Amélioration de la protection de la racine du protocole STP (Spanning Tree Protocol)

Contenu

Introduction

Ce document explique la fonctionnalité Root Guard du protocole STP (Spanning Tree Protocol). Cette fonctionnalité est l'une des améliorations de STP créée par Cisco. Elle améliore la fiabilité, la facilité de gestion et la sécurité du réseau commuté.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

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 à 0 afin de fixer la position du pont racine. Mais il n'y a aucune garantie contre un pont une priorité de 0 et une adresse MAC inférieure.

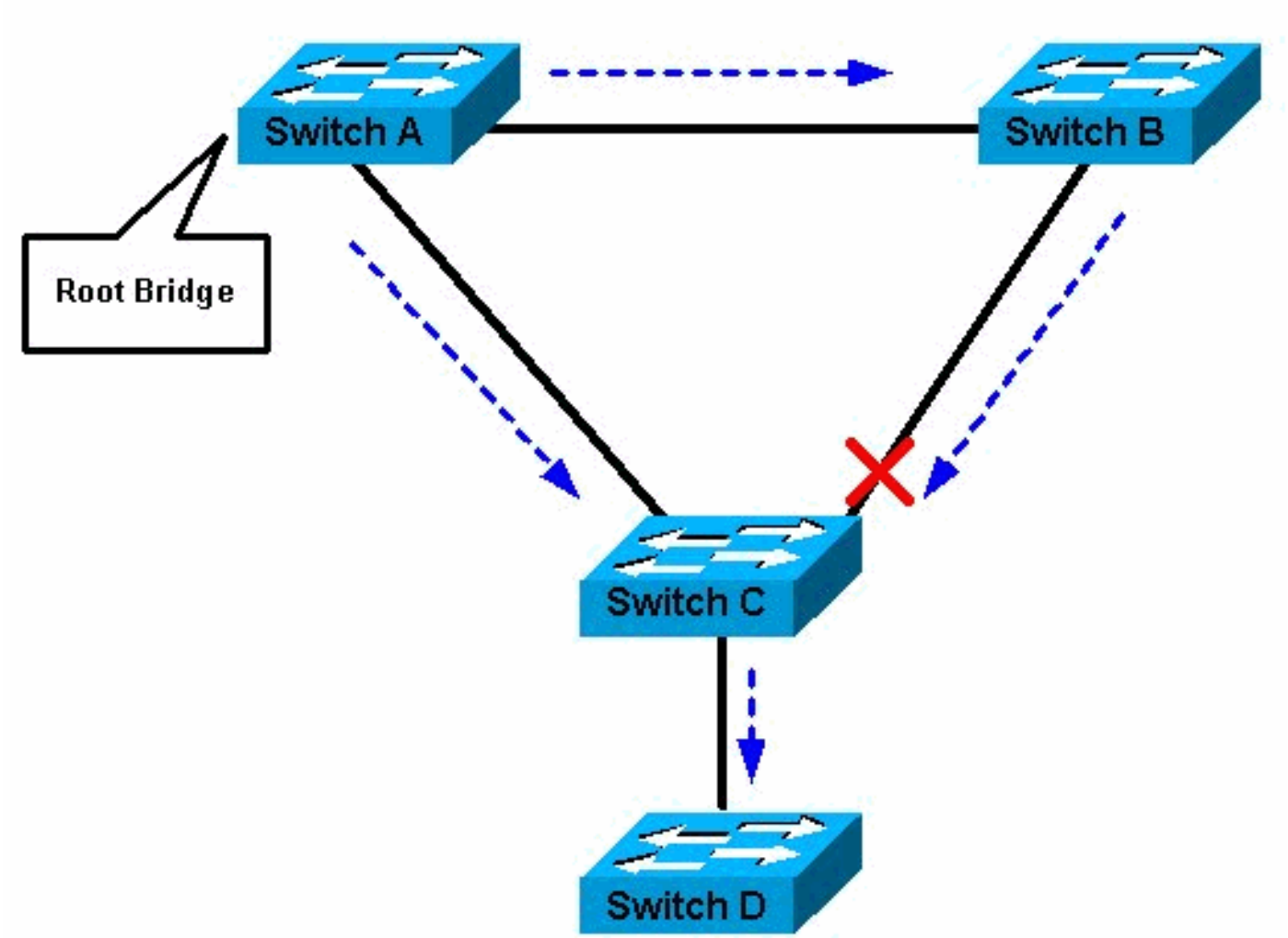
La fonctionnalité de protection de la racine fournit un moyen d'imposer le placement du pont racine dans le réseau.

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.

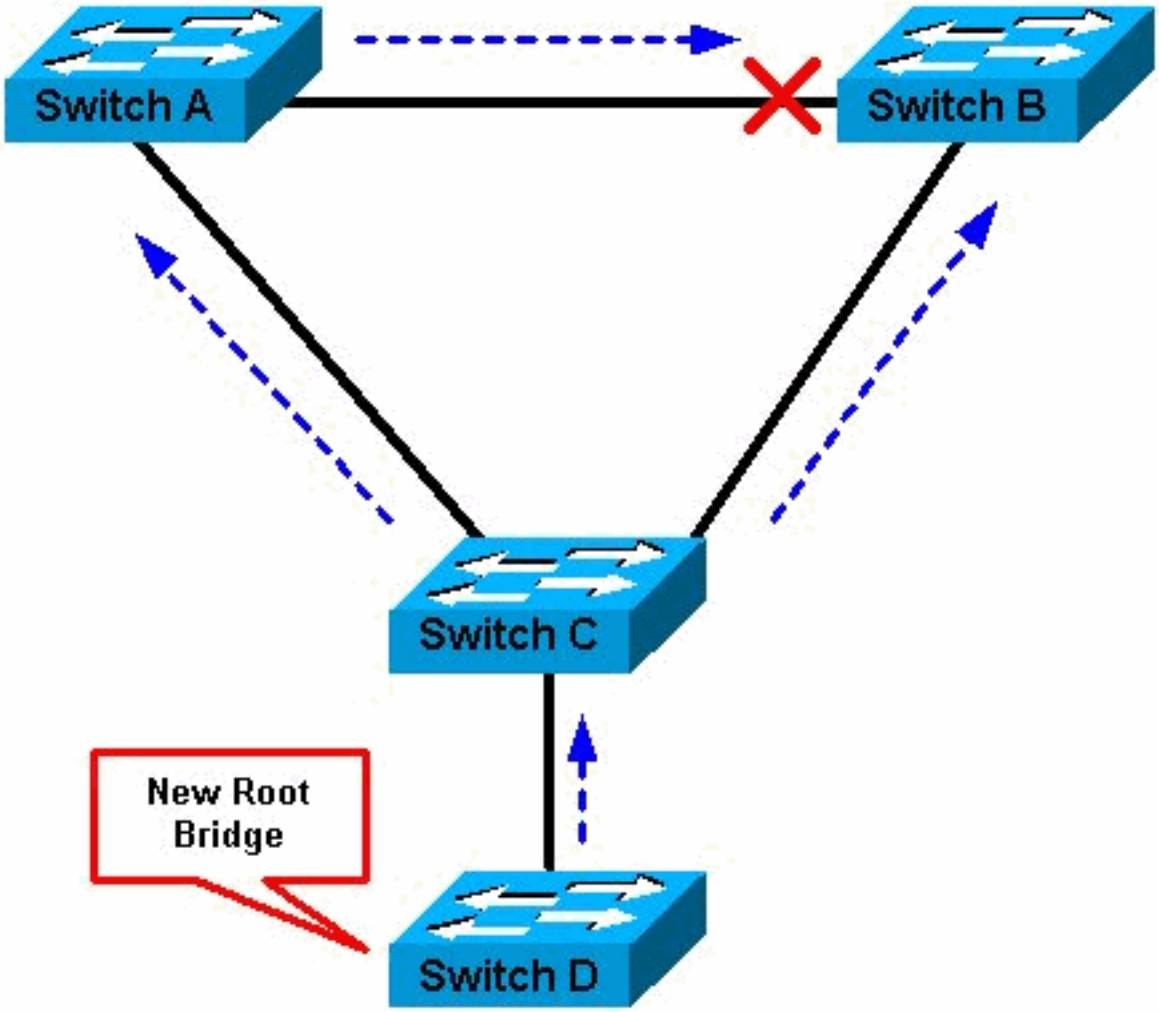
Dans la Figure 1, les commutateurs A et B forment le noyau du réseau, et A est le pont racine pour un VLAN. Le commutateur C est un commutateur de la couche d'accès. La liaison entre B et C bloque du côté de C. Les flèches montrent le flux des BPDU STP.

Figure 1



Dans la Figure 2, le périphérique D commence à participer au protocole STP. Par exemple, les applications de ponts basées sur un logiciel sont lancées sur des PC ou d'autres commutateurs qu'un client connecte à un réseau de prestataire 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 la quantité de données circulant par le noyau dans ce VLAN est supérieure à ce que peut accepter cette liaison, une perte de quelques trames se produit. Cette perte de trames génère une perte de performance ou une panne de connectivité.

Figure 2



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 Root Guard 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 la Figure 2, activez Root Guard sur le port du commutateur C qui se connecte au commutateur D.

Le commutateur C dans la Figure 2 bloque le port qui se connecte au commutateur D, après que le commutateur reçoit 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 BPDU 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 reprise 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 OS (CatOS) pour le logiciel Catalyst 29xx, 4500/4000, 5500/5000 et 6500/6000 Version 6.1.1 et ultérieure. Pour Catalyst 6500/6000 qui exécute la plate-forme logicielle 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.

Configuration

Configuration de CatOS

La configuration de Root Guard se fait sur une base par port. Sur les commutateurs Catalyst qui exécutent CatOS, configurez Root Guard de cette façon :

```
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)
```

Afin de vérifier si Root Guard est configurée, émettez cette commande :

```
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)
```

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 :

```
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
```

Remarque: Le logiciel Cisco IOS Version 12.1(3a)E3 pour Catalyst 6500/6000 qui exécute la plate-forme logicielle Cisco IOS a changé cette commande de **spanning-tree rootguard** en **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 :

```
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#
```

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

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 reprise se produit dès que l'équipement attentatoire cesse d'envoyer des BPDU supérieure.

Pour plus d'informations sur BPDU Guard, référez-vous à ce document :

- Amélioration de la protection des BPDU en PortFast pour le spanning tree

La fonctionnalité Root Guard aide-t-elle avec le problème des deux racines ?

Il peut y a 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 de panne du protocole STP et sur la façon de les résoudre, référez-vous à ce document :

- Problèmes liés au protocole STP (Spanning Tree Protocol) et considérations de conception

Informations connexes

- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Améliorations du protocole STP (Spanning Tree Protocol) avec les fonctions de protection contre les boucles et de détection des différences de temps de propagation des BPDU
- Support et documentation techniques - Cisco Systems