Configuring UDLD

This chapter describes how to configure the UniDirectional Link Detection (UDLD) protocol on the Catalyst 6500 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Master Command List*, Release 12.2SX at this URL:

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

This chapter consists of these sections:

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

Understanding How UDLD Works

These sections describe how UDLD works:

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.

Please refer to RFC 5171 for a more detailed description of the algorithm for UDLD. The UDLD algorithm requires that all the devices connected to the same LAN segment be running the protocol in order for a potential misconfiguration to be detected and for a corrective action to be taken promptly.

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.

The Catalyst 6500 series switch periodically transmits UDLD packets to neighbor devices on LAN ports with UDLD enabled. 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 49-1 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 49-1   Unidirectional Link
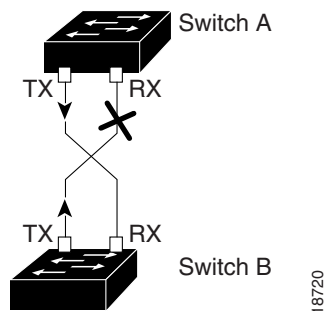
UDLD Aggressive Mode

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 discarding.

> **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.

Default UDLD Configuration

Table 49-1 shows the default UDLD configuration.

Table 49-1   UDLD Default Configuration

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

Configuring UDLD

These sections describe how to configure UDLD:

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.
Router(config)# **no udld** {**enable** | **aggressive**}	Disables UDLD globally on fiber-optic LAN ports.

Enabling UDLD on Individual LAN Interfaces

To enable UDLD on individual LAN ports, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** *type*[1] *slot/port*	Selects the LAN port to configure.
Step 2	Router(config-if)# **udld port** [**aggressive**]	Enables UDLD on a specific LAN port. Enter the **aggressive** keyword to enable aggressive mode. On a fiber-optic LAN port, this command overrides the **udld enable** global configuration command setting.
	Router(config-if)# **no udld port** [**aggressive**]	Disables UDLD on a nonfiber-optic LAN port. **Note** On fiber-optic LAN ports, the **no udld port** command reverts the LAN port configuration to the **udld enable** global configuration command setting.
Step 3	Router# **show udld** *type*[1] *slot/number*	Verifies the configuration.

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

Disabling UDLD on Fiber-Optic LAN Interfaces

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

	Command	Purpose
Step 1	Router(config)# **interface** *type*[1] *slot/port*	Selects the LAN port to configure.
Step 2	Router(config-if)# **udld port disable**	Disables UDLD on a fiber-optic LAN port.
	Router(config-if)# **no udld port disable**	Reverts to the **udld enable** global configuration command setting.
		Note This command is only supported on fiber-optic LAN ports.
Step 3	Router# **show udld** *type*[1] *slot/number*	Verifies the configuration.

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

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
Step 1	Router(config)# **udld message time** *interval*	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.
	Router(config)# **no udld message**	Returns to the default value (60 seconds).
Step 2	Router# **show udld** *type*[1] *slot/number*	Verifies the configuration.

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

Displaying Disabled LAN Interfaces

To display the status of LAN ports in an error-disabled state, perform this task:

Command	Purpose
Router# **show udld neighbors** Port Device Name Device ID Port ID Neighbor State ---- ----------- --------- ------- -------------- Gi3/1 SAL0734K5R2 1 Gi4/1 Bidirectional Gi4/1 SAL0734K5R2 1 Gi3/1 Bidirectional	Displays UDLD neighbors.

Displaying UDLD Neighbor Interfaces

To display UDLD-enabled neighbors, perform this task:

Command	Purpose
```Router# show udld neighbors Port Device Name Device ID Port ID Neighbor State ---- ----------- --------- ------- -------------- Gi3/1 SAL0734K5R2 1 Gi4/1 Bidirectional Gi4/1 SAL0734K5R2 1 Gi3/1 Bidirectional```	Displays UDLD neighbors.

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