

# Amélioration du protocole STP (Spanning Tree Protocol) avec Root Guard

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Description de la fonctionnalité](#)

[Disponibilité](#)

[Configuration](#)

[Configuration du logiciel Cisco IOS pour Catalyst 6500/6000 et Catalyst 4500/4000](#)

[Configuration du logiciel Cisco IOS pour Catalyst 2900XL/3500XL, 2950 et 3550](#)

[Quelle est la différence entre STP BPDU Guard et STP Root Guard ?](#)

[La fonction Root Guard aide-t-elle à résoudre le problème des deux racines ?](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit les fonctionnalités améliorées de protection de la racine STP qui améliorent la fiabilité, la facilité de gestion et la sécurité du réseau commuté.

## Conditions préalables

### Exigences

Aucune exigence spécifique n'est associée à ce document.

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

## Description de la fonctionnalité

La norme STP ne fournit aucun moyen pour que l'administrateur réseau mette en œuvre en toute sécurité la topologie du réseau commuté de couche 2 (L2). Un moyen d'appliquer la topologie peut être particulièrement important dans les réseaux avec un contrôle d'administration partagé, où des entités administratives ou sociétés différentes contrôlent un réseau commuté.

La topologie de transfert du réseau commuté est calculée. Le calcul est basé sur la position du pont racine, entre autres paramètres. Tout commutateur peut être le pont racine dans un réseau. Mais une topologie de transfert plus optimale place le pont racine à un emplacement prédéterminé spécifique. Avec la norme STP, tout pont dans le réseau avec un ID de pont inférieur joue le rôle de pont racine. L'administrateur ne peut pas appliquer la position du pont racine.

---

 Remarque : l'administrateur peut définir la priorité du pont racine sur 0 afin de sécuriser la position du pont racine. Mais il n'y a aucune garantie contre un pont une priorité de 0 et une adresse MAC inférieure.

---

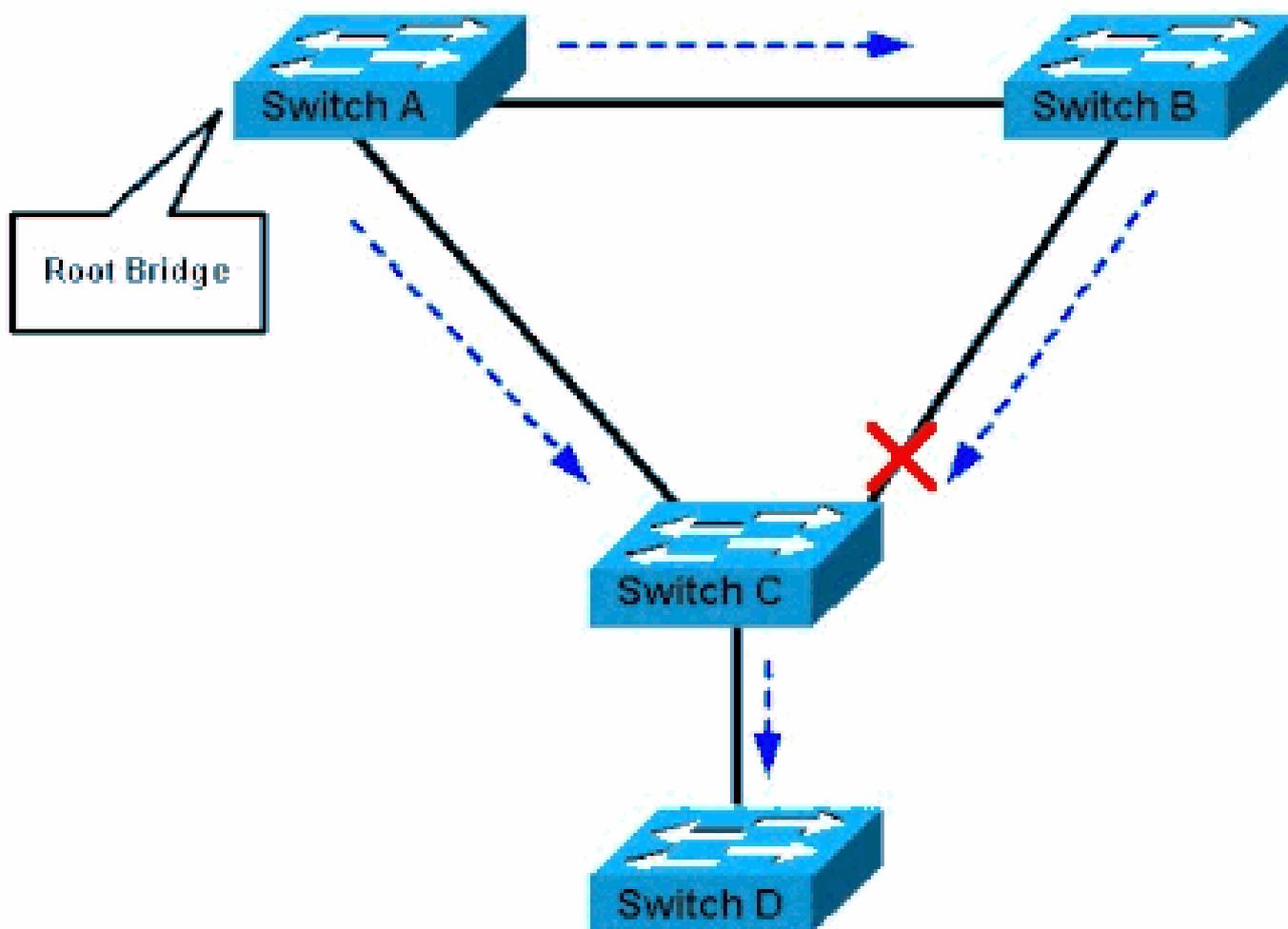
La fonctionnalité de protection de la racine fournit un moyen d'imposer le placement du pont racine dans le réseau.

Root Guard s'assure que le port sur lequel cette fonctionnalité est activée est le port désigné. Normalement, les ports du pont racine sont tous des ports désignés, à moins que deux ou plusieurs des ports du pont racine soient connectés ensemble. Si le pont reçoit des BPDU STP supérieures sur un port où Root Guard est activée, cette fonctionnalité place ce port à l'état de racine STP incohérente. Cet état contradictoire est effectivement égal à un état d'écoute. Aucun trafic n'est acheminé sur ce port. De cette façon, le dispositif de protection de la racine impose la position du pont racine.

L'exemple de cette section démontre comment un pont racine non autorisé peut poser des problèmes sur le réseau et comment Root Guard peut aider.

Dans l'image 1, les commutateurs A et B constituent le cœur du réseau et A est le pont racine d'un VLAN. Le commutateur C est un commutateur de la couche d'accès. La liaison entre B et C est bloquée du côté C. Les flèches montrent le flux des BPDU STP.

Image 1

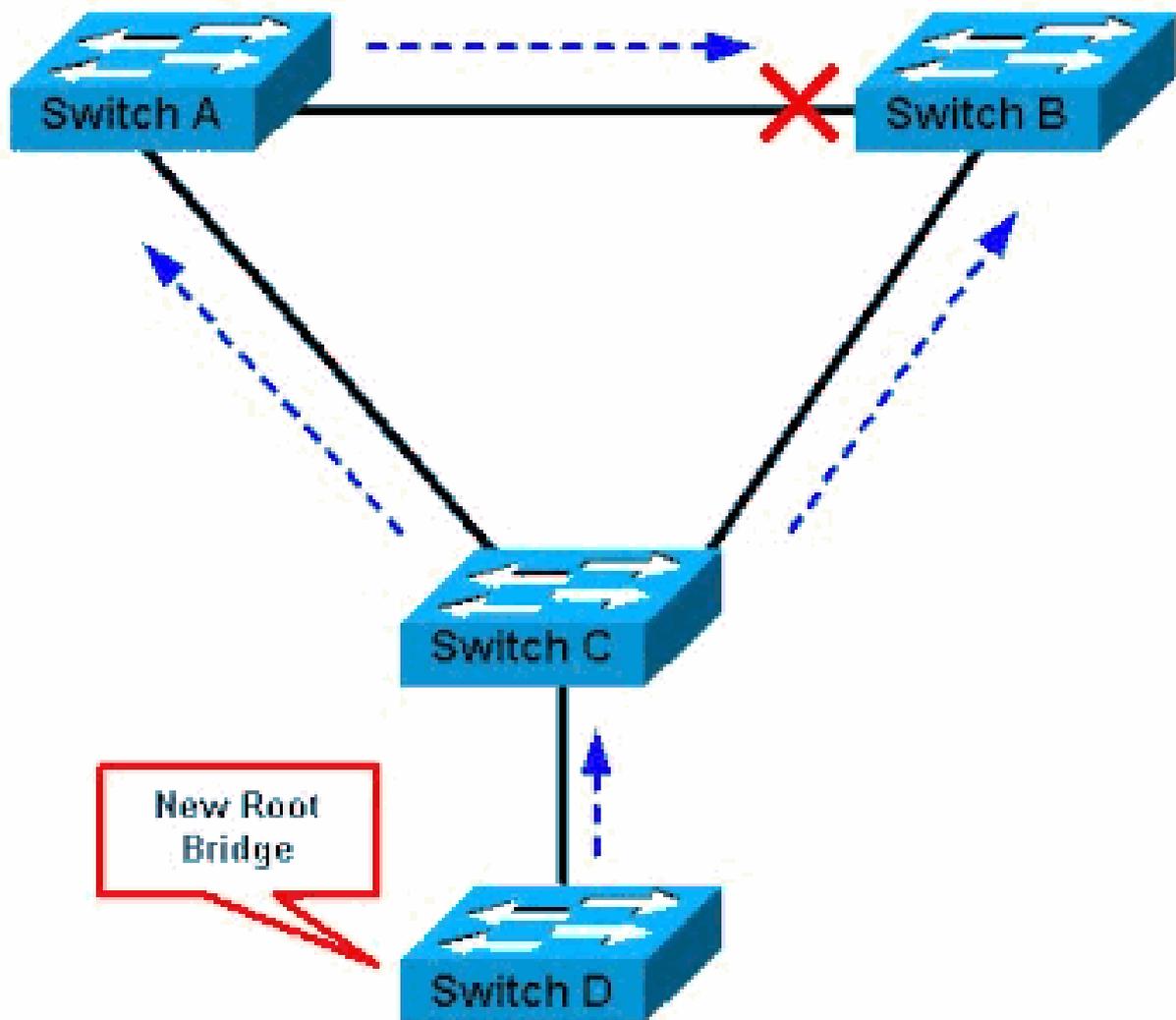


Le commutateur A est le pont racine

Dans l'image 2, le périphérique D commence à participer au protocole STP. Par exemple, des applications de pontage logicielles sont lancées sur des PC ou d'autres commutateurs que vous connectez à un réseau de fournisseur de services. Si la priorité du pont D est 0 ou toute valeur inférieure à la priorité du pont racine, le périphérique D est élu comme pont racine pour ce VLAN. Si la liaison entre le périphérique A et B est de 1 gigabit et les liaisons entre A et C ainsi que B et C sont de 100 Mbits/s, l'élection de D comme racine provoque le blocage de la liaison Gigabit Ethernet qui connecte les deux commutateurs principaux.

Ce blocage a pour conséquence que toutes les données dans ce VLAN circulent par l'intermédiaire d'une liaison 100 Mbits/s à travers la couche d'accès. Si plus de données circulent via le coeur dans ce VLAN que ce lien ne peut en accepter, la perte de certaines trames se produit. Cette perte de trames génère une perte de performance ou une panne de connectivité.

Image 2



Le commutateur D est un nouveau pont racine

La fonctionnalité Root Guard protège le réseau contre de tels problèmes.

La configuration de Root Guard se fait sur une base par port. Root Guard ne permet pas au port de devenir un port racine STP, ainsi le port est toujours désigné STP. Si une meilleure BPDU arrive sur ce port, Root Guard ne prend pas en compte l'unité BPDU et élit une nouvelle racine STP. Au lieu de cela, Root Guard met le port dans l'état de racine STP incohérente. Vous devez activer la protection de racine sur tous les ports où le pont racine ne doit pas apparaître. Dans un sens, vous pouvez configurer un périmètre autour de la partie du réseau dans laquelle la racine STP peut être située.

[Dans l'image 2](#), activez la protection de la racine sur le port du commutateur C qui se connecte au commutateur D.

Le commutateur C [dans l'image 2](#) bloque le port qui se connecte au commutateur D, après que le commutateur a reçu une BPDU supérieure. Root Guard met le port dans l'état de racine STP incohérente. Aucun trafic ne passe par le port dans cet état. Après que le périphérique D cesse d'envoyer des BPDUs supérieures, le port est de nouveau débloqué. Par l'intermédiaire de STP, le

port va de l'état d'écoute à l'état d'apprentissage, et par la suite à l'état d'acheminement. La récupération est automatique ; aucune intervention humaine n'est nécessaire.

Ce message apparaît après que Root Guard bloque un port :

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

## Disponibilité

Root Guard est disponible dans Catalyst 6500/6000 qui exécute le logiciel système Cisco IOS®. Cette fonctionnalité a été introduite pour la première fois dans le logiciel Cisco IOS Version 12.0(7)XE. Pour Catalyst 4500/4000, qui exécute la plate-forme logicielle Cisco IOS, cette fonctionnalité est disponible dans toutes les versions.

Pour les commutateurs Catalyst 2900XL et 3500XL, Root Guard est disponible dans le logiciel Cisco IOS Version 12.0(5)XU et ultérieure. Les commutateurs de la gamme Catalyst 2950 prennent en charge la fonctionnalité Root Guard dans le logiciel Cisco IOS Version 12.0(5.2)WC(1) et ultérieure. Les commutateurs de la gamme Catalyst 3550 prennent en charge la fonctionnalité Root Guard dans le logiciel Cisco IOS Version 12.1(4)EA1 et ultérieure.

Cette fonctionnalité est également disponible sur les commutateurs Cisco Catalyst plus récents.

## Configuration

### Configuration du logiciel Cisco IOS pour Catalyst 6500/6000 et Catalyst 4500/4000

Sur les commutateurs Catalyst 6500/6000 ou Catalyst 4500/4000 qui exécutent la plate-forme logicielle Cisco IOS, émettez cet ensemble de commandes afin de configurer Root Guard du protocole STP :

```
<#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  
  
!
```

---

 Remarque : la version 12.1(3a)E3 du logiciel Cisco IOS pour Catalyst 6500/6000 qui exécute le logiciel système Cisco IOS a modifié cette commande de spanning-tree rootguard à spanning-tree guard root . Catalyst 4500/4000, qui exécute la plate-forme logicielle Cisco IOS, utilise la commande spanning-tree guard root dans toutes les versions.

---

## Configuration du logiciel Cisco IOS pour Catalyst 2900XL/3500XL, 2950 et 3550

Sur Catalyst 2900XL, 3500XL, 2950 et 3550, configurez les commutateurs avec Root Guard en mode de configuration de l'interface, comme indiqué dans cet exemple :

```
<#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#
```

## Quelle est la différence entre STP BPDU Guard et STP Root Guard ?

BPDU Guard et Root Guard sont semblables, mais leur incidence est différente. BPDU Guard désactive le port à la réception des BPDU si PortFast est activé sur le port. La désactivation refuse effectivement que les périphériques derrière de tels ports participent à STP. Vous devez manuellement réactiver le port qui est placé dans l'état errdisable ou configurer errdisable-timeout.

Root Guard permet au périphérique de participer à STP tant qu'il n'essaye pas de devenir la racine. Si Root Guard bloque le port, la reprise ultérieure est automatique. La récupération se produit dès que le périphérique déviant cesse d'envoyer des unités BPDU supérieures.

Pour plus d'informations sur la protection BPDU, consultez [Amélioration de la protection BPDU PortFast du Spanning Tree](#).

## La fonction Root Guard aide-t-elle à résoudre le problème des deux racines ?

Il peut y avoir une défaillance de liaison unidirectionnelle entre deux ponts dans un réseau. En raison de la panne, un pont ne reçoit pas les unités BPDU du pont racine. Avec une telle panne, le commutateur racine reçoit les trames que d'autres commutateurs envoient, mais les autres commutateurs ne reçoivent pas les unités BPDU que le commutateur racine envoie. Ceci peut mener à une boucle STP. Puisque les autres commutateurs ne reçoivent aucune BPDU de la racine, ils croient qu'ils sont la racine et commencent à envoyer des unités BPDU.

Quand le pont racine réel commence à recevoir les BPDU, la racine les rejette parce qu'elles ne sont pas supérieures. Le pont racine ne change pas. Par conséquent, Root Guard n'aide pas à résoudre ce problème. Les fonctionnalités UniDirectional Link Detection (UDLD) et la protection contre les boucles résolvent ce problème.

Pour plus d'informations sur les scénarios d'échec STP et la façon de les dépanner, consultez [Problèmes de protocole Spanning Tree et Considérations de conception connexes](#).

### Informations connexes

- [Comprendre et configurer la fonctionnalité de protocole UDLD](#)
- [Récupérer l'état du port Errdisable sur les plateformes Cisco IOS](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.