Comprendre les fonctions de protection Spanning Tree PortFast et BPDU

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Conventions
- Informations générales
- PortFast et protection BPDU
  - Exemple 1 - Fonctionnement normal du protocole STP
  - Exemple 2 - Un pont non autorisé provoque une panne
- Configuration
  - Activer PortFast et la protection BPDU par interface
  - Activer la protection BPDU globalement
  - Configurer l'état errdisable de récupération automatique
- Vérification
- Informations connexes

Introduction

Ce document décrit la fonctionnalité d'amélioration de la protection des unités BPDU (PortFast and Bridge Protocol Data Unit) du protocole STP (Spanning Tree Protocol).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ces versions logicielles ont introduit la protection STP PortFast BPDU :

- Logiciel Cisco IOS® version 12.0(7)XE pour les plates-formes Catalyst 6500/6000
- Logiciel Cisco IOS Version 12.1(8a)EW pour Catalyst 4500/4000 Supervisor Engine III
- Logiciel Cisco IOS Version 12.1(12c)EW pour Supervisor Engine IV Catalyst 4500/4000
- Logiciel Cisco IOS Version 12.0(5)WC5 pour les gammes 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 Catalyst 3750 Metro
- 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 Catalyst 2950 LRE (Long-Reach Ethernet)
- Logiciel Cisco IOS Version 12.1(13)AY pour les commutateurs de la gamme Catalyst 2940

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

Reportez-vous aux conventions des conseils techniques Cisco pour plus d’information sur les conventions utilisées dans ce document.

Informations générales

Dans un réseau commuté correctement conçu, le protocole STP (Spanning Tree Protocol) empêche les boucles de couche 2 en plaçant les chemins redondants dans un état de blocage. Chaque port qui s’active passe normalement par les états STP (écoute, apprentissage et enfin transmission) avant de transmettre le trafic utilisateur. Ce délai de convergence, d'environ 30 secondes avec la norme 802.1D traditionnelle, est approprié pour les liaisons commutateur à

commutateur, mais inutile pour les ports connectés à des hôtes finaux tels que des PC, des serveurs ou des imprimantes, qui ne peuvent pas créer de boucle de commutation seuls.

Le défi est qu'un port se connectant à un hôte final ne doit pas du tout recevoir d'unités BPDU (Bridge Protocol Data Unit) STP. Si des BPDU arrivent sur un tel port, cela indique généralement l'un des deux problèmes suivants : une personne a connecté un commutateur non autorisé ou un périphérique exécute un logiciel qui émule un pont. Dans les deux cas, la topologie peut être déstabilisée, en particulier si le périphérique non autorisé annonce un ID de pont supérieur et force la sélection d'un pont racine auquel il ne doit jamais participer.

Un exemple concret illustre le risque. Un PC utilisateur exécutant une application de pontage Linux était connecté à un port d'accès. Comme l’application a envoyé des unités BPDU revendiquant une faible priorité de pont, le réseau a choisi le PC comme pont racine. La topologie Spanning Tree dans son ensemble a été déplacée vers un hôte sous-alimenté, ce qui a congestionné les liaisons et provoqué une panne du réseau. La protection BPDU existe précisément pour empêcher cette classe de défaillance.

PortFast et protection BPDU

PortFast fait passer immédiatement un port d'accès ou de liaison de l'état de blocage directement à l'état de transmission, en ignorant les phases d'écoute et d'apprentissage. Cela élimine le délai de démarrage pour les ports connectés aux périphériques finaux, ce qui est important pour les hôtes qui attendent un accès réseau immédiat (par exemple, les stations de travail utilisant DHCP au démarrage).

PortFast est uniquement destiné aux ports connectés à une station d'extrémité unique. L'activation sur un port qui se connecte à un autre commutateur réintroduit le risque de boucle même que STP est conçu pour empêcher, parce que le port commence le transfert avant que STP ait une chance de détecter un chemin redondant.

BPDU Guard complète la fonctionnalité PortFast en imposant l'hypothèse qu'un port PortFast activé ne doit jamais voir de BPDU. Lorsque la protection BPDU est activée et que le port reçoit une BPDU, le commutateur arrête immédiatement le port en le plaçant dans l'état errdisable. La topologie est ainsi protégée de deux manières :

- Il empêche un commutateur non autorisé ou mal configuré de s’injecter dans le Spanning Tree.
- Il empêche les périphériques, comme le pont Linux dans le scénario précédent, de détourner le rôle racine.

Comme le port est désactivé sur le plan administratif plutôt que simplement bloqué, l'opérateur réseau est averti de l'événement et le périphérique incriminé est clairement isolé jusqu'à ce que le problème soit résolu.

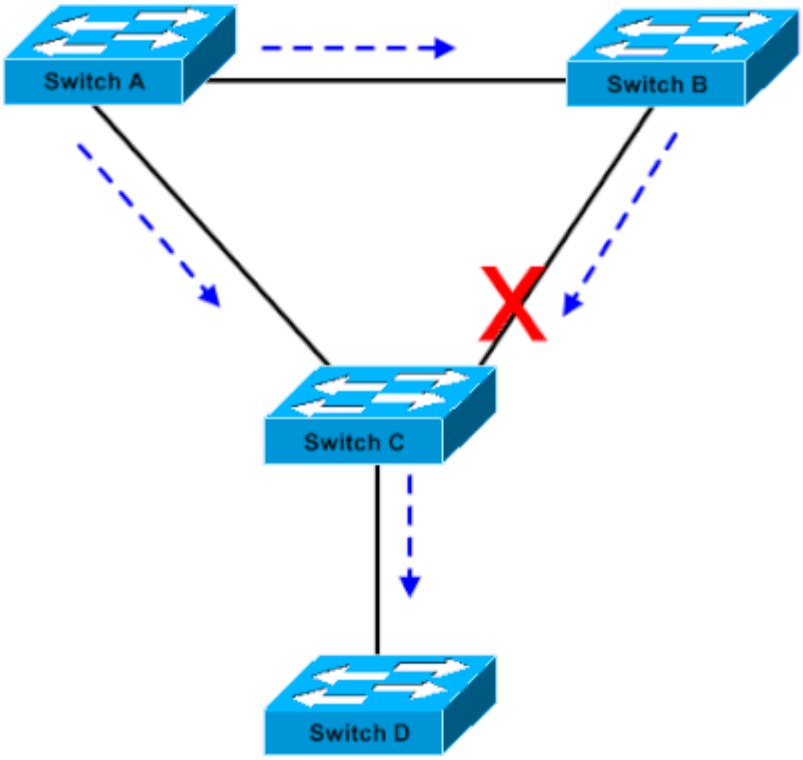
Un port placé dans errdisable ne récupère pas seul, sauf si errdisable recovery est configurée. Vous pouvez soit réactiver l'interface manuellement (shutdown suivi de no shutdown) ou configurer la récupération automatique pour la cause BPDU Guard.

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
```

Prenons l'exemple suivant :

Exemple 1 - Fonctionnement normal du protocole STP



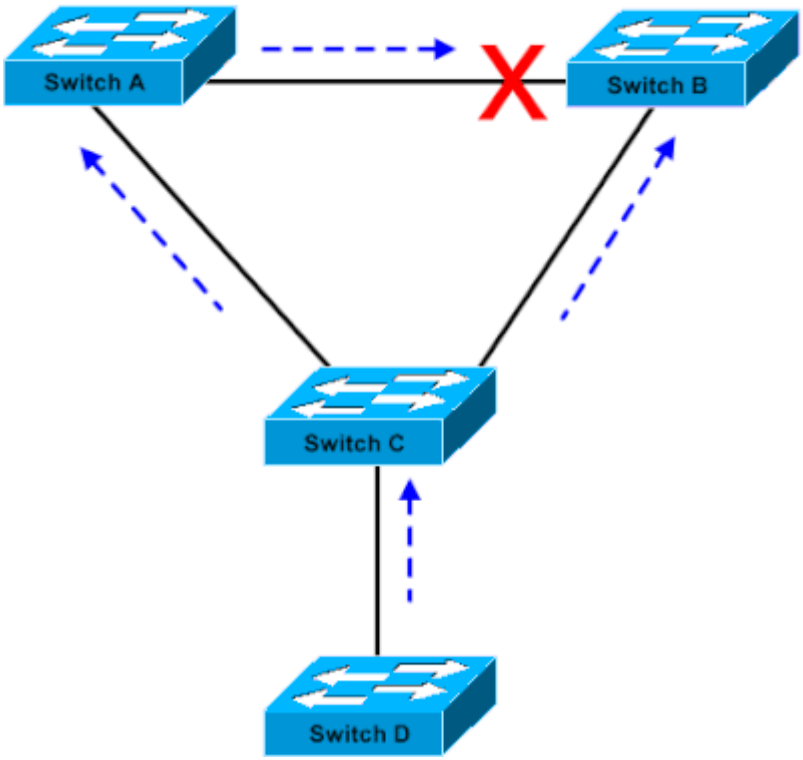
Connexion en pont

La topologie se compose de trois commutateurs formant les couches coeur de réseau et d’accès, ainsi que d’un périphérique final :

- Le commutateur A a une priorité de pont de 8192 et est le pont racine pour le VLAN.
- Le commutateur B a une priorité de pont de 16384, ce qui en fait le pont racine de secours pour le même VLAN.
- Les commutateurs A et Bare sont reliés par une liaison Ethernet Gigabit et forment ensemble le coeur du réseau.
- Le commutateur C est un commutateur d'accès. PortFast est configuré sur le port connecté au périphérique D.
- Le périphérique est un PC et ne participe pas au protocole STP.

Avec tous les autres paramètres STP laissés à leurs valeurs par défaut, STP converge comme prévu. Le commutateur A est choisi comme racine et le chemin redondant est bloqué pour rompre la boucle, en particulier, le port du commutateur C faisant face au commutateur B est placé dans l'état de blocage (indiqué par le « X » rouge sur cette liaison). Les flèches en pointillés tracent le flux normal des unités BPDU STP dans la topologie. Cela peut être considéré comme un réseau stable où PortFast fournit une connectivité immédiate au périphérique D, tandis que STP gère silencieusement les liaisons de coeur redondantes.

Exemple 2 - Un pont non autorisé provoque une panne



L'application Bridge basée sur Linux est lancée sur un PC

Cet exemple montre ce qui se passe lorsque le périphérique D cesse de se comporter comme un hôte d'extrémité simple et commence à participer au protocole STP, exactement comme dans le scénario où la protection BPDU est conçue pour s'arrêter. Une application de pont basée sur

Linux est lancée sur le PC (périphérique D). L'application annonce une priorité de pont de 0 (ou toute valeur inférieure à la priorité racine actuelle). Comme le protocole STP privilégie toujours l’ID de pont le plus bas, le pont basé sur Linux remporte la sélection de la racine et prend le rôle de pont racine à partir du commutateur A.

Cette réélection remodèle la topologie entière. La liaison Gigabit Ethernet haut débit entre les deux commutateurs principaux (A et B) passe au blocage (illustré par le « X » rouge passant sur la liaison principale). Par conséquent, tout le trafic VLAN qui utilisait auparavant le coeur Gigabit est forcé sur un chemin 100 Mbits/s plus lent. Lorsque la demande de trafic dépasse ce que cette liaison peut transporter, le commutateur commence à abandonner des trames et le résultat est une panne de connectivité.

Comment la protection BPDU empêche-t-elle le problème ? Comme PortFast est activé sur le port du commutateur C vers le périphérique D, ce port ne doit jamais recevoir de BPDU. Au moment où le périphérique D envoie une BPDU STP, la protection BPDU arrête le port en le plaçant dans l'état errdisable. Le périphérique D est isolé avant de pouvoir influencer le choix de la racine, et la topologie principale reste intacte.

Configuration

L'approche recommandée est d'activer PortFast et la protection BPDU ensemble sur les ports d'accès faisant face à l'hôte. Vous pouvez activer ou désactiver la protection BPDU STP PortFast sur une base globale ou par interface. Par défaut, la protection STP BPDU est désactivée.

Activer PortFast et la protection BPDU par interface

<#root>

```
CatSwitch-IOS(config-if)#
```

spanning-tree portfast

```
CatSwitch-IOS(config-if)#
```

spanning-tree bpduguard enable

Activer la protection BPDU globalement

<#root>

CatSwitch-IOS(config)#

spanning-tree portfast bpduguard default

Avec la commande globale, chaque port configuré avec PortFast hérite automatiquement de la protection BPDU, vous n'avez donc pas besoin de la définir individuellement sur chaque interface.

Configurer l'état errdisable de récupération automatique

Lorsque la protection STP BPDU désactive le port, celui-ci reste dans un état désactivé, sauf si le port est activé manuellement. Vous pouvez configurer un port pour qu'il se réactive automatiquement à partir de l'état errdisable. Émettez ces commandes, qui définissent l'intervalle errdisable-timeout et activent la fonctionnalité timeout :

<#root>

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.

Vérification

Pour vérifier si la fonctionnalité est activée ou désactivée, exécutez la commande suivante applicable :

<#root>

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

- 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.