the Unidirectional Link Detection (UDLD) protocol that:

- Detects unidirectional links caused by fiber misconnection when Layer 1 mechanisms fail,
- Leaves the logical link undetermined if traffic is unidirectional but Layer 1 mechanisms do not detect this condition, and
- Does not take action when autonegotiation detects a physical link issue caused by disconnection of one or more fiber strands.

Aggressive mode of operation for UDLD

UDLD aggressive mode is a protocol mode for Unidirectional Link Detection (UDLD) that:

- Detects unidirectional links using previously defined methods,
- Shuts down affected ports when a unidirectional link is detected, and
- Ensures bidirectional traffic flow on point-to-point links.

In aggressive mode, UDLD not only monitors the health of point-to-point links but also actively disables ports when unidirectional traffic patterns are detected. It is particularly effective in scenarios where device failures occur, such as:

- A port is unable to send or receive traffic,
- One port is down while the other remains up, or
- A fiber strand is disconnected within the cable.

UDLD differs from Layer 1 autonegotiation by operating at a higher layer, ensuring that traffic flows bidirectionally between the correct neighbors.

Example:

- On fiber-optic or twisted-pair links, one of the ports cannot send or receive traffic.
- One of the fiber strands in the cable is disconnected.

In a point-to-point link, UDLD hello packets can be considered as a "heart beat," ensuring the health of the link. A loss of the "heart beat" indicates a failure that requires the link to be disabled unless a bidirectional connection can be reestablished.

Unidirectional Link Detection Methods

UDLD operates by using two methods:

- Neighbor database maintenance
- Event-driven detection and echoing

How UDLD maintains neighbor databases

The process of UDLD neighbor database maintenance ensures that each device stays updated about its neighbors, maintains synchronized caches, and handles exceptional cases like errors or configuration changes.

The key components involved in the process are:

- UDLD-capable neighbors: Devices that exchange UDLD hello packets for neighbor discovery and synchronization.
- Hello packets: Periodic packets sent to exchange device information and keep caches updated.
- Cache entries: Stored information about neighbors with an expiration mechanism (age time).
- Configuration changes: Events such as port status changes, UDLD enable/disable actions, or device resets that trigger cache clearing.

The process involves the following stages:

1. Hello packet exchange and neighbor discovery
    - UDLD periodically sends hello packets (advertisements or probes) on active ports.
    - Devices receiving these packets cache the neighbor's details until the age time (hold time or time-to-live) expires.
2. Cache updates
    - If a new hello packet is received before an older cache entry ages, the device replaces the old entry with the new one.
3. Cache clearing during configuration changes
    - When a port is disabled, UDLD is disabled on a port, or the device is reset, all cache entries for affected ports are cleared.
    - UDLD sends a message to neighbors to inform them of the change, prompting the synchronization of their caches.
4. Handling multiple UDLD neighbors per interface
    - Interfaces do not support multiple UDLD neighbors.
    - If a UDLD PDU (protocol data unit) with multiple device IDs in the echo TLV (type, length, value) is received, the interface enters an error-disabled state to prevent ambiguity.

The process ensures accurate and synchronized neighbor database maintenance. However, interfaces receiving multiple device IDs will be placed in an error-disabled state to avoid misconfiguration.

Event-driven detection and echoing

UDLD relies on echoing as its detection operation. 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 are 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 port is disabled.

UDLD reset options

If an interface becomes disabled by UDLD, you can use one of the following options to reset UDLD:

- The **udld reset** interface command.
- The **shutdown** interface configuration command followed by the **no shutdown** interface configuration command restarts the disabled port.
- The **no udld** { **aggressive** | **enable**} global configuration command followed by the **udld** { **aggressive** | **enable**} global configuration command reenables the disabled ports.
- The **no udld port** interface configuration command followed by the **udld port** [**aggressive**] interface configuration command reenables the disabled fiber-optic port.
- The **errdisable recovery cause udld** global configuration command enables the timer to automatically recover from the UDLD error-disabled state, and the **errdisable recovery interval** *interval* global configuration command specifies the time to recover from the UDLD error-disabled state.

The **udld port disable** command disables UDLD on fiber-optic LAN ports.

Note:

This command is only supported on fiber-optic LAN ports.

Default UDLD configuration

Default UniDirectional Link Detection (UDLD) configuration governs network communication integrity by detecting unidirectional links.

The default settings for UDLD configuration are as follows:

Feature	Default Setting
UDLD global enable state	Globally disabled
UDLD per-port enable state for fiber-optic media	Disabled on all Ethernet fiber-optic ports
UDLD per-port enable state for twisted-pair (copper) media	Disabled on all Ethernet 10/100 and 1000BASE-TX ports
UDLD aggressive mode	Disabled
Fast UDLD per-port enable state	Disabled on all ports

This set of configurations ensures that UDLD operates under default settings until explicitly enabled or modified to suit specific network environments.

Configure UniDirectional Link Detection

The following sections provide information about configuring UDLD:

Default UDLD configuration

Default UniDirectional Link Detection (UDLD) configuration governs network communication integrity by detecting unidirectional links.

The default settings for UDLD configuration are as follows:

Feature	Default Setting
UDLD global enable state	Globally disabled
UDLD per-port enable state for fiber-optic media	Disabled on all Ethernet fiber-optic ports
UDLD per-port enable state for twisted-pair (copper) media	Disabled on all Ethernet 10/100 and 1000BASE-TX ports
UDLD aggressive mode	Disabled
Fast UDLD per-port enable state	Disabled on all ports

This set of configurations ensures that UDLD operates under default settings until explicitly enabled or modified to suit specific network environments.

Enable UniDirectional Link Detection Globally

Follow these steps to enable UDLD in the aggressive or normal mode and to set the configurable message timer on all fiber-optic ports on the device.

Procedure

Step 1 **enable**

Example:

```
Device>
enable
```

Enables privileged EXEC mode.

Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device#
configure terminal
```

Enters global configuration mode.

Step 3 **udld** { **aggressive** | **enable** | **message time** *message-timer-interval* }

Example:

```
Device(config)#
udld enable message time 10
```

Specifies the UDLD mode of operation:

- **aggressive** —Enables UDLD in aggressive mode on all fiber-optic ports.
- **enable** —Enables UDLD in normal mode on all fiber-optic ports on the device. UDLD is disabled by default.

  An individual interface configuration overrides the setting of the **udld enable** global configuration command.
- **message time** *message-timer-interval* —Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are detected to be bidirectional. The range is from 1 to 90 seconds; the default value is 15.

  Note
  This command affects fiber-optic ports only. Use the **udld** interface configuration command to enable UDLD on other port types.

Use the **no** form of this command, to disable UDLD.

Step 4 **end**

Example:

```
Device(config)#
end
```

Returns to privileged EXEC mode.

Enabling UDLD on an interface

Follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Specifies the port to be enabled for Fast UDLD, and enters interface configuration mode.

	Command or Action	Purpose
Step 3	**udld fast-hello** *message time interval* **Example:** `Device(config-if)# udld fast-hello 200`	Enables Fast UDLD on the specified port. • **message time** *message-timer-interval*—Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are detected to be bidirectional. **Note** Fast UDLD can be enabled only if UDLD is already enabled on the specified port.

Step 4	**end**
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode.

Enable Fast UniDirectional Link Detection on an interface

Follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port.

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode
Step 3	interface interface-id **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Specifies the port to be enabled for UDLD, and enters interface configuration mode.
Step 4	**udld port** [**aggressive**] **Example:** `Device(config-if)# udld port aggressive`	UDLD is disabled by default. • **udld port**—Enables UDLD in normal mode on the specified port. • **udld port aggressive**(Optional) Enables UDLD in aggressive mode on the specified port.

	Command or Action	Purpose

Step 5	end
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode. UDLD is configured on the specified interface, ensuring link detection and error prevention according to the chosen mode.

Enable Fast UDLD error reporting

Follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port.

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode
Step 3	interface interface-id **Example:** `Device(config)# interface gigabitethernet 1/0/1`	Specifies the port to be enabled for UDLD, and enters interface configuration mode.
Step 4	**udld port** [**aggressive**] **Example:** `Device(config-if)# udld port aggressive`	UDLD is disabled by default. • **udld port**—Enables UDLD in normal mode on the specified port. • **udld port aggressive**(Optional) Enables UDLD in aggressive mode on the specified port.

Step 5	end
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode. UDLD is configured on the specified interface, ensuring link detection and error prevention according to the chosen mode.

Disable UDLD on fiber-optic LAN interfaces

Follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port.

Procedure

	Command or Action	Purpose
Step 1	enable **Example:** `Device# enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode
Step 3	**interface** *type number* **Example:** `Device(config)#` **`interface gigabitethernet 0/1/1`**	Configures an interface and enters interface configuration mode.
Step 4	**udld port disable** **Example:** `Device(config-if)#` **`udld port disable`**	Disables UDLD on a fiber-optic LAN port. • The **udld port disable** command is only supported on fiber-optic LAN ports. • The **no udld port disable** command reverts to the **udld enable** global configuration command setting.

Step 5	end
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode. UDLD is configured on the specified interface, ensuring link detection and error prevention according to the chosen mode.

UDLD commands and their purposes

UDLD commands are used to monitor and verify the integrity of connections over network ports. Below is a list of UDLD commands with their specific purposes:

Command	Purpose
show udld [*interface-id* | **neighbors**]	Displays the UDLD status for the specified port or for all ports.
show udld fast-hello [*interface-id*]	Displays fast-hello information for the specified port or for all ports.

Console error messages for fast UDLD

Fast UDLD (Unidirectional Link Detection) generates error messages in the console when it detects a link failure. The type of error and the resulting action depend on whether **udld fast-hello error-reporting** is configured. Below are the possible error messages:

- If a unidirectional link is detected and the link is err-disabled by UDLD, the following message is displayed

  %UDLD-4-UDLD_PORT_DISABLED: UDLD disabled interface Hu1/0/10, unidirectional link detected

- If **udld fast-hello error-reporting** is configured, UDLD reports the link failure without err-disabling the affected port. The following message is displayed instead

  %UDLD-SP-4-UDLD_PORT_FAILURE: UDLD failure reported per user request, interface HU1/0/10, fast udld unidirectional link detected

- To clear the UDLD port state in either case, use the **udld reset** command. This command resets the port and resolves the error condition if the issue is fixed.