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

Contenu

Introduction

Ce document explique la fonctionnalité PortFast Bridge Protocol Data Unit (BPDU). Cette fonctionnalité est l'une des améliorations du protocole STP (Spanning Tree Protocol) créée par Cisco. Elle améliore la fiabilité, la facilité de gestion et la sécurité du réseau de commutation.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ces versions de logiciel ont introduit la fonctionnalité STP PortFast BPDU :

- Logiciel Catalyst (CatOS) Version 5.4.1 pour les plates-formes Catalyst 4500/4000 (Supervisor Engine II), 5500/5000, 6500/6000, 2926, 2926G, 2948G et 2980G
- Logiciel Cisco IOS® Version 12.0(7)XE pour les plates-formes Catalyst 6500/6000
- Logiciel Cisco IOS Version 12.1(8a)EW pour Supervisor Engine III Catalyst 4500/4000
- Logiciel Cisco IOS Version 12.1(12c)EW pour Supervisor Engine IV Catalyst 4500/4000
- Logiciel Cisco IOS Version 12.0(5)WC5 pour la gamme Catalyst 2900XL et 3500XL
- Logiciel Cisco IOS Version 12.1(11)AX pour les commutateurs de la gamme Catalyst 3750

- Logiciel Cisco IOS Version 12.1(14)AX pour les commutateurs de la gamme Catalyst 3750
- Logiciel Cisco IOS Version 12.1(19)EA1 pour les commutateurs de la gamme Catalyst 3560
- Logiciel Cisco IOS Version 12.1(4)EA1 pour les commutateurs de la gamme Catalyst 3550
- Logiciel Cisco IOS Version 12.1(11)AX pour les commutateurs de la gamme Catalyst 2970
- Logiciel Cisco IOS Version 12.1(12c)EA1 pour les commutateurs de la gamme Catalyst 2955
- Logiciel Cisco IOS Version 12.1(6)EA2 pour les commutateurs de la gamme Catalyst 2950
- Logiciel Cisco IOS Version 12.1(11)EA1 pour les commutateurs Ethernet à longue portée (LRE) Catalyst 2950
- Logiciel Cisco IOS Version 12.1(13)AY pour les commutateurs de la gamme Catalyst 2940

Remarque: La fonctionnalité STP PortFast BPDU Guard n'est *pas* disponible pour les commutateurs de la gamme Catalyst 8500, 2948G-L3 ou 4908G-L3.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

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

STP configure la topologie engrenée dans une topologie sans boucles de type arbre. Quand la liaison sur un port de pont monte, le calcul STP se produit sur ce port. Le résultat du calcul est la transition du port en l'état de transfert ou de blocage. Le résultat dépend de la position du port dans le réseau et des paramètres STP. Ces calculs et la période de transition prennent habituellement environ 30 à 50 secondes. À ce moment-là, aucune donnée utilisateur ne passe par le port. Quelques applications utilisateur peuvent s'arrêter au cours de la période.

Afin de permettre la transition immédiate du port à l'état de transfert, activez la fonctionnalité STP PortFast. Portfast passe immédiatement le port en mode de transfert STP au moment de l'établissement de la liaison. Le port participe toujours au protocole STP. Ainsi, si le port doit faire partie de la boucle, le port passe finalement en mode de blocage de STP.

Tant que le port participe au protocole STP, un périphérique peut assumer la fonction de pont racine et affecter la topologie STP active. Pour assumer la fonction de pont racine, le périphérique serait attaché au port et exécuterait STP avec une priorité de point inférieure à celle du pont racine actuel. Si un autre périphérique assume la fonction de pont racine de cette façon, il rend le réseau suboptimal. C'est une forme simple d'attaque de déni de service (DOS) sur le réseau. L'introduction provisoire et le retrait ultérieur des périphériques STP avec une priorité de pont (0) faible provoque un recalcul STP constant.

L'amélioration de la fonctionnalité STP PortFast BPDU permet aux concepteurs de réseau de mettre en œuvre les frontières du domaine STP et de maintenir la topologie active prévisible. Les périphériques derrière les ports pour lesquels STP PortFast est activé ne peuvent pas influencer la topologie STP. À la réception des BPDU, l'opération de BPDU Guard désactive le port pour lequel PortFast est configuré. BPDU Guard passe le port à l'état errdisable, et un message apparaît sur la console. Ce message est un exemple :

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast enable port.
Disabling 2/1
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

Considérez cet exemple :

Figure 1

Le pont A a la priorité 8192 et est la racine pour le VLAN. Le pont B a la priorité 16384 et est le pont racine de secours pour le même VLAN. Les ponts sur A et B, connectés par une liaison Gigabit Ethernet, composent un noyau de réseau. Le pont C est un commutateur d'accès et a PortFast configuré sur le port connecté au périphérique D. Si les autres paramètres STP sont des paramètres par défaut, le port du pont C qui se connecte au pont B est en état de blocage de STP. Le périphérique D (PC) ne participe pas à STP. Les flèches à tiret indiquent le flux des BPDU de STP.

Figure 2

Dans la Figure 2, le périphérique D a démarré pour participer au STP. Par exemple, une application de pont basée sur Linux est lancée sur un PC. Si la priorité du pont du logiciel est 0 ou n'importe quelle valeur en dessous de la priorité du pont racine, le pont du logiciel assume la fonction de pont racine. La liaison Gigabit Ethernet qui connecte les deux commutateurs principaux passe en mode de blocage. La transition a pour conséquence que toutes les données dans ce VLAN circulent par la liaison 100 Mbps. Si la quantité de données circulant par le noyau dans le VLAN est supérieure à ce que peut accepter la liaison, une perte de trames se produit. La perte de trames génère une panne de connectivité.

La fonctionnalité STP PortFast BPDU Guard empêche une telle situation. La fonctionnalité désactive le port dès que le pont C reçoit STP BPDU du périphérique D.

Configuration

Vous pouvez activer ou désactiver la fonctionnalité STP PortFast BPDU Guard de façon globale, ce qui affecte tous les ports configurés en PortFast. Par défaut, la fonctionnalité STP BPDU Guard est désactivée. Émettez cette commande afin d'activer la fonctionnalité STP PortFast BPDU Guard sur le commutateur :

Commande CatOS

```
Console> (enable) set spantree portfast bpdu-guard enable

Spantree portfast bpdu-guard enabled on this switch.

Console> (enable)
```

Commande du logiciel Cisco IOS

```
CatSwitch-IOS(config)# spanning-tree portfast bpduguard
CatSwitch-IOS(config)
```

Quand la fonctionnalité STP BPDU Guard désactive le port, il reste à l'état de désactivé à moins qu'il ne soit activé manuellement. Vous pouvez configurer un port de façon à ce qu'il se réactive lui-même automatiquement depuis l'état errdisable. Émettez ces commandes, qui définissent **l'intervalle de délai d'attente errdisable** et activent la fonctionnalité **délai d'attente** :

Commandes CatOS

```
Console> (enable) set errdisable-timeout interval 400

Console> (enable) set errdisable-timeout enable bpdu-guard
```

Commandes du logiciel Cisco IOS

```
CatSwitch-IOS(config)# errdisable recovery cause bpduguard

CatSwitch-IOS(config)# errdisable recovery interval 400
```

Remarque: L'intervalle de délai d'attente est de 300 secondes et, par défaut, la fonctionnalité de délai d'attente est désactivée.

Surveillance

Afin de vérifier si la fonctionnalité est activée ou désactivée, émettez cette commande :

Sortie de commande

Commande CatOS

```
Console> (enable) show spantree summary
Root switch for vlans: 3-4.
Portfast bpdu-guard enabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of Connected Spanning Tree Ports By VLAN:

Vlan  Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

   1         0         0        0          1          1

   3         0         0        0          1          1

   4         0         0        0          1          1

  20         0         0        0          1          1


Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

Total        0         0        0          4          4

Console> (enable)
```

Commande du logiciel Cisco IOS

```
CatSwitch-IOS# show spanning-tree summary totals
Root bridge for: none.
PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short
```

```
Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
  1 VLAN                 0         0         0         1          1

CatSwitch-IOS#
```

Informations connexes

- Pages de support pour les produits LAN
- Page de support sur la commutation LAN
- Support et documentation techniques - Cisco Systems