Unidirectional Link Detection (UDLD)

Unidirectional Link Detection (UDLD) is a Cisco proprietary layer 2 protocol used to determine the physical status of a link. The purpose of Unidirectional Link Detection (UDLD) is to detect and deter issues that arise from Unidirectional Links. UDLD helps to prevent forwarding loops and blackholing of traffic by identifying and acting on logical one-way links that would otherwise go undetected.

UDLD Overview

Each switch port that is configured for UDLD exchanges UDLD protocol packets that include information about the port’s device and port ID, and the port also sends the same device and port ID information that it knows about its connected neighbor. Because of this, a port should receive its own device and port ID information from its neighbor if the link is bi-directional. If a port does not receive information about its own device and port ID from its neighbor, the link is considered to be unidirectional. This can occur when the link is up on both sides, but one side is not receiving packets, or when wiring mistakes occur, causing the transmit and receive wires to not be connected to the same ports on both ends of a link.

Note: Both ends of a link need to support UDLD for this feature to work correctly.

Supported Models for UDLD: MS22, MS42, MS120, MS125, MS210, MS220, MS225, MS250, MS320, MS350, MS355, MS400 series

Meraki Implementation Overview

- UDLD is supported in all Meraki switches running 10.10 and above
- UDLD is run independently on a per-switch basis, regardless of any stacking involved
- An Event Log will be generated upon detecting a UDLD-error state
- Both ends of a link need to support UDLD for this feature to initiate
- The Meraki implementation is fully interoperable with the one implemented in traditional Cisco switches
- Upon detecting a UDLD issue, there are two configurable responses:
  1. Alert only
     - Alerts will be generated if UDLD detects an error, but traffic will not be blocked
     - This is the default configuration
2. **Enforce**
   - Recommended on point-to-point links to prevent loops
   - Non-UDLD traffic will be blocked if UDLD detects an error. While other traffic is discarded while in a UDLD-error state, UDLD traffic will continue to monitor the link, providing auto-recovery functionality

---

**UDLD Error Conditions**

UDLD will trigger both when there is a Unidirectional Link and when there is a Transmit(TX)/Receive(RX) Loop, as outlined below.
Configuring UDLD

How a switch responds to a UDLD-error state can be configured per switchport by navigating to the Switch > Monitor > Switch ports page and clicking on an individual switchport. This will bring up a switchport configuration window that will allow you to select how the individual switchport responds to a UDLD-error state.

Multi-Point Setup

For UDLD in a point-to-point link, both ends of a link support UDLD. With UDLD multi-point links, however, two or more UDLD-capable ports are connected through one or more switches that don't support UDLD (e.g. non-Cisco switches or Meraki switches with older firmware).

We do not enable the Enforce mode by default since this can result in ports being disabled too aggressively on some multi-point setups. Take the network bellow as an example, where the link from A to D goes unidirectional. Here, UDLD on switch C would disable the link to D, cutting at the same time its path to B, which doesn't exhibit any issues.
Network without UDLD

In the below example we have three interconnected switches with an extra redundant link. Switch A is the STP root bridge, the flow of BPDUs are denoted by purple arrows, and STP convergence results in Switch B placing its connection to C into a blocking state.

1. This is our baseline topology.

2. The link then becomes unidirectional such that packets only go from B to C. As a result, Switch B stops receiving BPDUs from Switch C.
3. Switch B transitions its port to a forwarding state and broadcast packets begin to loop through the network.

**Network with UDLD**

The same unidirectional link suddenly arrises as outlined in step 2 above. With UDLD, however, the unidirectional link is detected even before STP on Switch B has had time to transition its port to a forwarding state.
Via UDLD, Switch B detects a unidirectional link and begins to block traffic on the port leading to Switch C. This loop, which would have otherwise gone undetected by STP, has been identified and mitigated.

For some additional reading on relevant MS configurations and loop-prevention features:

- Configuring Spanning Tree on Meraki Switches
- RSTP on the MS switch

**Cisco Interoperability Clarifications**

The Meraki implementation is fully inter-operable with the one implemented in traditional Cisco switches. However, there are a few differences that should be noted:

- Traditional Cisco equipment supports 'aggressive' and 'normal' UDLD modes. Meraki is able to implement similar functionality using just the 'normal' mode
In Alert only mode, the Meraki implementation generates a Dashboard alert and Event Log entry. Traffic is still forwarded when a UDLD-error state is seen while configured in Alert only mode.

In Enforce mode, our behavior is mostly comparable to Cisco's aggressive mode. In our way of 'disabling' the port, we block all traffic, similar to the STP blocking state. This does not physically bring the link down, though, as in a traditional Cisco 'aggressive' configuration.

<table>
<thead>
<tr>
<th>Behavior when Unidirectional Link is Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Normal Mode</strong></td>
</tr>
<tr>
<td>- Port state is marked as undetermined</td>
</tr>
<tr>
<td>- Port behaves according to STP state</td>
</tr>
<tr>
<td><strong>Cisco Aggressive Mode</strong></td>
</tr>
<tr>
<td>- UDLD attempts to re-establish state of the port</td>
</tr>
<tr>
<td>- Port is put into the <strong>errdisable</strong> state if unable to re-establish port state</td>
</tr>
<tr>
<td>- Port is actually disabled</td>
</tr>
<tr>
<td><strong>Meraki Alert Only Mode</strong></td>
</tr>
<tr>
<td>- Generates dashboard alert and event log entry</td>
</tr>
<tr>
<td>- Port behaves according to STP state</td>
</tr>
<tr>
<td><strong>Meraki Enforce Mode</strong></td>
</tr>
<tr>
<td>- All traffic on the port is blocked, similar to STP blocking</td>
</tr>
<tr>
<td>- Port is not disabled</td>
</tr>
<tr>
<td>- UDLD traffic will continue to monitor the link, providing auto-recovery functionality</td>
</tr>
</tbody>
</table>