Configuring UniDirectional Link Detection

Finding Feature Information, page 1
Restrictions for Configuring UDLD, page 1
Information About UDLD, page 2
How to Configure UDLD, page 5
Monitoring and Maintaining UDLD, page 7
Additional References for UDLD, page 8
Feature Information for UDLD, page 9

Finding Feature Information

IEEE 802.1x port-based authentication prevents unauthorized devices (clients) from gaining access to the network. Unless otherwise noted, the term switch refers to a standalone switch and to a switch stack.

Note
Stacking is supported only on Catalyst 2960-S switches running the LAN base image.

Restrictions for Configuring UDLD

The following are restrictions for configuring UniDirectional Link Detection (UDLD):

- A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another controller.
- When configuring the mode (normal or aggressive), make sure that the same mode is configured on both sides of the link.

Caution
Loop guard works only on point-to-point links. We recommend that each end of the link has a directly connected device that is running STP.
Information About UDLD

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 and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it disables the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

Modes of Operation

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

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic port are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the ports 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 this case, the logical link is considered undetermined, and UDLD does not disable the port.

When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up because the Layer 1 mechanisms detects a physical problem with the link. In this case, UDLD does not take any action and the logical link is considered undetermined.

Related Topics

- Enabling UDLD Globally (CLI), on page 5
- Enabling UDLD on an Interface (CLI), on page 6

Aggressive Mode

In aggressive mode, UDLD detects a unidirectional link by using the previous detection methods. UDLD in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It can also detect a unidirectional link when one of these problems exists:

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

In these cases, UDLD disables the affected port.

In a point-to-point link, UDLD hello packets can be considered as a heart beat whose presence guarantees the health of the link. Conversely, the loss of the heart beat means that the link must be shut down if it is not possible to reestablish a bidirectional link.

If both fiber strands in a cable are working normally from a Layer 1 perspective, UDLD in aggressive mode detects whether those fiber strands 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.

Related Topics
   Enabling UDLD Globally ( CLI ), on page 5
   Enabling UDLD on an Interface ( CLI ), on page 6

Methods to Detect Unidirectional Links

UDLD operates by using two methods:

• Neighbor database maintenance
• Event-driven detection and echoing

Related Topics
   Enabling UDLD Globally ( CLI ), on page 5
   Enabling UDLD on an Interface ( CLI ), on page 6

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 port to keep each device informed about its neighbors.

When the controller receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the controller receives a new hello message before an older cache entry ages, the controller replaces the older entry with the new one.

Whenever a port is disabled and UDLD is running, whenever UDLD is disabled on a port, or whenever the controller is reset, UDLD clears all existing cache entries for the ports 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 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 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 port is disabled.

Related Topics
- Enabling UDLD Globally (CLI), on page 5
- Enabling UDLD on an Interface (CLI), on page 6

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 configuration 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.

Related Topics
- Enabling UDLD Globally (CLI), on page 5
- Enabling UDLD on an Interface (CLI), on page 6

Default UDLD Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDLD global enable state</td>
<td>Globally disabled</td>
</tr>
<tr>
<td>UDLD per-port enable state for fiber-optic media</td>
<td>Disabled on all Ethernet fiber-optic ports</td>
</tr>
<tr>
<td>UDLD per-port enable state for twisted-pair (copper) media</td>
<td>Disabled on all Ethernet 10/100 and 1000BASE-TX ports</td>
</tr>
<tr>
<td>UDLD aggressive mode</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Related Topics
- Enabling UDLD Globally (CLI), on page 5
How to Configure UDLD

Enabling UDLD Globally (CLI)

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 controller.

**SUMMARY STEPS**

1. `configure terminal`
2. `udld {aggressive | enable | message time message-timer-interval}`
3. `end`

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * `configure terminal` | Enters global configuration mode. |

  **Example:**
  ```
  Controller# configure terminal
  ```

| **Step 2**
  * `udld {aggressive | enable | message time message-timer-interval}` | 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 controller. UDLD is disabled by default. |

  **Example:**
  ```
  Controller(config)# udld enable message time 10
  ```

  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.
### Enabling UDLD on an Interface (CLI)

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Controller# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Controller(config)# <code>interface</code></td>
</tr>
</tbody>
</table>

---

### Related Topics
- Monitoring and Maintaining UDLD
- Aggressive Mode, on page 2
- Normal Mode, on page 2
- Methods to Detect Unidirectional Links, on page 3
- Event-Driven Detection and Echoing, on page 3
- UDLD Reset Options, on page 4
- Default UDLD Configuration, on page 4

---

### Command or Action

**Step 3**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Controller(config)# <code>end</code></td>
</tr>
</tbody>
</table>
Configuring UniDirectional Link Detection

### Step 3

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>gigabitethernet 1/0/1</td>
<td>UDLD is disabled by default.</td>
</tr>
</tbody>
</table>

**Example:**

```
Controller(config-if)# udld port
```

- **udld port**—Enables UDLD in normal mode on the specified port.
- **udld port aggressive**—(Optional) Enables UDLD in aggressive mode on the specified port.

**Note** Use the `no udld port` interface configuration command to disable UDLD on a specified fiber-optic port.

### Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Controller(config-if)# end
```

### Related Topics

- Monitoring and Maintaining UDLD
- Aggressive Mode, on page 2
- Normal Mode, on page 2
- Methods to Detect Unidirectional Links, on page 3
- Event-Driven Detection and Echoing, on page 3
- UDLD Reset Options, on page 4
- Default UDLD Configuration, on page 4

### Monitoring and Maintaining UDLD

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show udld [interface-id</td>
<td>neighbors]`</td>
</tr>
</tbody>
</table>
# Additional References for UDLD

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 command reference</td>
<td><em>Layer 2 Command Reference (Cisco WLC 5700 Series)</em></td>
</tr>
</tbody>
</table>

## Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

## Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed</td>
<td></td>
</tr>
<tr>
<td>from Field Notices), the Cisco Technical Services Newsletter, and Really</td>
<td></td>
</tr>
<tr>
<td>Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for UDLD

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.2SE</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Feature Information for UDLD