



UniDirectional Link Detection (UDLD)

- [Prerequisites for UDLD, page 12-1](#)
- [Restrictions for UDLD, page 12-1](#)
- [Information About UDLD, page 12-2](#)
- [Default Settings for UDLD, page 12-4](#)
- [How to Configure UDLD, page 12-4](#)



Note

- For complete syntax and usage information for the commands used in this chapter, see these publications:
http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
 - Cisco IOS Release 15.4SY supports only Ethernet interfaces. Cisco IOS Release 15.4SY does not support any WAN features or commands.
-



Tip

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

[Participate in the Technical Documentation Ideas forum](#)

Prerequisites for UDLD

None.

Restrictions for UDLD

None.

Information About UDLD

- [UDLD Overview, page 12-2](#)
- [UDLD Aggressive Mode, page 12-3](#)
- [Fast UDLD, page 12-4](#)

UDLD Overview

The Cisco-proprietary UDLD protocol allows devices connected through fiber-optic or copper (for example, Category 5 cabling) Ethernet cables connected to LAN ports to monitor the physical configuration of the cables and detect when a unidirectional link exists. When a unidirectional link is detected, UDLD shuts down the affected LAN port and alerts the user. Unidirectional links can 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. 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 LAN ports. When you enable both autonegotiation and UDLD, 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 transmitted by the local device over a link is received by the 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, as long as autonegotiation is active, the link does not stay up. In this case, the logical link is undetermined, and UDLD does not take any action. If both fibers are working normally at Layer 1, then UDLD at Layer 2 determines whether those fibers are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation, because autonegotiation operates at Layer 1.

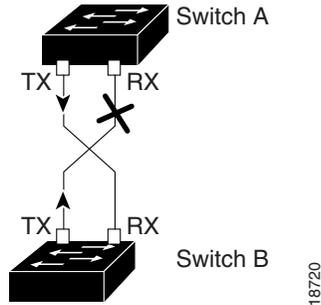
LAN ports with UDLD enabled periodically transmit UDLD packets to neighbor devices. If the packets are echoed back within a specific time frame and they are lacking a specific acknowledgment (echo), the link is flagged as unidirectional and the LAN port is shut down. Devices on both ends of the link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

**Note**

By default, UDLD is locally disabled on copper LAN ports to avoid sending unnecessary control traffic on this type of media since it is often used for access ports.

[Figure 12-1](#) shows an example of a unidirectional link condition. Switch B successfully receives traffic from Switch A on the port. However, Switch A does not receive traffic from Switch B on the same port. UDLD detects the problem and disables the port.

Figure 12-1 Unidirectional Link



18720

UDLD Aggressive Mode

UDLD aggressive mode is disabled by default. Configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

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 you enable UDLD aggressive mode, you receive additional benefits in the following situations:

- One side of a link has a port stuck (both Tx and Rx)
- One side of a link remains up while the other side of the link has gone down

In these cases, UDLD aggressive mode disables one of the ports on the link, which prevents traffic from being discarded.



Note

In UDLD normal mode, when a unidirectional error is detected, the port is not disabled. In UDLD aggressive mode, when a unidirectional error is detected, the port is disabled.

Fast UDLD

Release 15.0(1)SY1 and later releases support fast UDLD.

Fast UDLD is a per-port configuration option that supports UDLD message time intervals between 200 and 1000 milliseconds. Fast UDLD can be configured to provide subsecond unidirectional link detection. (Without fast UDLD, the message time intervals are 7 through 90 seconds).

When configuring fast UDLD, note the following guidelines and restrictions:

- Fast UDLD is disabled by default.
- Normal and aggressive mode both support fast UDLD.
- Fast UDLD ports do not support the **link debounce** command.
- Fast UDLD supports only point-to-point links between network devices that support fast UDLD.
- Configure fast UDLD on at least two links between each connected network device. Fast UDLD does not support single-link connections to neighbor devices.
- Fast UDLD does not report a unidirectional link if the same error occurs simultaneously on more than one link to the same neighbor device.
- Fast UDLD cannot detect unidirectional links when the CPU utilization exceeds 60 percent.
- Fast UDLD is supported on 60 ports with a Supervisor Engine 2T.

Default Settings for UDLD

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

How to Configure UDLD

- [Enabling UDLD Globally, page 12-5](#)
- [Enabling UDLD on LAN Interfaces, page 12-5](#)
- [Disabling UDLD on Nonfiber-Optic LAN Interfaces, page 12-5](#)
- [Disabling UDLD on Fiber-Optic LAN Interfaces, page 12-6](#)
- [Configuring the UDLD Probe Message Interval, page 12-6](#)
- [Configuring Fast UDLD, page 12-6](#)
- [Resetting Disabled LAN Interfaces, page 12-7](#)

Enabling UDLD Globally

To enable UDLD globally on all fiber-optic LAN ports, perform this task:

Command	Purpose
Router(config)# udld { enable aggressive }	Enables UDLD globally on fiber-optic LAN ports. Note This command only configures fiber-optic LAN ports. Individual LAN port configuration overrides the setting of this command.

Enabling UDLD on LAN Interfaces

To enable UDLD on a LAN port, perform this task:

	Command	Purpose
Step 1	Router(config)# interface <i>type slot/port</i>	Selects the LAN port to configure.
Step 2	Router(config-if)# udld port [aggressive]	Enables UDLD on a LAN port. <ul style="list-style-type: none"> • Enter the aggressive keyword to enable aggressive mode. • On a fiber-optic LAN port, this command overrides the udld enable global configuration command setting. • On fiber-optic LAN ports, the no udld port command reverts the LAN port configuration to the udld enable global configuration command setting.

Disabling UDLD on Nonfiber-Optic LAN Interfaces

To disable UDLD on a nonfiber-optic LAN port., perform this task:

	Command	Purpose
Step 1	Router(config)# interface <i>type slot/port</i>	Selects the LAN port to configure.
Step 2	Router(config-if)# no udld port [aggressive]	Disables UDLD on a nonfiber-optic LAN port.

Disabling UDLD on Fiber-Optic LAN Interfaces

To disable UDLD on individual fiber-optic LAN ports, perform this task:

Command	Purpose
Router(config)# interface <i>type slot/port</i>	Selects the LAN port to configure.
Router(config-if)# udld port disable	Disables UDLD on a fiber-optic LAN port. Note The no form of this command, which reverts to the udld enable global configuration command setting, is only supported on fiber-optic LAN ports.

Configuring the UDLD Probe Message Interval

To configure the time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional, perform this task:

Command	Purpose
Router(config)# udld message time <i>interval</i>	Configures the time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 7 to 90 seconds.

Configuring Fast UDLD

Release 15.0(1)SY1 and later releases support fast UDLD. These sections describe how to configure fast UDLD:

- [Configuring Fast UDLD on a Port, page 12-7](#)
- [Enabling Fast UDLD Error Reporting, page 12-7](#)



Note

You can configure fast UDLD on ports where UDLD is not enabled, but fast UDLD is active only when UDLD is enabled on the port.

Configuring Fast UDLD on a Port

To configure fast UDLD on a port, perform this task:

	Command	Purpose
Step 1	Router(config-if)# udld fast-hello <i>interval</i>	Configures the fast UDLD probe message interval on a port. <ul style="list-style-type: none"> • See the guidelines and restrictions in the “Fast UDLD” section on page 12-4. • When selecting the value, follow these guidelines: <ul style="list-style-type: none"> – Valid values are from 200 to 1000 milliseconds. – Adjust the fast UDLD probe message interval to the longest interval possible that will provide the desired link failure detection time. A shorter message interval increases the likelihood that UDLD will falsely report link failures under stressful conditions.
Step 2	Router# show udld fast-hello	Displays fast UDLD configuration and operational state.
Step 3	Router# show udld fast-hello <i>type</i> ¹ <i>slot/number</i>	Verifies the per-port fast UDLD configuration and operational state.

1. *type* = fastethernet, gigabitethernet, or tengigabitethernet

Enabling Fast UDLD Error Reporting

By default, fast UDLD error-disables ports with unidirectional links. You can globally enable fast UDLD to report unidirectional links with a message displayed on the console instead of error-disabling ports with unidirectional links.



Note

When fast UDLD error reporting is enabled, you must manually take the action appropriate for the state of the link.

To globally enable fast UDLD error reporting, perform this task:

Command	Purpose
Router(config)# udld fast-hello error-reporting	Enables fast UDLD error reporting.

Resetting Disabled LAN Interfaces

To reset all LAN ports that have been shut down by UDLD, perform this task:

Command	Purpose
Router# udld reset	Resets all LAN ports that have been shut down by UDLD.

**Tip**

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

[Participate in the Technical Documentation Ideas forum](#)
