スパニングツリー プロトコル ルート ガード機能拡張

目次

概要

このドキュメントでは、Spanning-Tree Protocol（STP; スパンニング ツリー プロトコル）ルート ガード機能について説明します。 この機能は、Cisco によって開発された STP の機能拡張の 1 つです。 この機能は、交換回線ネットワークの信頼性、管理性、およびセキュリティを強化するものです。

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。

機能説明

標準の STP には、ネットワーク管理者が交換レイヤ 2 (L2) ネットワークのトポロジを確実に指定する方法がありません。 トポロジを指定する手段は、共用の管理制御のあるネットワークでは特に重要になる可能性があります。これは、異なる管理エンティティや企業が、1 つの交換回線ネットワークを管理している場合などです。

交換回線ネットワークの転送トポロジは、算出されるものです。 この計算は、他にもあるパラメータの中から、ルート ブリッジの位置に基づくものです。 ネットワークでは任意のスイッチがルート ブリッジになることができます。 ただし、より最適化された転送トポロジでは、ルート ブリッジはある特別な事前定義された位置に配置されます。 標準的な STP では、より低いブリッジ ID を持つネットワーク内の任意のブリッジにルート ブリッジの役割が割り当てられます。 管理者はルート ブリッジの位置を指定できません。

注: 管理者は、ルート ブリッジの位置を確定させるために、ルート ブリッジのプライオリティを 0 に設定できます。 ただし、プライオリティ 0 と、より低い MAC アドレスを持つブリッジに対する保証はありません。

ルート ガード機能により、ネットワーク内でのルート ブリッジの配置を指定する手段が提供されます。

ルート ガードにより、ルート ガードがイネーブルであるポートが確実に指定ポートになります。通常、ルート ブリッジ ポートは、そのルート ブリッジの 2 つ以上のポートが相互に接続されていない限り、すべて指定ポートです。 ルート ガードがイネーブルにされたポート上で、ブリッジが上位の STP Bridge Port Data Unit (BPDU; ブリッジ ポート データ ユニット) を受信した場合、ルート ガードはこのポートを root-inconsistent の STP ステートに移行させます。 この root-inconsistent ステートは、事実上はリスニング ステートと同等になります。 このポートからは、トラフィックは転送されません。 このようにして、ルート ガードではルート ブリッジの位置が指定されます。

このセクションの例では、不正なルート ブリッジがネットワーク上で問題を引き起こすしくみ、およびルート ガードがこれを防止するしくみを示します。

図 1 では、スイッチ A と B はネットワークのコアを構成し、A は VLAN のルート ブリッジです。 スイッチ C はアクセス層スイッチです。 B と C の間のリンクでは C 側がブロッキング状態です。 矢印は STP BPDU の流れを示しています。

図 1

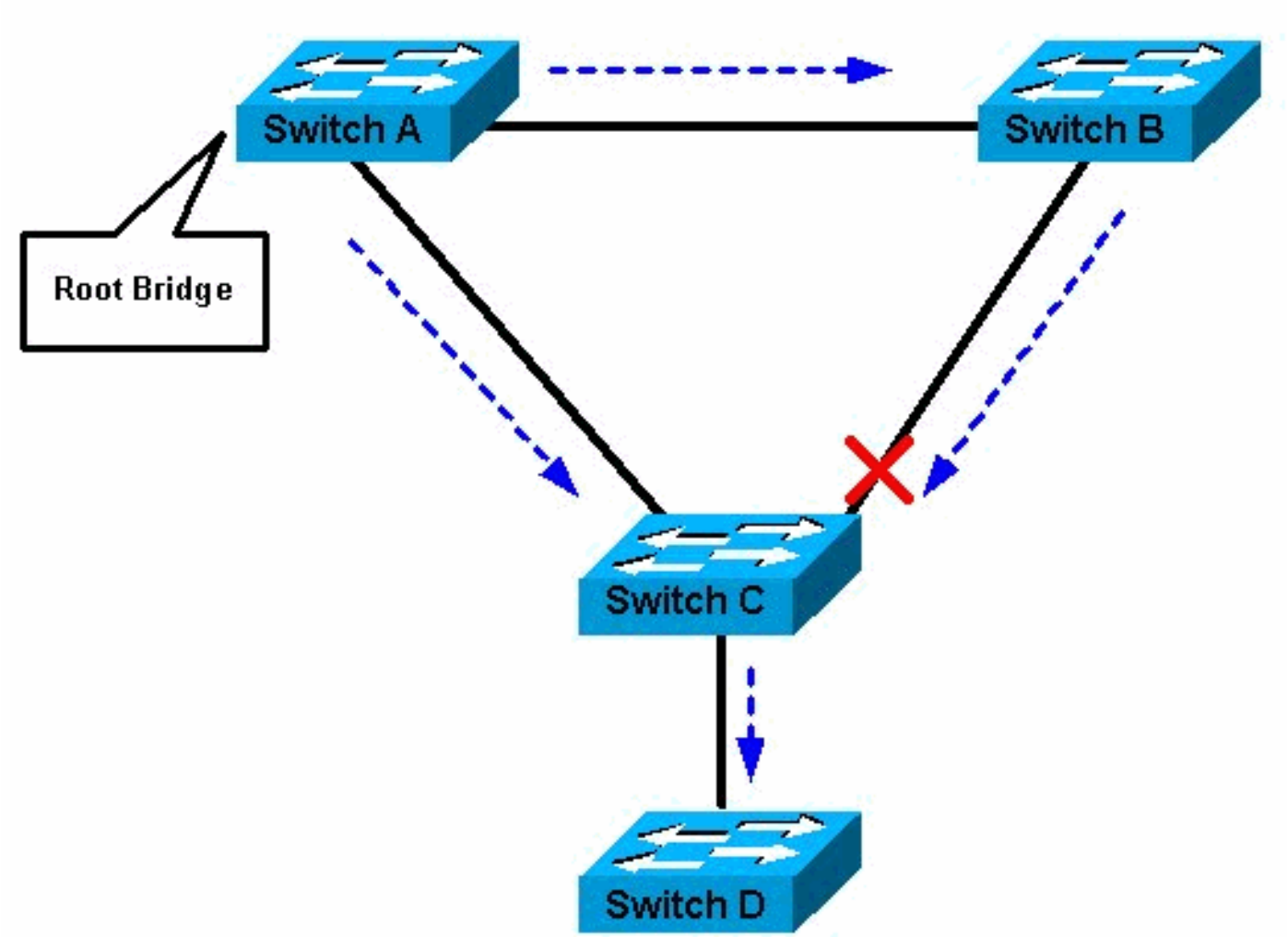
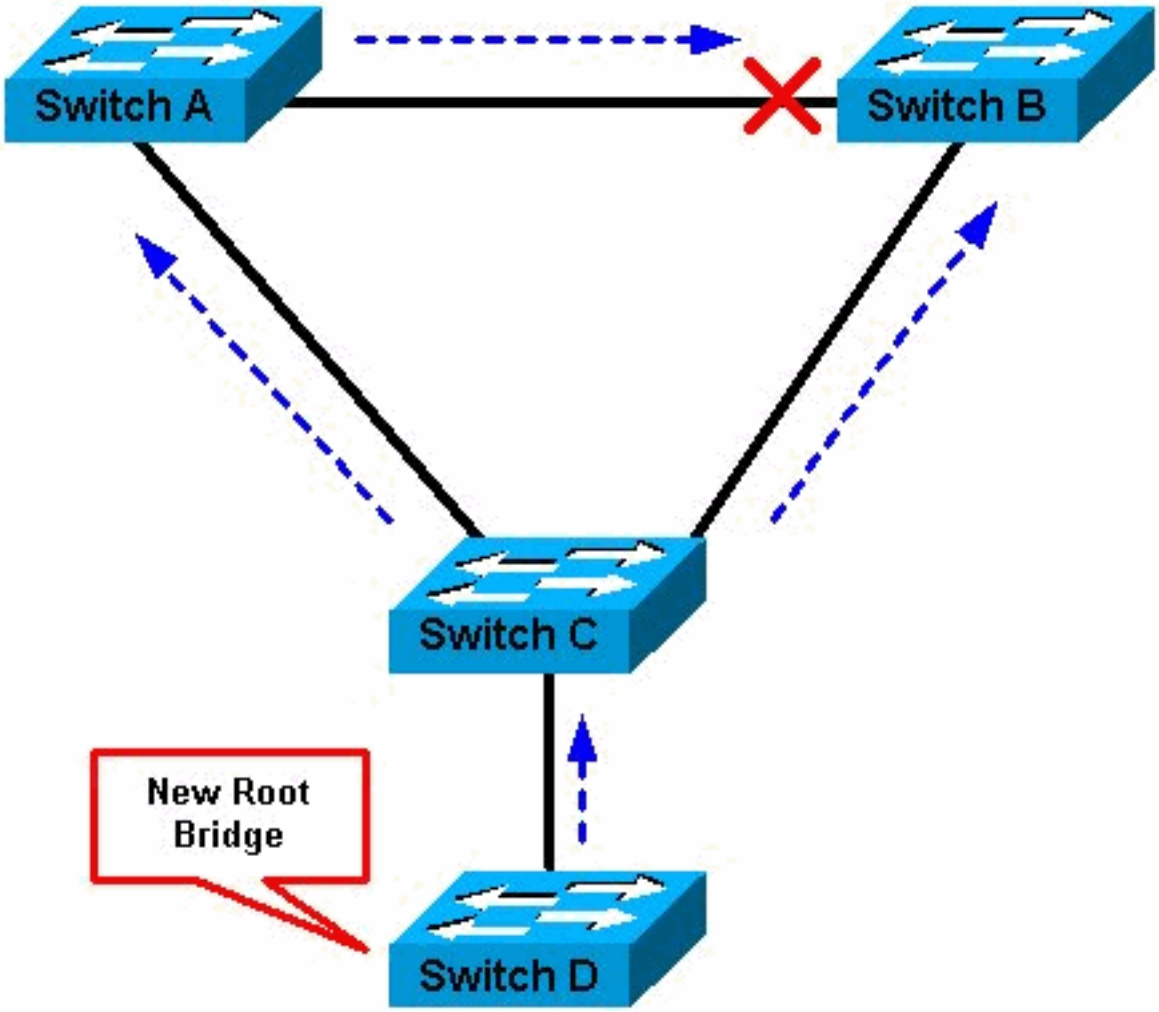


図 2 で、デバイス D は STP に参加します。 たとえば、ソフトウェア ベースのブリッジ アプリケーションが、PC 上や、お客様によってサービス プロバイダーのネットワークに接続されているその他のスイッチ上で起動されます。 ブリッジ D のプライオリティが 0 またはルート ブリッジのプライオリティよりも低い値の場合、デバイス D がこの VLAN のルート ブリッジとして選択されます。 デバイス A と B の間のリンクが 1 ギガビットであり、A と C および B と C の間のリンクが 100 Mbps である場合、D をルートとして選択すると、2 つのコア スイッチを接続しているギガビット イーサネット リンクでブロックが働きます。 このブロックにより、その VLAN 内にあるすべてのデータが、アクセス レイヤを横断する 100 Mbps リンクを介して流れるようになります。 このリンクが対応できるよりも多くのデータが、その VLAN のコアを経由して流れた場合、一部のフレームの廃棄が発生します。 フレームの廃棄は、パフォーマンスの損失や接続停止に至ります。

図 2



ネットワークは、ルート ガード機能により、このような問題から保護されます。

ルート ガードの設定は、ポートごとに行われます。 ルート ガードでは、ポートが STP ルート ポートになることが許可されないため、ポートは常に STP-designated になっています。 より上位の BPDU がこのポートに到達しても、ルート ガードではこの BPDU は考慮されず、新しい STP ルートは選択されません。 その代わりに、ルート ガードにより、そのポートは root-inconsistent の STP ステートにされます。 ルート ブリッジが出現してはならないポートではすべて、ルート ガードをイネーブルにする必要があります。 また、STP ルートを配置可能なネットワークの部分の周囲に、境界を設定することができます。

図 2 では、スイッチ D に接続するスイッチ C ポートで、ルート ガードをイネーブルにします。

スイッチが上位の BPDU を受信すると、図 2 のスイッチ C では、スイッチ D に接続しているポートがブロックされます。 ルート ガードにより、そのポートは root-inconsistent の STP ステートにされます。 このステートでは、ポートを通過するトラフィックはありません。 デバイス D が上位の BPDU の送信を停止すると、ポートでのブロックは解除されます。 STP により、このポートは listening 状態から learning 状態に移行し、最終的には forwarding 状態に移行します。 リカバリは自動です; 人間の介入は必要ではないです。

ルート ガードによりポートがブロックされると、次のメッセージが表示されます。

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
```

```
Moved to root-inconsistent state
```

アベイラビリティ

ルート ガードは、ソフトウェア バージョン 6.1.1 以降の Catalysts 29xx、4500/4000、5500/5000、および 6500/6000 向け Catalyst OS (CatOS) で使用可能です。 Cisco IOS(R) システム ソフトウェアが稼働する Catalyst 6500/6000 に関しては、この機能は Cisco IOS ソフトウェア リリース 12.0(7)XE で最初に導入されました。 Cisco IOS システム ソフトウェアが稼働する Catalyst 4500/4000 に関しては、この機能はすべてのリリースで使用可能です。

Catalyst 2900XL および 3500XL スイッチに関しては、ルート ガードは Cisco IOS ソフトウェア リリース 12.0(5)XU 以降で使用可能です。 Catalyst 2950 シリーズ スイッチでは、Cisco IOS ソフトウェア リリース 12.0(5.2)WC(1) 以降でルート ガード機能がサポートされています。 Catalyst 3550 シリーズ スイッチでは、Cisco IOS ソフトウェア リリース 12.1(4)EA1 以降でルート ガード機能がサポートされています。

設定

CatOS の設定

ルート ガードの設定は、ポートごとに行われます。 CatOS が稼働する Catalyst スイッチでは、次のようにルート ガードを設定します。

```
vega> (enable) set spantree guard root 1/1 Rootguard on port 1/1 is enabled. Warning!! Enabling rootguard may result in a topology change. vega> (enable)
```

ルート ガードが設定されているかどうかを確認するには、次のコマンドを発行します。

```
vega> (enable) show spantree guard Port VLAN Port-State Guard Type ----------------------- ---------- ---------- 1/1 1 forwarding root 1/2 1 not-connected none 3/1 1 not-connected none 3/2 1 not-connected none 3/3 1 not-connected none 3/4 1 not-connected none 5/1 1 forwarding none 5/25 1 not-connected none 15/1 1 forwarding none vega> (enable)
```

Catalyst 6500/6000 および Catalyst 4500/4000 での Cisco IOS ソフトウェアの設定

Cisco IOS システム ソフトウェアが稼働している Catalyst 6500/6000 スイッチまたは Catalyst 4500/4000 スイッチでは、STP ルート ガードを設定するために次のコマンド セットを発行します。

```
Cat-IOS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Cat-IOS#(config)# interface fastethernet 3/1 Cat-IOS#(config-if)# spanning-tree guard root
```

注: Cisco IOS システム ソフトウェアが稼働する Catalyst 6500/6000 用の Cisco IOS ソフトウェア リリース 12.1(3a)E3 では、このコマンドは spanning-tree rootguard から spanning-tree guard root に変更されています。 Cisco IOS システム ソフトウェアが稼働する Catalyst 4500/4000 では、すべてのリリースで spanning-tree guard root コマンドを使用します。

Catalyst 2900XL/3500XL、2950、および 3550 での Cisco IOS ソフトウェアの設定

Catalyst 2900XL、3500XL、2950、および 3550 では、次の例のように、ルート ガードを搭載したスイッチをインターフェイス設定モードで設定します。

```
Hinda# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hinda(config)# interface fastethernet 0/8 Hinda(config-if)# spanning-tree rootguard Hinda(config-if)# ^Z *Mar 15 20:15:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard enabled on
```

```
port FastEthernet0/8 VLAN 1.^Z Hinda#
```

STP BPDU ガードと STP ルートガードの相違点

BPDU ガードとルート ガードは類似していますが、その影響は異なります。 BPDU ガードは、ポートで PortFast がイネーブルされている場合は BPDU 受信時にポートをディセーブルにします。 このディセーブル化により、該当ポートの背後にあるデバイスは、事実上 STP への参加を拒否されます。 errdisable ステートになっているポートは、手動で再度イネーブルにするか、errdisable-timeout を設定する必要があります。

ルート ガードは、デバイスがルートになろうとしない限り、デバイスが STP に関与するのを許可します。 ルート ガードによりポートがブロックされた場合、その後の回復は自動的に行われます。 回復は、問題のあるデバイスが上位 BPDU を送信しなくなると同時に自動的に行われます。

BPDU ガードの詳細については、次のドキュメントを参照してください。

- スパニング ツリー PortFast BPDU ガード機能拡張

ルート ガードは 2 つのルート問題の解決に役立つか

ネットワーク内の 2 つのブリッジ間で、単方向リンク障害が発生することがあります。 この障害により、1 つのブリッジがルート ブリッジから BPDU を受信しなくなります。 このような障害が発生した場合、ルート スイッチでは相手側のスイッチから送信されたフレームが受信されますが、相手側のスイッチでは、ルート スイッチから送信された BPDU が受信されません。 これが STP ループの原因となる可能性があります。 相手側のスイッチではルートからの BPDU が受信されないため、自身がルートであると認識して BPDU を送信し始めます。

本当のルート ブリッジで BPDU の受信が始まると、これらは上位 BPDU ではないため、ルートでは BPDU が廃棄されます。 ルート ブリッジは変更されません。 したがって、ルート ガードはこの問題の解決には役立ちません。 UniDirectional Link Detection（UDLD; 単方向リンク検出）機能とループ ガード機能がこの問題に対応します。

STP 障害のシナリオおよび障害のトラブルシューティング方法に関する詳細は、次のドキュメントを参照してください。

- スパニング ツリー プロトコルの問題点と設計上の考慮事項

関連情報

- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- ループ ガードと BPDU スキュー検出機能を使用したスパニング ツリー プロトコルの拡張
- テクニカルサポートとドキュメント - Cisco Systems