Amélioration du protocole STP avec Root Guard

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Description des fonctionnalités

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 la fonctionnalité de protection de la racine du protocole STP (Spanning Tree Protocol) qui améliore la fiabilité et la facilité de gestion 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.

Description des fonctionnalités

Le protocole STP standard ne permet pas à l’administrateur réseau d’appliquer de manière sécurisée la topologie du réseau commuté de couche 2 (L2). Un moyen d’appliquer la topologie peut être particulièrement important dans les réseaux avec contrôle administratif partagé, où différentes entités administratives ou entreprises 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 d’un réseau. Mais une topologie de transfert plus optimale place le pont racine à un emplacement prédéterminé spécifique. Avec le protocole STP standard, tout pont du réseau ayant un ID de pont inférieur joue le rôle de pont racine.

Remarque : L'administrateur peut définir la priorité du pont racine sur 0 afin de sécuriser la position du pont racine. La commande spanning-tree vlan <vlan-id> {priority|root} {primary|secondary|<value>} configure la priorité de pont d'un VLAN, mais il n'y a aucune garantie contre un pont avec une priorité de 0 et une adresse MAC inférieure.

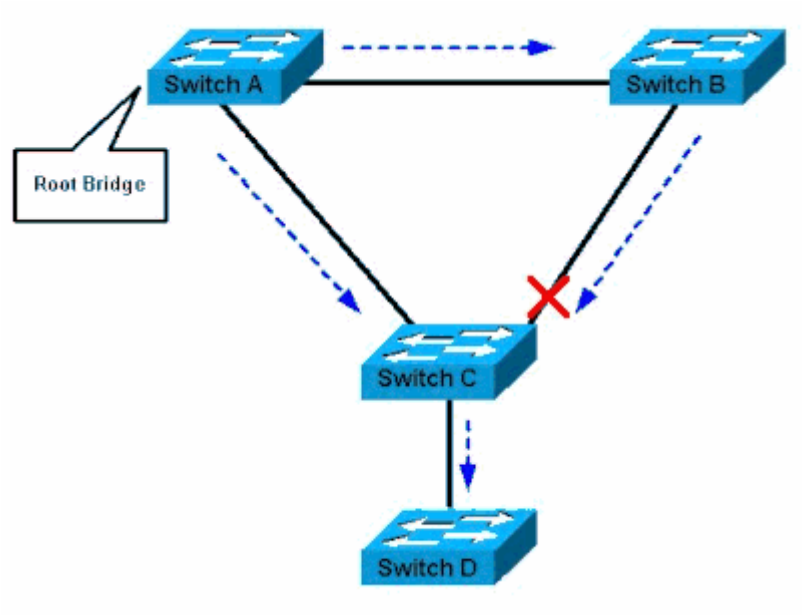
La fonction de protection de la racine permet d’imposer l’emplacement du pont racine dans le réseau.

La protection de racine garantit que le port sur lequel la protection de racine est activée est le port désigné. Normalement, les ports du pont racine sont tous des ports désignés, à moins que deux ou plusieurs ports du pont racine soient connectés ensemble. Si le pont reçoit des unités BPDU (Bridge Protocol Data Unit) STP supérieures sur un port compatible avec la protection de la racine, la protection de la racine fait passer ce port à un état STP incohérent de la racine. Cet état d'incohérence racine est effectivement égal à un état d'écoute. Aucun trafic n'est transféré via ce port. De cette manière, la protection de racine applique la position du pont racine.

L'exemple de cette section montre comment un pont racine non autorisé peut provoquer des problèmes sur le réseau et comment la protection de la racine peut aider.

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

Image 1

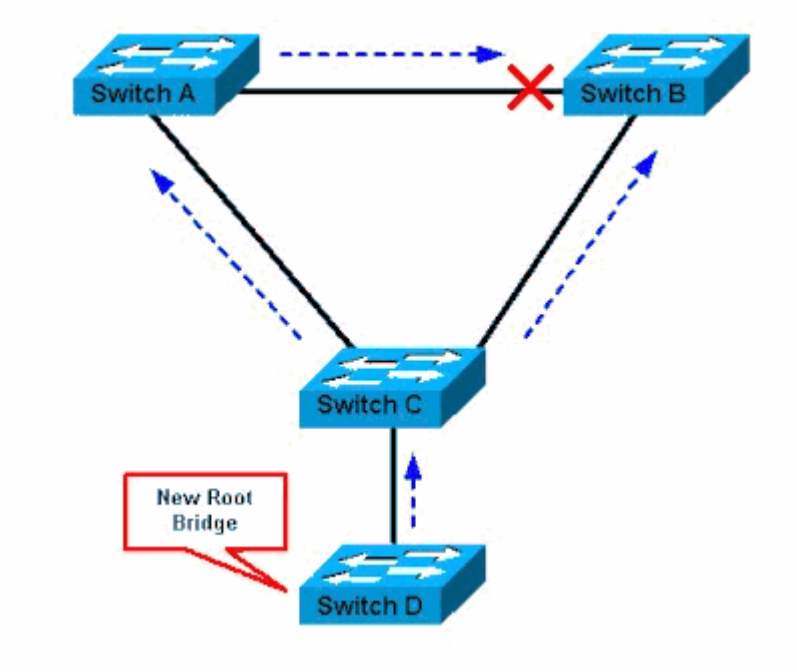


Le commutateur A est le pont racine

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 sélectionné comme pont racine pour ce VLAN. Si la liaison entre les périphériques A et B est de 1 gigabit et que les liaisons entre A et C ainsi que B et C sont de 100 Mbits/s, la sélection de D comme racine provoque le blocage de la liaison Gigabit Ethernet qui connecte les deux commutateurs principaux.

Ce bloc fait circuler toutes les données de ce VLAN via une liaison de 100 Mbits/s sur 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. La perte de trame entraîne une perte de performances ou une panne de connectivité.

Image 2



Le commutateur D est un nouveau pont racine

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

La configuration de la protection de la racine s'effectue port par port. Root Guard ne permet pas au port de devenir un port racine STP, de sorte que le port est toujours désigné STP. Si une meilleure BPDU arrive sur ce port, la protection de la racine ne prend pas en compte la BPDU et sélectionne une nouvelle racine STP. Au lieu de cela, la protection de la racine place le port dans l'état de racine STP incohérent. Vous devez activer la protection de racine sur tous les ports où le pont racine ne doit pas apparaître. D'une certaine manière, vous pouvez configurer un périmètre autour de la partie du réseau où la racine STP peut être localisée.

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, une fois que le commutateur reçoit une unité BPDU supérieure. Root Guard place le port dans l'état de racine STP incohérente. Aucun trafic ne passe par le port dans cet état. Une fois que le périphérique D a cessé d'envoyer des BPDU supérieures, le port est à nouveau débloqué. Via STP, le port passe de l'état d'écoute à l'état d'apprentissage, et passe éventuellement à l'état de transmission. La récupération est automatique ; aucune intervention humaine n'est nécessaire.

Ce message apparaît après que la protection de la racine bloque un port :

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

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 le 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, la protection de racine 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 fonction de protection de la racine 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 fonction de protection de la racine 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 le logiciel système Cisco IOS, émettez cet ensemble de commandes afin de configurer STP root guard :

<#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 : Le logiciel Cisco IOS Version 12.1(3a)E3 pour Catalyst 6500/6000 qui exécute le logiciel système Cisco IOS a modifié cette commande de spanning-tree rootguard à spanning-tree guard root . Le Catalyst 4500/4000 qui exécute le logiciel système 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 les commutateurs Catalyst 2900XL, 3500XL, 2950 et 3550, configurez les commutateurs avec la protection de racine en mode de configuration d'interface, comme le montre 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 ?

La protection BPDU et la protection de racine sont similaires, mais leur impact est différent. La protection BPDU désactive le port lors de la réception BPDU si PortFast est activé sur le port. La désactivation empêche effectivement les périphériques derrière ces ports de participer au protocole STP. Vous devez réactiver manuellement le port qui est placé dans l'état errdisable ou

configurer errdisable-timeout .

Root Guard permet au périphérique de participer au protocole STP tant qu'il n'essaie pas de devenir la racine. Si la protection de la racine bloque le port, la restauration suivante 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 défaillance, un pont ne reçoit pas les unités BPDU du pont racine. Avec une telle défaillance, le commutateur racine reçoit les trames envoyées par les autres commutateurs, mais les autres commutateurs ne reçoivent pas les BPDU envoyées par le commutateur racine. Cela peut conduire à une boucle STP. Étant donné que les autres commutateurs ne reçoivent aucune trame BPDU de la racine, ils pensent qu'ils sont la racine et commencent à envoyer des trames BPDU.

Lorsque le pont racine réel commence à recevoir des unités BPDU, la racine rejette les unités BPDU car 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 de 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.