Understanding and Configuring the Unidirectional Link Detection Protocol Feature

Document ID: 10591

Contents

Introduction

This document explains how the Unidirectional Link Detection (UDLD) protocol can help to prevent forwarding loops and blackholing of traffic in switched networks.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Problem Definition

Spanning−Tree Protocol (STP) resolves redundant physical topology into a loop−free, tree−like forwarding topology.

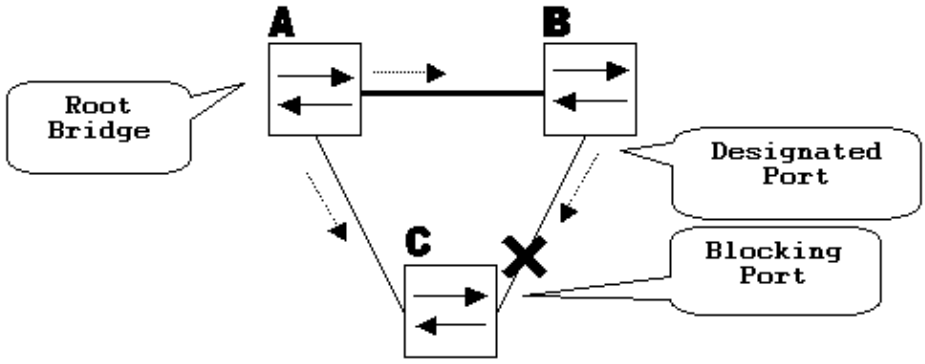
This is done by blocking one or more ports. By blocking one or more ports, there are no loops in the forwarding topology. STP relies in its operation on reception and transmission of the Bridge Protocol Data Units (BPDUs). If the STP process that runs on the switch with a blocking port stops receiving BPDUs from its upstream (designated) switch on the port, STP eventually ages out the STP information for the port and moves it to the `forwarding` state. This creates a forwarding loop or STP loop.

Packets start to cycle indefinitely along the looped path, and consumes more and more bandwidth. This leads to a possible network outage.

How is it possible for the switch to stop receiving BPDUs while the port is `up`? The reason is unidirectional link. A link is considered unidirectional when this occurs:

- The link is `up` on both sides of the connection. The local side is not receiving the packets sent by the remote side while remote side receives packets sent by local side.

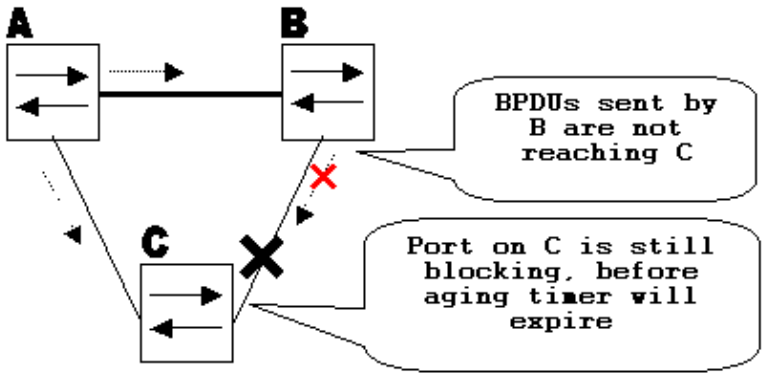
Consider this scenario. The arrows indicate the flow of STP BPDUs.



During normal operation, bridge B is designated on the link B−C. Bridge B sends BPDUs down to C, which is blocking the port. The port is blocked while C sees BPDUs from B on that link.

Now, consider what happens if the link B−C fails in the direction of C. C stops receiving traffic from B, however, B still receives traffic from C.

C stops receiving BPDUs on the link B−C, and ages the information received with the last BPDU. This takes up to 20 seconds, depending on the maxAge STP timer. Once the STP information is aged out on the port, that port transitions from the `blocking` state to the `listening`, `learning`, and eventually to the `forwarding` STP state. This creates a forwarding loop, as there is no blocking port in the triangle A−B−C. Packets cycle along the path (B still receives packets from C) taking additional bandwidth until the links are completely filled up. This brings the network down.



Another possible issue that can be caused by a unidirectional link is traffic blackholing.

How Unidirectional Link Detection Protocol Works

In order to detect the unidirectional links before the forwarding loop is created, Cisco designed and implemented the UDLD protocol.

UDLD is a Layer 2 (L2) protocol that works with the Layer 1 (L1) mechanisms to determine the physical status of a link. At Layer 1, auto−negotiation takes care of physical signaling and fault detection. UDLD performs tasks that auto−negotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both auto−negotiation and UDLD, Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

UDLD works by exchanging protocol packets between the neighboring devices. In order for UDLD to work, both devices on the link must support UDLD and have it enabled on respective ports.

Each switch port configured for UDLD sends UDLD protocol packets that contain the port's own device/port ID, and the neighbor's device/port IDs seen by UDLD on that port. Neighboring ports should see their own device/port ID (echo) in the packets received from the other side.

If the port does not see its own device/port ID in the incoming UDLD packets for a specific duration of time, the link is considered unidirectional.

This echo−algorithm allows detection of these issues:

- Link is `up` on both sides, however, packets are only received by one side.
- Wiring mistakes when receive and transmit fibers are not connected to the same port on the remote side.

Once the unidirectional link is detected by UDLD, the respective port is disabled and this message is printed on the console:

```
UDLD−3−DISABLE: Unidirectional link detected on port 1/2. Port disabled
```

Port shutdown by UDLD remains disabled until it is manually reenabled, or until `errdisable` timeout expires (if configured).

UDLD Modes of Operation

UDLD can operate in two modes: `normal` and `aggressive`.

In `normal` mode, if the link state of the port was determined to be bi−directional and the UDLD information times out, no action is taken by UDLD. The port state for UDLD is marked as `undetermined`. The port behaves according to its STP state.

In `aggressive` mode, if the link state of the port is determined to be bi−directional and the UDLD information times out while the link on the port is still `up`, UDLD tries to re−establish the state of the port. If not successful, the port is put into the `errdisable` state.

Aging of UDLD information happens when the port that runs UDLD does not receive UDLD packets from the neighbor port for duration of hold time. The hold time for the port is dictated by the remote port and depends on the message interval at the remote side. The shorter the message interval, the shorter the hold time and the faster the detection. Recent implementations of UDLD allow configuration of message interval.

UDLD information can age out due to the high error rate on the port caused by some physical issue or duplex mismatch. Such packet drop does not mean that the link is unidirectional and UDLD in `normal` mode will not disable such link.

It is important to be able to choose the right message interval in order to ensure proper detection time. The message interval should be fast enough to detect the unidirectional link before the forwarding loop is created, however, it should not overload the switch CPU. The default message interval is 15 seconds, and is fast enough to detect the unidirectional link before the forwarding loop is created with default STP timers. The detection time is approximately equal to three times the message interval.

For example: $T_{detection}$ ~ message_interval x3

This is 45 seconds for the default message interval of 15 seconds.

It takes $T_{reconvergence}$=max_age + 2x forward_delay for the STP to reconverge in case of unidirectional link failure. With the default timers, it takes 20+2x15=50 seconds.

It is recommended to keep $T_{detection} < T_{reconvergence}$ by choosing an appropriate message interval.

In `aggressive` mode, once the information is aged, UDLD will make an attempt to re−establish the link state by sending packets every second for eight seconds. If the link state is still not determined, the link is disabled.

`Aggressive` mode adds additional detection of these situations:

- The port is stuck (on one side the port neither transmits nor receives, however, the link is `up` on both sides).
- The link is `up` on one side and `down` on the other side. This is issue might be seen on fiber ports. When transmit fiber is unplugged on the local port, the link remains `up` on the local side. However, it is `down` on the remote side.

Most recently, fiber FastEthernet hardware implementations have Far End Fault Indication (FEFI) functions in order to bring the link `down` on both sides in these situations. On Gigabit Ethernet, a similar function is provided by link negotiation. Copper ports are normally not susceptible to this type of issue, as they use Ethernet link pulses to monitor the link. It is important to mention that in both cases, no forwarding loop occurs because there is no connectivity between the ports. If the link is `up` on one side and `down` on the other, however, blackholing of traffic might occur. Aggressive UDLD is designed to prevent this.

Availability

UDLD is available in normal mode for:

- Catalyst OS Version 5.1.1 and later for Catalyst 4500/4000, 5500/5000, and 6500/6000 family switches
- Cisco IOS® Software Release 12.0(5)XU and later for Catalyst 2900XL and 3500XL switches
- Cisco IOS Software Release 12.1(13)AY and later for Catalyst 2940 switches
- Cisco IOS Software Release 12.0(5)WC(1) or later for Catalyst 2950 switches
- Cisco IOS Software Release 12.1(12c)EA1 or later for Catalyst 2955 switches
- Cisco IOS Software Release 12.1(11)AX or later for Catalyst 2970 switches
- Cisco IOS Software Release 12.1(4)EA1 or later for the Catalyst 3550 switches
- Cisco IOS Software Release 12.1(19)EA1 or later for the Catalyst 3560 switches
- Cisco IOS Software Release 12.1(11)AX or later for the Catalyst 3750 switches
- Cisco IOS Software Release 12.1(2)E and later for Catalyst 6500/6000 switches running Cisco IOS

system software
- Cisco IOS Software Release 12.1(8a)EW and later for Catalyst 4500/4000 switches running Cisco IOS

`Aggressive` mode is implemented beginning with these software versions:

- Catalyst OS Version 5.4.3 and later for Catalyst 4500/4000, 5500/5000, and 6500/6000 family switches
- Cisco IOS Software Release 12.1(3a)E3 and later for Catalyst 6500/6000 switches running Cisco IOS system software
- Cisco IOS Software Release 12.1(6)EA2 or later for the Catalyst 2950 switches
- Cisco IOS Software Release 12.1(12c)EA1 or later for Catalyst 2955 switches
- Cisco IOS Software Release 12.1(11)AX or later for the Catalyst 2970 switches
- Cisco IOS Software Release 12.1(4)EA1 or later for the Catalyst 3550 switches
- Cisco IOS Software Release 12.1(11)AX or later for the Catalyst 3750 switches

Configuration and Monitoring

These commands detail the UDLD configuration on Catalyst switches that run CatOS. UDLD needs to first be enabled globally (default is disabled) with this command:

```
Vega> (enable) set udld enable
UDLD enabled globally
```

Issue this command: to verify whether the UDLD is enabled

```
Vega> (enable) show udld
UDLD:  enabled
Message Interval: 15 seconds
```

UDLD also needs to be enabled on necessary ports with this command:

```
Vega> (enable) set udld enable 1/2
UDLD enabled on port 1/2
```

Issue the **show udld port** command to verify whether UDLD is enabled or disabled on the port and what the link state is:

```
Vega> (enable) show udld port
UDLD              : enabled
Message Interval  : 15 seconds

Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
 1/1      enabled       disabled         undetermined
 1/2      enabled       disabled         bidirectional
```

Aggressive UDLD is enabled on a per−port basis with the **set udld aggressive−mode enable** <*module/port*> command:

```
Vega> (enable) set udld aggressive-mode enable 1/2
Aggressive UDLD enabled on port 1/2.
Vega> (enable) show udld port 1/2
UDLD              : enabled
Message Interval  : 15 seconds

Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
```

```
1/2      enabled       enabled          undetermined
```

Issue this command to change the message interval:

```
Vega> (enable) set udld interval 10
UDLD message interval set to 10 seconds
```

The interval can range from 7 to 90 seconds, with the default being 15 seconds.

Refer to these documents for more information on the IOS UDLD configuration:

- For Catalyst 6500/6000 switches that run Cisco IOS system software, refer to Configuring UDLD.
- For Catalyst 2900XL/3500XL switches, refer to the *Configuring UniDirectional Link Detection* section of Configuring the Switch Ports.
- For Catalyst 2940 switches, refer to Configuring UDLD.
- For Catalyst 2950/2955 switches, refer to Configuring UDLD.
- For Catalyst 2970 switches, refer to Configuring UDLD.
- For Catalyst 3550 switches, refer to Configuring UDLD.
- For Catalyst 3560 switches, refer to Configuring UDLD.
- For Catalyst 4500/4000 running Cisco IOS, refer to Configuring UDLD.

Related Information

- **LAN Switching Technology Support**
- **Catalyst LAN and ATM Switches Product Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jul 09, 2007 Document ID: 10591