ルートガードによるスパニングツリープロトコル(STP)の強化

内容

はじめに

このドキュメントでは、スイッチド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改善されたSTPルートガード機能について説明します。

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

このドキュメントの内容は、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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『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保するために、ルートブリッジプライオリティを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。

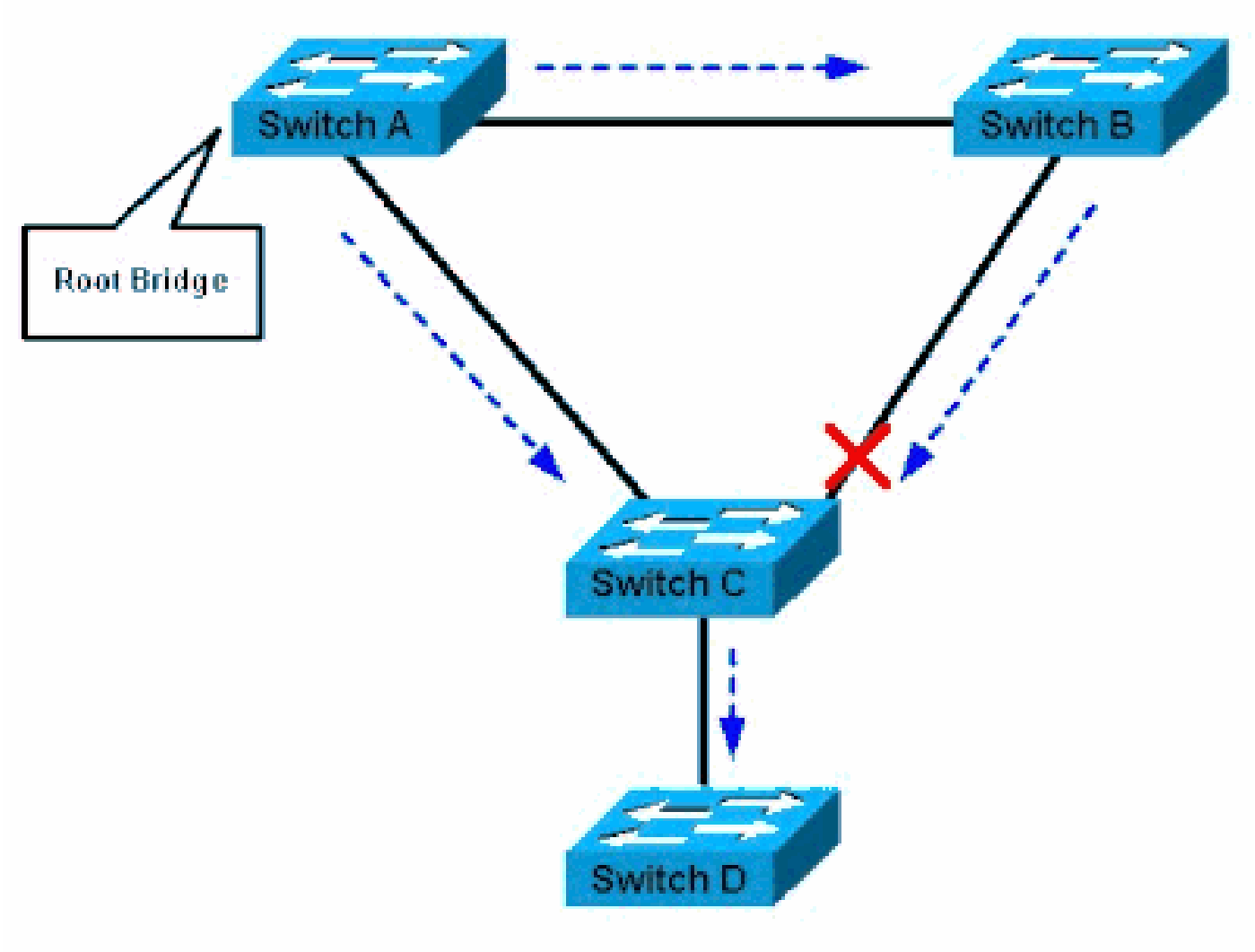
ルート ガード機能には、ネットワークにルート ブリッジを強制的に配置する方法があります。

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 ブリッジの 2 つ以上のポートが互いに接続されている場合を除き、ルート ブリッジのポートはすべて指定ポートになります。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。root-inconsistent ステートは、実質的にはリスニング ステートと同じです。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の間のリンクは、C側でブロックされています。矢印は STP BPDU の流れを示しています。

画像 1

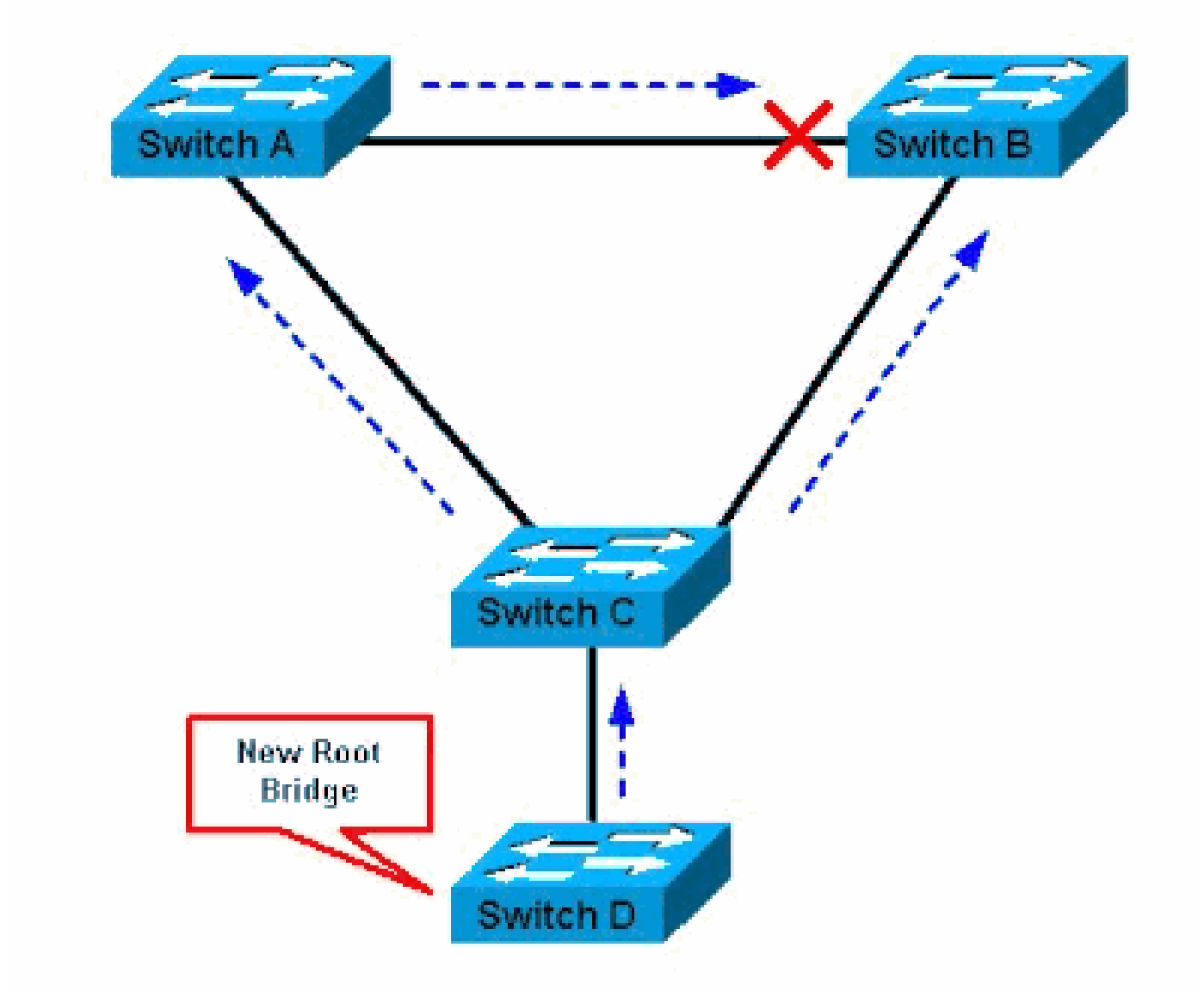


スイッチAはルートブリッジである

図2では、デバイスDがSTPに参加し始めています。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は、サービスプロバイダーのネットワークに接続しているPCやその他のスイッチで起動されます。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フローがそのVLANのコアを通過すると、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。

画像 2



スイッチDが新しいルートブリッジになる

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。ルートブリッジが表示されないすべてのポートでルートガードを有効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。

InImage 2で、スイッチDに接続するスイッチCポートのルートガードを有効にします。

スイッチが上位のBPDUを受信すると、スイッチCのinImage 2で、スイッチDに接続す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

自動的に行われるため、手動による操作は必要ありません。

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、Cisco IOS®システムソフトウェアが稼働するCatalyst 6500/6000で使用できます。この機能は、Cisco IOSソフトウェアリリース12.0(7)XEで初めて導入されました。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。

この機能は、新しいCisco Catalystシリーズスイッチでも使用できます。

コンフィギュレーション

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。

<#root>

```
Switch#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
!
Switch#(config)#

interface fastethernet 3/1

Switch#(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、このコマンドが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。

<#root>

```
Switch#

configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#

interface fastethernet 0/8

Switch(config-if)#

spanning-tree rootguard

Switch(config-if)#

^Z

*Mar 15 20:15:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard enabled on
port FastEthernet0/8 VLAN 1.

Switch#
```

STP BPDUガードとSTPルートガードの違い

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。リカバリは、デバイスが上位BPDUを送信しなくなるとすぐに行われます。

BPDUガードの詳細については、『スパニングツリーPortFast BPDUガード機能拡張』を参照してください。

ルートガードは2つのルートの問題に役立つか

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障害のシナリオとトラブルシューティング方法の詳細については、『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』を参照してください。

関連情報

- UDLD プロトコル機能の理解と設定
- Cisco IOS プラットフォームでの Errdisable ポート状態の回復
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。