

単方向リンク検出プロトコル機能の説明と設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[問題の定義](#)

[単方向リンク検出プロトコルの動作のしくみ](#)

[UDLD の動作モード](#)

[アベイラビリティ](#)

[設定とモニタリング](#)

[関連情報](#)

概要

このドキュメントでは、Unidirectional Link Detection (UDLD; 単方向リンク検出) プロトコルが、スイッチド ネットワークでのトラフィックのフォワーディング ループとブラック ホールの発生を防止するのに、どのように役立つかを説明しています。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

問題の定義

Spanning-Tree Protocol (STP; スパニングツリー プロトコル) を使用すれば、冗長な物理トポロジを解決して、ループが発生しないツリー状の転送トポロジを構築できます。

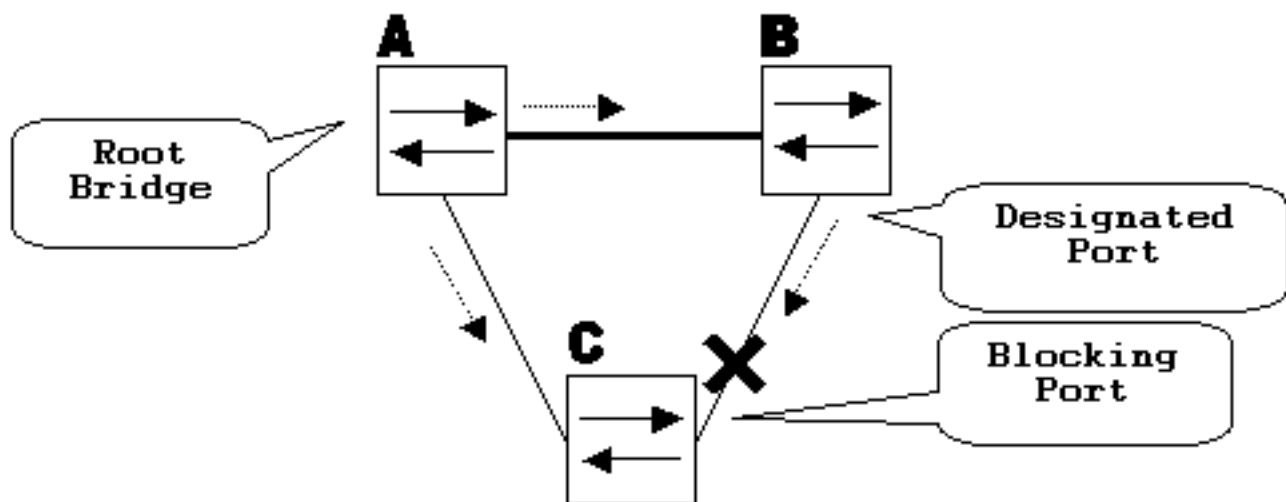
この機能は、1つまたは複数のポートをブロックすることによって実現されます。1つ以上のポートをブロックすることにより、転送トポロジにループがなくなります。STPの動作は、Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータユニット)の受信と送信に依存しています。ポートがブロックされたスイッチ上で動作するSTPプロセスで、そのポートのアップストリームの(指定された)スイッチからのBPDUが受信されなくなると、STPにより最終的にはそのポートのSTP情報がエージングアウトされて、forwarding状態に移行されます。こうなると、フォワーディングループまたはSTPループが発生します。

ループになったパスをパケットが無限に回り始め、ますます帯域幅が消費されるようになります。その結果、ネットワークが停止する可能性があります。

ポートがup状態である間、どのようにすればスイッチがBPDUの受信を停止することができますか。これは単方向リンクが原因です。次の状況が発生すると、リンクは単方向とみなされます。

- リンクの接続の両端がup状態になっている。ローカル側はリモート側から送信されたパケットを受信していないが、リモート側はローカル側から送信されたパケットを受信している。

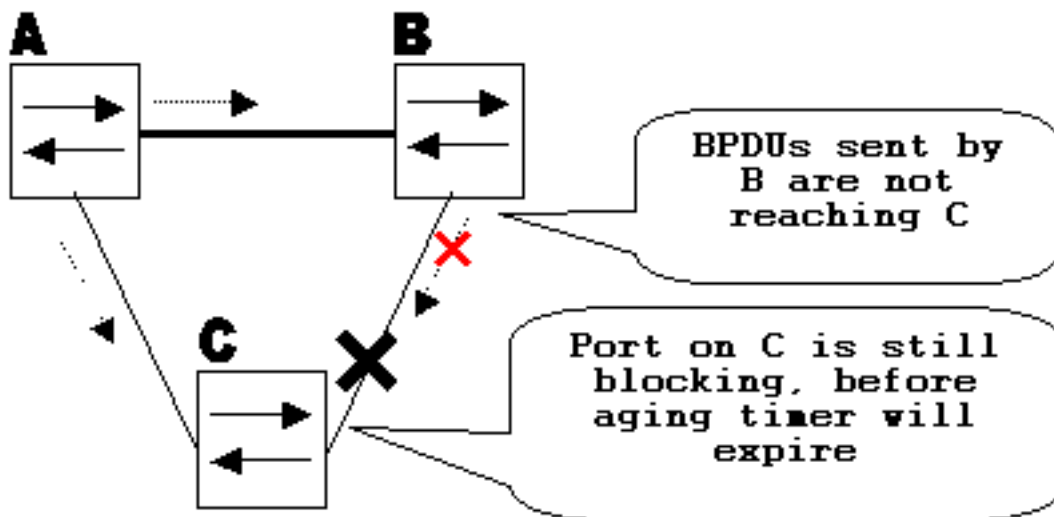
次のシナリオについて考えます。矢印はSTP BPDUの流れを示しています。



通常の実作では、ブリッジ B はリンク B-C で指定ブリッジです。ブリッジ B は、ポートをブロックしている C に BPDU を送信します。B からの BPDU がそのリンク上に正しく送信されていることが C で認識されている間は、ポートがブロックされます。

ここで、リンク B-C に C 方向の障害が発生したらどうなるかを考えます。C は B からのトラフィックを受信しなくなりますが、B は引き続き C からのトラフィックを受信します。

C はリンク B-C 上の BPDU を受信しなくなり、最後の BPDU で受信した情報のエージングが行われます。maxAge STP タイマーの設定によりますが、これには最大 20 秒かかります。ポートの STP 情報がエージングアウトされると、そのポートの状態は blocking から listening、learning に移行し、最終的には forwarding STP 状態に移行します。これにより、A-B-C の三点内にブロッキングポートがなくなるので、フォワーディングループが発生します。パケットはこのパスを循環することになり (B は引き続き C からのパケットを受信します)、リンクが完全にいっぱいになるまで帯域幅がさらに使用されていきます。その結果、ネットワークがダウンします。



単方向リンクにより発生する可能性のある問題にはほかに、トラフィックのブラックホール化があります。

単方向リンク検出プロトコルの動作のしくみ

転送ループが発生する前に単方向リンクを検出するために、シスコは UDLD プロトコルを設計し、実装しています。

UDLD は、レイヤ 1 (L1) メカニズムと連携し、リンクの物理的な状態を判別するレイヤ 2 (L2) プロトコルです。レイヤ 1 では、オートネゴシエーションによって、物理的シグナリングと障害検出が行われます。UDLD では、隣接ルータの識別情報の検出や正しく接続されていないポートのシャットダウンなど、オートネゴシエーションでは行えないタスクが実行されます。オートネゴシエーションと UDLD の両方を有効にすると、レイヤ 1 とレイヤ 2 の検出機能がともに動作して、物理的および論理的な単方向接続と他のプロトコルの動作不良が防止されます。

UDLD は、隣接デバイス間でプロトコル パケットを交換することによって動作しています。UDLD が正しく動作するには、リンク上の両方のデバイスで UDLD がサポートされており、それぞれのポートで有効になっている必要があります。

UDLD が設定されている各スイッチ ポートでは、そのポート自身のデバイス ID またはポート ID およびそのポートの UDLD で認識された隣接デバイスまたは隣接ポートの ID が格納された、UDLD プロトコル パケットが送信されます。隣接ポートでは、もう一方の側から受信したパケットに、自分のデバイス ID またはポート ID (エコー) が認識される必要があります。

着信 UDLD パケットで、自分のデバイス ID またはポート ID を特定の期間認識できないと、リンクは単方向とみなされます。

エコーアルゴリズムを使用すれば、次の問題を検出できます。

- リンクは両側で up 状態になっているが、パケットは片側だけで受信されている。
- リモート側の同じポートに受信ファイバと送信ファイバが接続されていない場合の配線ミス。

UDLD により単方向リンクが検出されると、対応するポートが無効にされて、次のメッセージがコンソールに表示されます。

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

UDLD によってシャットダウンされたポートは、手動で再び有効にするか、(設定されている場合は) errdisable タイムアウトの有効期限が切れるまで、無効のままになります。

UDLD の動作モード

UDLD は、2 つのモードで操作できます。normal および aggressive。

normal モードでは、ポートのリンク状態が双方向と判別されている場合に UDLD 情報がタイムアウトした場合、UDLD では何のアクションも取られません。UDLD のポート状態は undetermined となります。ポートは STP の状態に従って動作します。

aggressive モードでは、ポートのリンク状態が双方向と判別されている場合に、ポート上のリンクが引き続き up 状態の間に UDLD 情報がタイムアウトすると、UDLD ではポートの状態の再確立が試みられます。再確立に失敗したら、ポートは errdisable 状態になります。

UDLD が動作しているポートで、保留時間の間に隣接ポートから UDLD パケットが受信されないと、UDLD 情報のエイジングアウトが発生します。ポートの保留時間はリモートポートによって規定され、リモート側のメッセージ間隔に依存します。メッセージ間隔が短ければ短いほど、保留時間が短くなって検出が速くなります。最近実装された UDLD では、メッセージ間隔を設定できます。

一部の物理的な問題や全二重/半二重の mismatch が原因でポートでのエラー率が高くなると、UDLD 情報がエイジングアウトする場合があります。この場合のパケットの廃棄はリンクが単方向になったことを意味するものではないので、normal モードの UDLD では、そのようなリンクが無効にされることはありません。

適正な検出時間を確保するためには、正しいメッセージ間隔を選択できることが重要です。メッセージ間隔は、フォワーディング ループが形成される前に単方向リンクを検出できる程度には速い必要がありますが、スイッチの CPU を過負荷にする程ではありません。デフォルトのメッセージ間隔は 15 秒ですが、これはデフォルトの STP タイマーでフォワーディング ループが形成される前に単方向リンクを検出するのに十分な速さです。検出時間は、メッセージ間隔のおよそ 3 倍です。

次に、例を示します。 $T_{\text{検出}} | \text{message_interval} \times 3$

これは、デフォルトのメッセージ間隔 15 秒に対し、45 秒になります。

それは単方向リンク障害の場合には再収束する STP のために forward_delay $T_{\text{reconvergence}=\text{max_age}} + 2x$ を奪取します。デフォルト タイマーの設定では、 $20+2x15=50$ 秒かかります。

適切なメッセージ インターバルの選択によって $T_{\text{検出}} < T_{\text{再収束}}$ を保存することを推奨します。

aggressive モードでは、情報がエイジングされると、UDLD は、8 秒ごとにパケット送信を行い、リンク状態の再確立を試行します。リンク状態を引き続き判別できない場合は、リンクが無効になります。

aggressive モードでは、さらに次の状況が検出されます。

- ポートがスタックしている (ポートの片側は送信も受信もしていないが、リンクは両側で up 状態である)。

- リンクの片側は up 状態で、もう一方の側は down 状態である。この問題は、ファイバポートで発生する場合があります。ローカルポートの送信ファイバが抜かれても、ローカル側のリンクは up 状態を維持します。ただし、リモート側では down 状態になります。

最近では、これらの場合に両側のリンクを down 状態にするために、ファイバの FastEthernet のハードウェアに Far End Fault Indication (FEFI) 機能が実装されています。ギガビットイーサネットでは、リンクネゴシエーションによって同様の機能が実現されています。銅線ポートでは、イーサネットリンクのパルスを使用してリンクが監視されているので、このタイプの問題は通常発生しません。両方のケースともに重要なのは、ポート間が接続されていないので、フォワーディングループは形成されないという点です。ただし、リンクが一方で up、他方で down になっている場合は、トラフィックのブラックホールが発生する場合があります。アグレッシブ UDLD は、これを回避する設計になっています。

アベイラビリティ

通常モードの UDLD は、次のバージョンで使用可能です。

- Catalyst 4500/4000、5500/5000、および 6500/6000 ファミリスイッチでは Catalyst OS バージョン 5.1.1 以降
- Catalyst 2900XL および 3500XL スイッチ用の Cisco IOS® ソフトウェアリリース 12.0(5)XU およびそれ以降
- Catalyst 2940 スイッチでは Cisco IOS ソフトウェア リリース 12.1(13)AY 以降
- Catalyst 2950 スイッチでは Cisco IOS ソフトウェア リリース 12.0(5)WC(1) 以降
- Catalyst 2955 スイッチでは Cisco IOS ソフトウェア リリース 12.1(12c)EA1 以降
- Catalyst 2970 スイッチでは Cisco IOS ソフトウェア リリース 12.1(11)AX 以降
- Catalyst 3550 スイッチでは Cisco IOS ソフトウェア リリース 12.1(4)EA1 以降
- Catalyst 3560 スイッチでは Cisco IOS ソフトウェア リリース 12.1(19)EA1 以降
- Catalyst 3750 スイッチでは Cisco IOS ソフトウェア リリース 12.1(11)AX 以降
- Cisco IOS システム ソフトウェアが稼働している Catalyst 6500/6000 スイッチでは Cisco IOS ソフトウェア リリース 12.1(2)E 以降
- Cisco IOS が稼働している Catalyst 4500/4000 スイッチでは Cisco IOS ソフトウェア リリース 12.1(8a)EW 以降

aggressive モードは、次のソフトウェアバージョン以降で実装されています。

- Catalyst 4500/4000、5500/5000、および 6500/6000 ファミリスイッチでは Catalyst OS バージョン 5.4.3 以降
- Cisco IOS システム ソフトウェアが稼働している Catalyst 6500/6000 スイッチでは Cisco IOS ソフトウェア リリース 12.1(3a)E3 以降
- Catalyst 2950 スイッチでは Cisco IOS ソフトウェア リリース 12.1(6)EA2 以降
- Catalyst 2955 スイッチでは Cisco IOS ソフトウェア リリース 12.1(12c)EA1 以降
- Catalyst 2970 スイッチでは Cisco IOS ソフトウェア リリース 12.1(11)AX 以降
- Catalyst 3550 スイッチでは Cisco IOS ソフトウェア リリース 12.1(4)EA1 以降
- Catalyst 3750 スイッチでは Cisco IOS ソフトウェア リリース 12.1(11)AX 以降

設定とモニタリング

次のコマンドは、CatOS が稼働している Catalyst スイッチで UDLD の設定の詳細を示します。次のコマンドを使用して、まず UDLD をグローバルに有効にする必要があります (デフォルトでは無効になっています)。

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

次のコマンドを発行します。UDLD が有効かどうかを確認します。

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

また、次のコマンドを使用して、必要なポートで UDLD を有効にすることも必要です。

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

UDLD がポートで有効なのか無効なのか、およびリンクの状態を確認するには、**show udld port** コマンドを発行します。

```
Vega> (enable) show udld port UDLD : enabled Message Interval : 15 seconds Port Admin Status
Aggressive Mode Link State -----
disabled undetermined 1/2 enabled disabled bidirectional
```

ポートごとに **set udld aggressive-mode enable <module/port>** コマンドを発行すると、aggressive モードの UDLD が有効になります。

```
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 -----
enabled undetermined
```

メッセージ間隔を変更するには、次のコマンドを発行します。

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

間隔は 7 から 90 秒の範囲で設定できます。デフォルトは 15 秒です。

IOS UDLD の設定の詳細は、次のドキュメントを参照してください。

- Cisco IOS システム ソフトウェアが稼働している Catalyst 6500/6000 スイッチの場合は、「[UDLD の設定](#)」を参照してください。
- Catalyst 2900XL/3500XL スイッチの場合は、「[スイッチ ポートの設定](#)」の「[単方向リンク検出の設定](#)」のセクションを参照してください。
- Catalyst 2940 スイッチの場合は、「[UDLD の設定](#)」を参照してください。
- Catalyst 2950/2955 スイッチの場合は、「[UDLD の設定](#)」を参照してください。
- Catalyst 2970 スイッチの場合は、「[UDLD の設定](#)」を参照してください。
- Catalyst 3550 スイッチの場合は、「[UDLD の設定](#)」を参照してください。
- Catalyst 3560 スイッチの場合は、「[UDLD の設定](#)」を参照してください。
- Cisco IOS が稼働している Catalyst 4500/4000 の場合は、「[UDLD の設定](#)」を参照してください。

[関連情報](#)

- [LAN スイッチングに関するサポート ページ](#)
- [Catalyst LAN スイッチおよび ATM スイッチの製品サポート](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)