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

Contenu

Introduction

Le protocole Spanning Tree (STP) résout les topologies physiquement redondantes dans les topologies sans boucles de type arbre. Le plus grand problème avec STP est que quelques défaillances matérielles peuvent le faire échouer. Cette panne crée des boucles de transfert (ou boucles STP). D'importantes pannes du réseau sont provoquées par les boucles STP.

Ce document décrit la fonctionnalité de la protection contre les boucles STP, qui est destinée à améliorer la stabilité des réseaux de couche 2. Ce document décrit également la détection des différences de temps de propagation des BPDU. La détection des différences de temps de propagation des BPDU est une fonctionnalité de diagnostic qui produit des messages syslog quand les BPDU ne sont pas reçues dans les délais.

Conditions préalables

Conditions requises

Ce document suppose que le lecteur est au courant du fonctionnement de base de STP. Référez-vous à Compréhension et configuration du Protocole Spanning Tree (STP) sur les commutateurs Catalyst afin d'apprendre comment fonctionne STP.

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.

Disponibilité des fonctionnalités

CatOS

- La fonctionnalité de protection contre les boucles STP a été introduite dans CatOS Version 6.2.1 du logiciel Catalyst pour les plates-formes Catalyst 4000 et Catalyst 5000 et dans la version 6.2.2 pour la plate-forme Catalyst 6000.
- La fonctionnalité de détection des différences de temps de propagation des BPDU de STP a été introduite dans CatOS Version 6.2.1 du logiciel Catalyst pour les plates-formes Catalyst 4000 et Catalyst 5000 et dans la version 6.2.2 pour la plate-forme Catalyst 6000.

Cisco IOS®

- La fonctionnalité de protection contre les boucles STP a été introduite dans le logiciel Cisco IOS Version 12.1(12c)EW pour les commutateurs Catalyst 4500 et dans le logiciel Cisco IOS Version 12.1(11b)EX pour Catalyst 6500.
- La fonctionnalité de détection des différences de temps de propagation des BPDU n'est pas prise en charge dans les commutateurs Catalyst exécutant le logiciel Cisco IOS.

Résumé rapide des rôles des ports STP

En interne, STP assigne à chacun port de pont (ou commutateur) un rôle qui est basé sur la configuration, la topologie, la position relative du port dans la topologie, et sur d'autres considérations. Le rôle du port définit le comportement du port du point de vue du protocole STP. Basé sur son rôle, le port envoie ou reçoit des BPDU STP et transmet ou bloque le trafic de données. Cette liste fournit un résumé rapide de chaque rôle de port STP :

- *Designated* : (désigné) un port désigné est élu par liaison (segment). Le port désigné est le port le plus proche du pont racine. Ce port envoie des BPDU sur la liaison (segment) et achemine le trafic vers le pont racine. Dans un réseau STP convergé, chaque port désigné est dans l'état de transfert STP.
- *Root* : (racine) le pont peut avoir seulement un port racine. Le port racine est le port qui mène au pont racine. Dans un réseau STP convergé, le port racine est dans l'état de transfert STP.
- *Alternate* : (de remplacement) les ports de remplacement mènent au pont racine, mais ne sont pas des ports racine. Les ports alternatifs mettent à jour l'état de blocage de STP.
- *Backup* : (de secours) ceci est un cas spécial quand deux ou plusieurs ports du même pont

(commutateur) sont connectés ensemble, directement ou par des supports partagés. Dans ce cas, un port est désigné, et les ports restants bloquent. Le rôle pour ce port est backup (de secours) .

Protection contre les boucles STP

Description de la fonctionnalité

La fonctionnalité de protection contre les boucles STP fournit une protection supplémentaire contre les boucles de transfert de couche 2 (boucles STP). Une boucle STP est créée lorsqu'un port de blocage de STP dans une topologie redondante passe par erreur dans l'état de transfert. Cela se produit généralement parce que l'un des ports d'une topologie redondante physiquement (pas nécessairement le port de blocage de STP) ne reçoit plus les unités de données de protocole de pont (BDPU) STP. Dans son fonctionnement, STP compte sur la réception ou la transmission continue de BPDU en fonction du rôle du port. Le port désigné transmet les BPDU, et le port non désigné les reçoit.

Lorsque l'un des ports d'une topologie redondante physiquement ne reçoit plus les BPDU, STP conçoit que la topologie est sans boucle. En définitive, le port de blocage du port de remplacement ou de secours devient le port désigné et passe dans l'état de transfert. Cette situation crée une boucle.

La fonctionnalité de protection contre les boucles effectue des contrôles supplémentaires. Si les BPDU ne sont pas reçues sur un port non désigné, et que la protection contre les boucles est activée, ce port est passé dans l'état de blocage de boucles STP incohérentes, plutôt que dans l'état d'écoute/apprentissage/transfert. Sans la fonctionnalité de protection contre les boucles, le port prend par défaut le rôle du port désigné. Le port passe dans l'état de transfert via STP et crée une boucle.

Lorsque la protection contre les boucles bloque un port incohérent, ce message est enregistré :

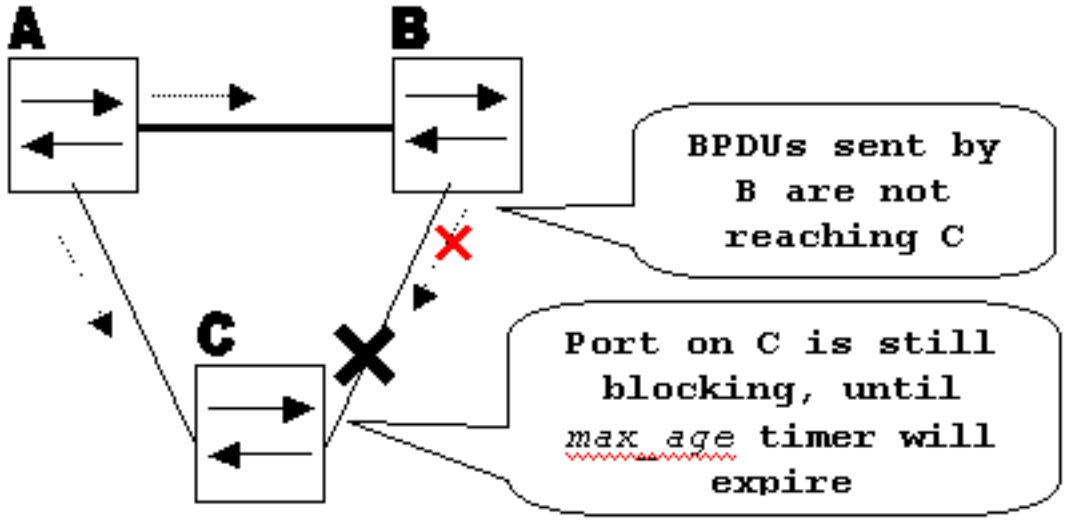
- CatOS`%SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan 3. Moved to loop-inconsistent state.`
- Cisco IOS`%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet0/24 on VLAN0050.`

Une fois que les BPDU sont reçues sur un port dans un état de boucles STP incohérentes, le port passe à un autre état STP. Selon les BPDU reçues, ceci signifie que la reprise est automatique et qu'une intervention n'est pas nécessaire. Après la reprise, ce message est enregistré :

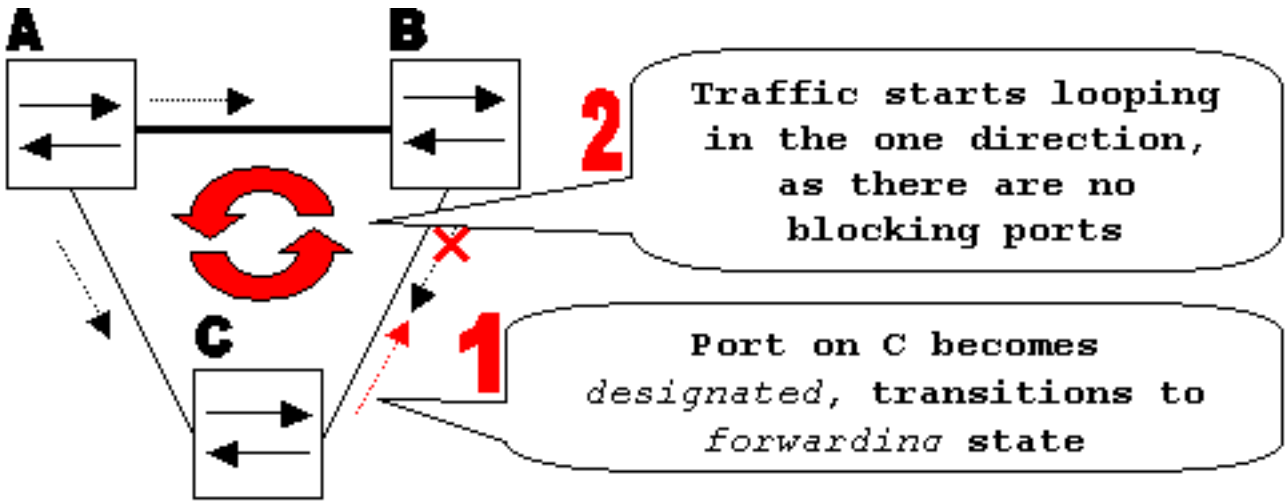
- CatOS`%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.`
- Cisco IOS`%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port FastEthernet0/24 on VLAN0050.`

Considérez cet exemple afin d'illustrer ce comportement :

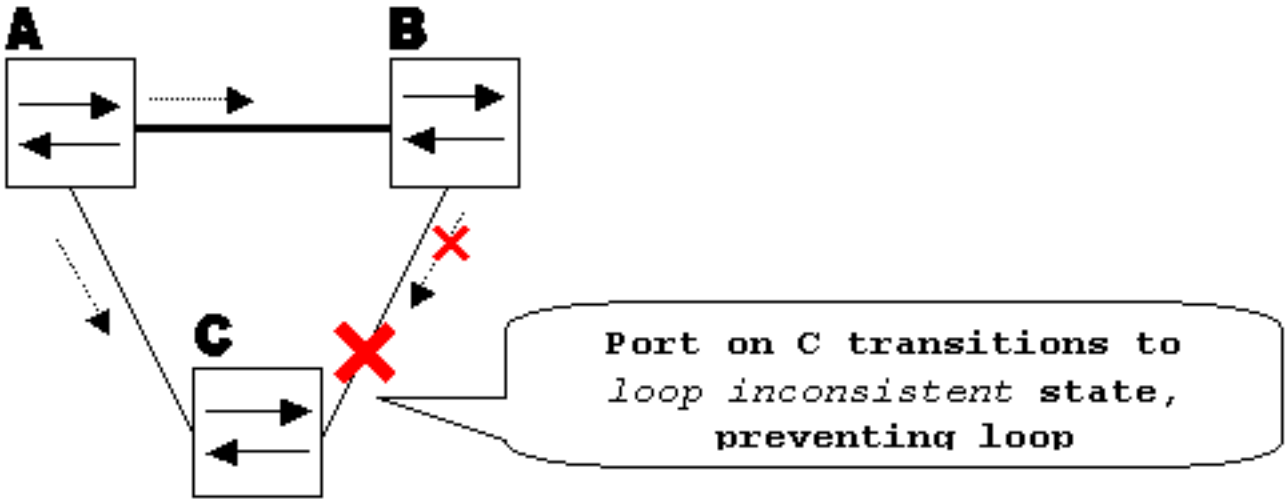
Le commutateur A est le commutateur racine. Le commutateur C ne reçoit pas d'unités BPDU du commutateur B dû à la défaillance de la liaison unidirectionnelle sur la liaison entre le commutateur B et le commutateur C.



Sans la fonctionnalité de protection contre les boucles, le port de blocage de STP sur le commutateur C passe à l'état d'écoute de STP quand le temporisateur de max_age expire, puis il passe à l'état de transfert en deux fois plus de temps que la valeur forward_delay. Cette situation crée une boucle.



La protection contre les boucles étant activée, le port de blocage sur le commutateur C passe à l'état de boucles STP incohérentes quand le temporisateur de max_age expire. Un port dans l'état de boucles STP incohérentes ne passant pas le trafic utilisateur, une boucle n'est pas créée. (L'état de boucle incohérente est effectivement égal à l'état de blocage.)

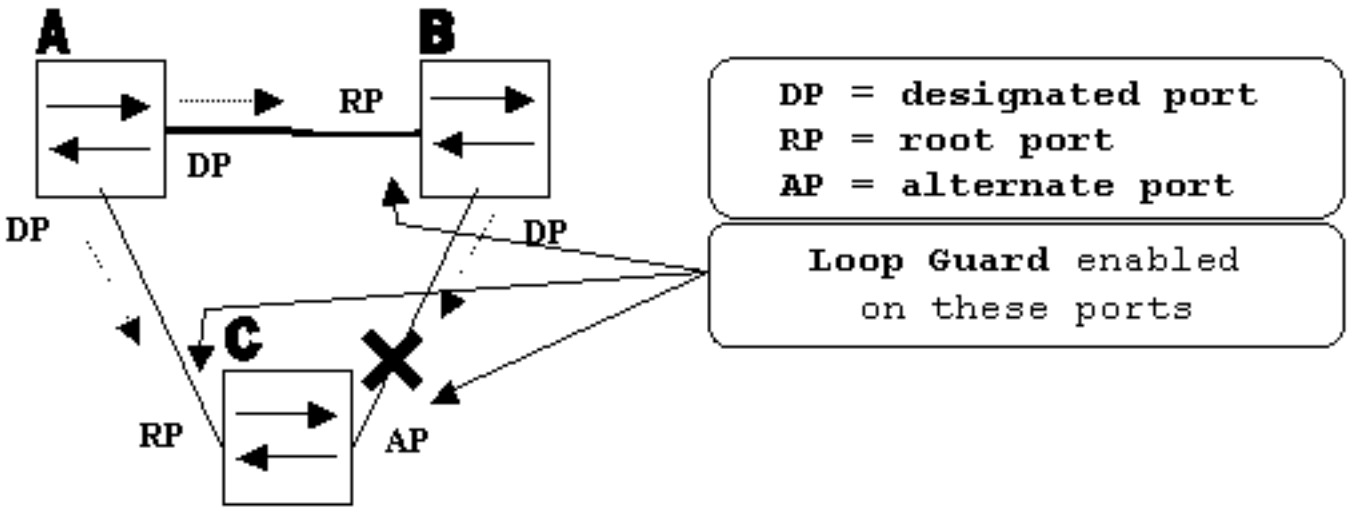


Considérations de configuration

La fonctionnalité de protection contre les boucles est activée sur une base par port. Cependant, tant qu'elle bloque le port au niveau du STP, la protection contre les boucles bloque les ports incohérents sur une base per-VLAN (en raison de per-VLAN STP). C'est-à-dire que si les BPDU ne sont pas reçues sur le port de jonction pour seulement un VLAN particulier, ce VLAN seulement est bloqué (placé dans l'état de boucles STP incohérentes). Pour la même raison, si elle est activée sur une interface EtherChannel, le canal entier est bloqué pour un VLAN particulier, pas simplement une liaison (parce que l'EtherChannel est considéré comme un port logique du point de vue de STP).

Sur quels ports le dispositif de protection contre les boucles devrait-il être activé ? La réponse la plus évidente est sur les ports de blocage. Cependant, ce n'est pas totalement correct. Le dispositif de protection contre les boucles doit être activé sur les ports non désignés (plus précisément, sur les ports racine et alternatifs) pour toutes les combinaisons possibles de topologies actives. Tant que le dispositif de protection contre les boucles n'est pas une fonctionnalité per-VLAN, le même port (jonction) pourrait être indiqué pour un VLAN et non désigné pour l'autre. Les scénarios de panne possible devraient également être pris en considération.

Considérez cet exemple :



Par défaut, la protection contre les boucles est désactivée. Cette commande est utilisée pour activer la protection contre les boucles :

- CatOS

```
set spantree guard loop <mod/port>

Console> (enable) set spantree guard loop 3/13
Enable loopguard will disable rootguard if it's currently enabled on the port(s).
Do you want to continue (y/n) [n]? y
Loopguard on port 3/13 is enabled.
```

- Cisco IOS

```
spanning-tree guard loop

Router(config)#interface gigabitEthernet 1/1
Router(config-if)#spanning-tree guard loop
```

Avec la version 7.1(1) du logiciel Catalyst (CatOS), la protection contre les boucles peut être

activée globalement sur tous les ports. En fait, la protection contre les boucles est activée sur toutes les liaisons point par point. La liaison point à point est détectée par l'état duplex de la liaison. Si le mode duplex est bidirectionnel simultané, la liaison est considérée point à point. Il est toujours possible de configurer, ou d'ignorer, les configurations globales sur une base par port.

Émettez cette commande afin d'activer globalement la protection contre les boucles :

- CatOS`Console> (enable) **set spantree global-default loopguard enable**`
- Cisco IOS`Router(config)#**spanning-tree loopguard default**`

Émettez cette commande afin de désactiver la protection contre les boucles :

- CatOS`Console> (enable) **set spantree guard none <mod/port>**`
- Cisco IOS`Router(config-if)#**no spanning-tree guard loop**`

Émettez cette commande afin de désactiver globalement la protection contre les boucles :

- CatOS`Console> (enable) **set spantree global-default loopguard disable**`
- Cisco IOS`Router(config)#**no spanning-tree loopguard default**`

Émettez cette commande afin de vérifier la protection contre les boucles :

- CatOS
  show spantree guard <mod/port>

  ```
  Console> (enable) show spantree guard 3/13
  Port                     VLAN Port-State    Guard Type
  ------------------------ ---- ------------- ----------
  3/13                     2    forwarding          loop
  Console> (enable)
  ```
- Cisco IOS
  show spanning-tree

  ```
  Router#show spanning-tree summary
  Switch is in pvst mode
  Root bridge for: none
  EtherChannel misconfig guard is enabled
  Extended system ID           is disabled
  Portfast Default             is disabled
  PortFast BPDU Guard Default  is disabled
  Portfast BPDU Filter Default is disabled
  Loopguard Default            is enabled
  UplinkFast                   is disabled
  BackboneFast                 is disabled
  Pathcost method used         is short

  Name                   Blocking Listening Learning Forwarding STP Active
  ---------------------- -------- --------- -------- ---------- ----------
  Total                         0         0        0          0          0
  ```

Protection contre les boucles et UDLD

La protection contre les boucles et la fonctionnalité UDLD (UniDirectional Link Detection) se superposent, en partie parce que chacune protège contre les pannes STP entraînées par des liaisons unidirectionnelles. Cependant, ces deux fonctionnalités diffèrent dans leur fonctionnement et leur approche du problème. Cette table décrit la protection contre les boucles et la fonctionnalité UDLD :

Fonctionnalité	Protection contre les boucles	UDLD
Configuration	Par port	Par port
Granularité d'action	Per-VLAN	Par port
Autorecover	Oui	Oui, avec la fonctionnalité errer-disable timeout
Protection contre les pannes STP provoquées par des liaisons unidirectionnelles	Oui, une fois activée sur tous les ports racine et alternatifs dans la topologie redondante	Oui, une fois activée sur toutes les liaisons dans la topologie redondante
Protection contre les pannes STP provoquées par des problèmes dans le logiciel (le commutateur désigné n'envoie pas de BPDU)	Oui	Non
Protection contre les erreurs de câblage.	Non	Oui

Basé sur les diverses considérations de conception, vous pouvez choisir la fonctionnalité UDLD ou celle de protection contre les boucles. Concernant STP, la différence la plus apparente entre les deux fonctionnalités est l'absence de protection dans UDLD contre les pannes STP provoquées par des problèmes dans le logiciel. En conséquence, le commutateur désigné n'envoie pas de BPDU. Cependant, ce type de panne est (par un ordre de grandeur) plus rare que les pannes provoquées par des liaisons unidirectionnelles. En échange, UDLD pourrait être plus flexible dans le cas des liaisons unidirectionnelles sur EtherChannel. Dans ce cas, UDLD désactive seulement les liaisons défaillantes, et le canal devrait demeurer fonctionnel avec les liaisons qui restent. Dans une telle panne, le dispositif de protection contre les boucles le met dans l'état de boucle incohérente de bloquer tout le canal.

D'autre part, la protection contre les boucles ne travaille pas sur des liaisons partagées ou dans les situations où la liaison a été unidirectionnelle depuis l'établissement de la liaison. Dans le dernier cas, le port ne reçoit jamais les BPDU et devient désigné. Puisque ce comportement pourrait être normal, ce cas particulier n'est pas couvert par la protection contre les boucles. UDLD fournit une protection contre un tel scénario.

Comme décrit, le niveau le plus haut de protection est fourni quand vous activez UDLD et la protection contre les boucles.

Interopérabilité de la protection contre les boucles avec d'autres fonctionnalités STP

Protection de la racine

La protection de la racine est mutuellement exclusif avec la protection contre les boucles. La protection de la racine est utilisée sur les ports désignés et ne permet pas au port de devenir non

désigné. La protection contre les boucles fonctionne sur les ports non désignés et ne permet pas au port de devenir désigné par l'expiration du max_age. La protection de la racine ne peut pas être activée sur le même port que la protection contre les boucles. Quand la protection contre les boucles est configuré sur le port, elle désactive la protection de la racine configurée sur ce même port.

Uplink Fast et Backbone Fast

Uplink Fast et Backbone Fast sont transparents pour la protection contre les boucles. Quand le max_age est ignoré par Backbone Fast au moment de la reconvergence, il ne déclenche pas la protection contre les boucles. Pour plus d'informations sur Uplink Fast et Backbone Fast, référez-vous à ces documents :

- Compréhension et configuration de la fonctionnalité Cisco Uplink Fast
- Présentation et configuration de la fonction Backbone Fast sur les commutateurs Catalyst

Portfast et la protection des BPDU, et VLAN dynamique

La protection contre les boucles ne peut pas être activée pour les ports sur lesquels portfast est activé. Puisque la protection des BPDU fonctionne sur les ports en portfast, quelques restrictions s'appliquent à la protection des BPDU. La protection contre les boucles ne peut pas être activée sur les ports VLAN dynamiques puisque ces ports sont en portfast.

Liens partagés

La protection contre les boucles ne devrait pas être activée sur des liens partagés. Si vous activez la protection contre les boucles sur des liens partagés, le trafic des hôtes connectés aux segments partagés pourrait être bloqué.

Protocole MSTP (Multiple Spanning Tree Protocol)

La protection contre les boucles fonctionne correctement dans l'environnement MST.

Détection des différences de temps de propagation des BPDU

La protection contre les boucles devrait fonctionner correctement avec la détection des différences de temps de propagation des BPDU.

Détection des différences de temps de propagation des BPDU

Description de la fonctionnalité

STP compte fortement sur la réception opportune des BPDU. À chaque message hello_time (2 secondes par défaut), le pont racine envoie des BPDU. Les ponts non racine ne régénèrent pas les BPDU pour chaque message hello_time, mais ils reçoivent les BPDU relayées par le pont racine. Par conséquent, chaque pont non racine devrait recevoir des BPDU sur chaque VLAN pour chaque message hello_time. Dans certains cas, des BPDU sont perdues ou la CPU du pont est trop occupée pour relayer les BPDU en temps utile. Ces problèmes, de même que d'autres, peuvent provoquer l'arrivée tardive des BPDU (si elles arrivent). Ce problème compromet potentiellement la stabilité de la topologie d'interconnexion arborescente.

La détection des différences de temps de propagation des BPDU permet au commutateur

d'assurer le suivi des BPDU qui arrivent tard et d'informer l'administrateur avec des messages syslog. Pour chaque port sur lequel une BPDU est jamais arrivée en retard (ou est décalée), la détection des différences de temps de propagation enregistre le décalage le plus récent et sa durée (latence). Elle enregistre également le retard de BPDU le plus long sur ce port particulier.

Afin de protéger la CPU du pont d'une surcharge, un message syslog n'est pas généré chaque fois qu'un décalage de BPDU se produit. Les messages sont limités en débit à un message toutes les 60 secondes. Cependant, si le retard des BPDU dépasse le max_age divisé par 2 (ce qui équivaut à 10 secondes par défaut), le message est immédiatement imprimé.

Remarque: La détection des différences de temps de propagation des BPDU est une fonctionnalité de diagnostic. À la détection des différences de propagation des BPDU, elle envoie un message syslog. La détection des différences de temps de propagation des BPDU ne prend aucune autre action corrective.

Ceci est un exemple de message syslog produit par la détection des différences de temps de propagation des BPDU :

show spanning-tree

```
Router#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID           is disabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Pathcost method used         is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
Total                         0         0        0          0          0
```

Considérations de configuration

La détection des différences de temps de propagation des BPDU est configurée par commutateur. Le paramètre par défaut est désactivé. Émettez cette commande afin d'activer la détection des différences de temps de propagation des BPDU :

```
Cat6k> (enable) set spantree bpdu-skewing enable
   Spantree bpdu-skewing enabled on this switch.
```

Afin de voir les informations de décalage des BPDU, utilisez la commande **show spantree bpdu-skewing <vlan>|<mod/port>** comme expliqué en cet exemple :

```
Cat6k> (enable) show spantree bpdu-skewing 1
Bpdu skewing statistics for vlan 1
Port Last Skew (ms) Worst Skew (ms) Worst Skew Time
-------------- -------------- -------------- -------------------------
3/12 4000 4100 Mon Nov 19 2001, 16:36:04
```

Informations connexes

- Amélioration de la protection de la racine du protocole STP (Spanning Tree Protocol)
- Amélioration de la protection des BPDU en PortFast pour le spanning tree
- Présentation et configuration du protocole UDLD (Unidirectional Link Detection)
- Utilisation de PortFast et d'autres commandes pour remédier aux délais de connectivité lors du démarrage de la station de travail
- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems