

Résolution des problèmes STP sur les commutateurs Catalyst

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Causes des défaillances STP](#)

[Dépannage des boucles de transfert](#)

- [1. Identifier la boucle](#)
- [2. Détection de la topologie \(portée\) de la boucle](#)
- [3. Briser la boucle](#)
- [4. Trouver et corriger la cause de la boucle](#)
- [5. Restaurer la redondance](#)

[Examen des modifications topologiques](#)

[Trouver la cause de l'inondation](#)

[Trouver la source des CT](#)

[Prendre des mesures pour prévenir les TC excessifs](#)

[Résolution des problèmes liés au temps de convergence](#)

[Utiliser les commandes de débogage STP](#)

[Sécurisation du réseau contre les boucles de transfert](#)

- [1. Activez la détection de liaison unidirectionnelle \(UDLD\) sur toutes les liaisons de commutateur à commutateur](#)
- [2. Activez la protection contre les boucles sur tous les commutateurs](#)
- [3. Activez Portfast sur tous les ports des stations d'extrémité](#)
- [4. Définissez EtherChannels sur DesirableMode des deux côtés \(si pris en charge\) et sur Non-SilentOption](#)
- [5. Ne désactivez pas la négociation automatique \(si elle est prise en charge\) sur les liaisons commutateur à commutateur](#)
- [6. Faites attention lorsque vous réglez les compteurs STP](#)
- [7. Si des attaques par déni de service sont possibles, sécurisez le périmètre STP du réseau avec Root Guard](#)
- [8. Activez la protection BPDU sur les ports compatibles Portfast, pour empêcher le protocole STP d'être affecté par des périphériques réseau non autorisés \(tels que des concentrateurs, des commutateurs et des routeurs de pontage\) connectés aux ports](#)
- [9. Éviter le trafic utilisateur sur le VLAN de gestion](#)
- [10. Un emplacement racine STP prédictible \(codé en dur\) et racine STP de secours](#)

[Informations connexes](#)

Introduction

Ce document décrit comment utiliser le logiciel Cisco IOS® pour dépanner les problèmes avec le

protocole STP (Spanning Tree Protocol).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Différents types de Spanning Tree et comment les configurer. Référez-vous [à Configuration de STP et IEEE 802.1s](#) MST pour plus d'informations.
- Diverses fonctionnalités Spanning Tree et comment les configurer. Référez-vous [à Configuration des fonctions STP](#) pour plus d'informations.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Catalyst 6500 avec moteur Supervisor 2
- Logiciel Cisco IOS Version 12.1(13)E

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

Il existe des commandes spécifiques qui s'appliquent uniquement aux commutateurs Catalyst 6500/6000 ; cependant, vous pouvez appliquer la plupart des principes à n'importe quel commutateur Cisco Catalyst qui exécute le logiciel Cisco IOS.

Les problèmes avec la plupart des STP présentent les trois problèmes suivants :

- Boucles de transfert.
- Inondation excessive due à un taux élevé de modifications de topologie STP (TC).
- Problèmes liés au temps de convergence.

Parce qu'un pont n'a pas de mécanisme pour suivre si un certain paquet est transféré plusieurs fois (par exemple, une durée de vie IP [TTL]) ou est utilisé pour rejeter le trafic qui circule trop

longtemps sur le réseau. Un seul chemin peut exister entre deux périphériques dans le même domaine de couche 2 (L2).

Le but du protocole STP est de bloquer les ports redondants sur la base d'un algorithme STP et de résoudre la topologie physique redondante en une topologie arborescente. Une boucle de transfert (telle qu'une boucle STP) se produit lorsqu'aucun port d'une topologie redondante n'est bloqué et que le trafic est transféré en cercle indéfiniment.

Une fois que la boucle de transfert démarre, elle encombre les liaisons à bande passante la plus faible le long de son chemin. Si toutes les liaisons ont la même bande passante, toutes les liaisons sont encombrées. Cet encombrement entraîne une perte de paquets et entraîne une panne du réseau dans le domaine L2 affecté.

Avec une inondation excessive, les symptômes ne sont pas aussi évidents. Les liaisons lentes peuvent devenir encombrées par le trafic inondé, et les périphériques ou utilisateurs derrière ces liaisons encombrées peuvent subir une lenteur ou une perte totale de connectivité.

Causes des défaillances STP

Le protocole STP émet certaines hypothèses concernant son environnement opérationnel. Voici les hypothèses les plus pertinentes pour ce document :

- Chaque liaison entre les deux ponts est bidirectionnelle. Cela signifie que, si A se connecte directement à B, alors A reçoit ce que B a envoyé et B reçoit ce que A a envoyé, tant que la liaison est active entre eux.
- Chaque pont qui exécute le protocole STP est capable de recevoir, traiter et transmettre régulièrement des unités BPDU (Bridge Protocol Data Unit), également appelées paquets STP.

Bien que ces hypothèses semblent logiques et évidentes, il existe des situations où elles ne sont pas satisfaites. La plupart de ces situations impliquent un type de problème matériel ; cependant, des défauts logiciels peuvent également conduire à des pannes STP. Diverses défaillances matérielles, erreurs de configuration et problèmes de connexion sont à l'origine de la majorité des défaillances du protocole STP, tandis que les défaillances logicielles sont la cause de la minorité. Des défaillances STP peuvent également se produire en raison de connexions supplémentaires inutiles entre les commutateurs. Les VLAN passent en état down (inactif) en raison de ces connexions supplémentaires. Pour résoudre ce problème, supprimez toutes les connexions indésirables entre les commutateurs.

Lorsque l'une de ces hypothèses n'est pas satisfaite, un ou plusieurs ponts ne peuvent pas recevoir ou traiter les unités BPDU. Cela signifie que le ou les ponts ne découvrent pas la topologie du réseau. Sans connaissance de la topologie correcte, le commutateur ne peut pas bloquer les boucles. Par conséquent, le trafic inondé circule sur la topologie en boucle, consomme toute la bande passante et met le réseau hors service.

Les émetteurs-récepteurs défectueux ou les convertisseurs d'interface Gigabit (GBIC), les problèmes de câbles ou les défaillances matérielles sur le port, la carte de ligne ou le moteur de

supervision sont des exemples de raisons pour lesquelles les commutateurs ne peuvent pas recevoir de BPDU. Une raison fréquente des pannes STP est une liaison unidirectionnelle entre les ponts. Dans un tel cas, un pont envoie des BPDU, mais le pont en aval ne les reçoit jamais. Le traitement STP peut également être perturbé par un CPU surchargé (99 % ou plus) parce que le commutateur ne peut pas traiter les BPDU reçues. Les unités BPDU peuvent être corrompues le long du chemin d'un pont à l'autre, ce qui empêche également un comportement STP correct.

En dehors des boucles de transfert, lorsqu'aucun port n'est bloqué, il existe des situations où seuls certains paquets sont incorrectement transférés via les ports qui bloquent le trafic. Dans la plupart des cas, cela est dû à des problèmes logiciels. Un tel comportement peut provoquer des boucles lentes. Cela signifie que certains paquets sont mis en boucle, mais que la majorité du trafic circule toujours sur le réseau, car les liaisons ne sont pas encombrées.

Dépannage des boucles de transfert

Les boucles de transfert varient considérablement en termes d'origine (cause) et d'effet. En raison de la grande variété de problèmes qui peuvent affecter le STP, ce document ne peut fournir que des directives générales sur la façon de dépanner les boucles de transfert.

Avant de commencer le dépannage, vous avez besoin des informations suivantes :

- Un schéma de topologie réel qui détaille tous les commutateurs et ponts.
- Les numéros de port correspondants (interconnectés).
- Les détails de la configuration STP, tels que le commutateur qui est la racine et la racine de secours, les liaisons qui ont un coût ou une priorité autre que par défaut, et l'emplacement des ports qui bloquent le trafic.

1. Identifier la boucle

Lorsqu'une boucle de transfert s'est développée sur le réseau, les symptômes habituels sont les suivants :

- Perte de connectivité vers, depuis et via les régions du réseau affectées.
- Utilisation élevée du CPU sur les routeurs connectés aux segments affectés ou aux VLAN qui peut entraîner divers symptômes, tels que le battement du voisin du protocole de routage ou le battement du routeur actif HSRP (Hot Standby Router Protocol).
- Utilisation élevée des liaisons (souvent 100 %).
- Utilisation élevée du fond de panier du commutateur (par rapport à l'utilisation de base).
- Les messages Syslog qui indiquent le bouclage des paquets dans le réseau (par exemple, les messages d'adresse IP dupliquée HSRP).
- Messages Syslog qui indiquent des messages de réapprentissage d'adresse constant ou de

battement d'adresse MAC.

- Le nombre de sorties diminue sur de nombreuses interfaces augmente.

N'importe laquelle de ces raisons peut indiquer différents problèmes (ou aucun problème du tout). Cependant, lorsque plusieurs d'entre elles sont observées en même temps, il est très probable qu'une boucle de transfert se soit développée dans le réseau. Le moyen le plus rapide de vérifier cela est de vérifier l'utilisation du trafic du fond de panier du commutateur :

```
<#root>
```

```
cat#
```


```
show catalyst6000 traffic-meter
```

```
traffic meter = 13%
```

```
Never cleared
```

```
peak = 14%
```

```
reached at 12:08:57 CET Fri Oct 4 2002
```

 Remarque : le commutateur Catalyst 4000 équipé de la plate-forme logicielle Cisco IOS ne prend actuellement pas en charge cette commande.

Si le niveau de trafic actuel est excessif ou si le niveau de base n'est pas connu, vérifiez si le niveau de crête a été atteint récemment et s'il est proche du niveau de trafic actuel. Par exemple, si le niveau de trafic maximal est de 15 % et qu'il a été atteint il y a tout juste deux minutes et que le niveau de trafic actuel est de 14 %, cela signifie que le commutateur a une charge inhabituellement élevée. Si la charge de trafic est à un niveau normal, cela signifie probablement qu'il n'y a pas de boucle ou que ce périphérique n'est pas impliqué dans la boucle. Cependant, il pourrait encore être impliqué dans une boucle lente.

2. Détection de la topologie (portée) de la boucle

Une fois qu'il a été établi que la raison de la panne réseau est une boucle de transfert, la priorité la plus élevée est d'arrêter la boucle et de restaurer le fonctionnement du réseau.

Pour arrêter la boucle, vous devez savoir quels ports participent à la boucle : regardez les ports avec l'utilisation de liaison la plus élevée (paquets par seconde). La commande `show interface` Logiciel Cisco IOS affiche l'utilisation de chaque interface.

Pour afficher uniquement les informations d'utilisation et le nom de l'interface (pour une analyse rapide), filtrez le résultat de l'expression régulière avec le logiciel Cisco IOS. Émettez l'interface `show | include line|vsec` pour afficher uniquement les statistiques paquet par seconde et le nom de

l'interface :

```
<#root>
```

```
cat#
```

```
show interface | include line|\ /sec
```

```
GigabitEthernet2/1 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/2 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

GigabitEthernet2/3 is up, line protocol is up
  5 minute input rate 99765230 bits/sec, 24912 packets/sec

  5 minute output rate 0 bits/sec, 0 packets/sec

GigabitEthernet2/4 is up, line protocol is up

  5 minute input rate 1000 bits/sec, 27 packets/sec

  5 minute output rate 101002134 bits/sec, 25043 packets/sec

GigabitEthernet2/5 is administratively down, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/6 is administratively down, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/7 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

GigabitEthernet2/8 is up, line protocol is up


  5 minute input rate 2000 bits/sec, 41 packets/sec


  5 minute output rate 99552940 bits/sec, 24892 packets/sec
```


Faites attention aux interfaces qui utilisent le plus de liaisons. Dans cet exemple, il s'agit des interfaces g2/3, g2/4 et g2/8 ; ce sont les ports qui participent à la boucle.


3. Briser la boucle

Pour rompre la boucle, vous devez arrêter ou déconnecter les ports concernés. Il est particulièrement important non seulement d'arrêter la boucle, mais aussi de trouver et de corriger la cause première de la boucle. Il est relativement plus facile de rompre la boucle

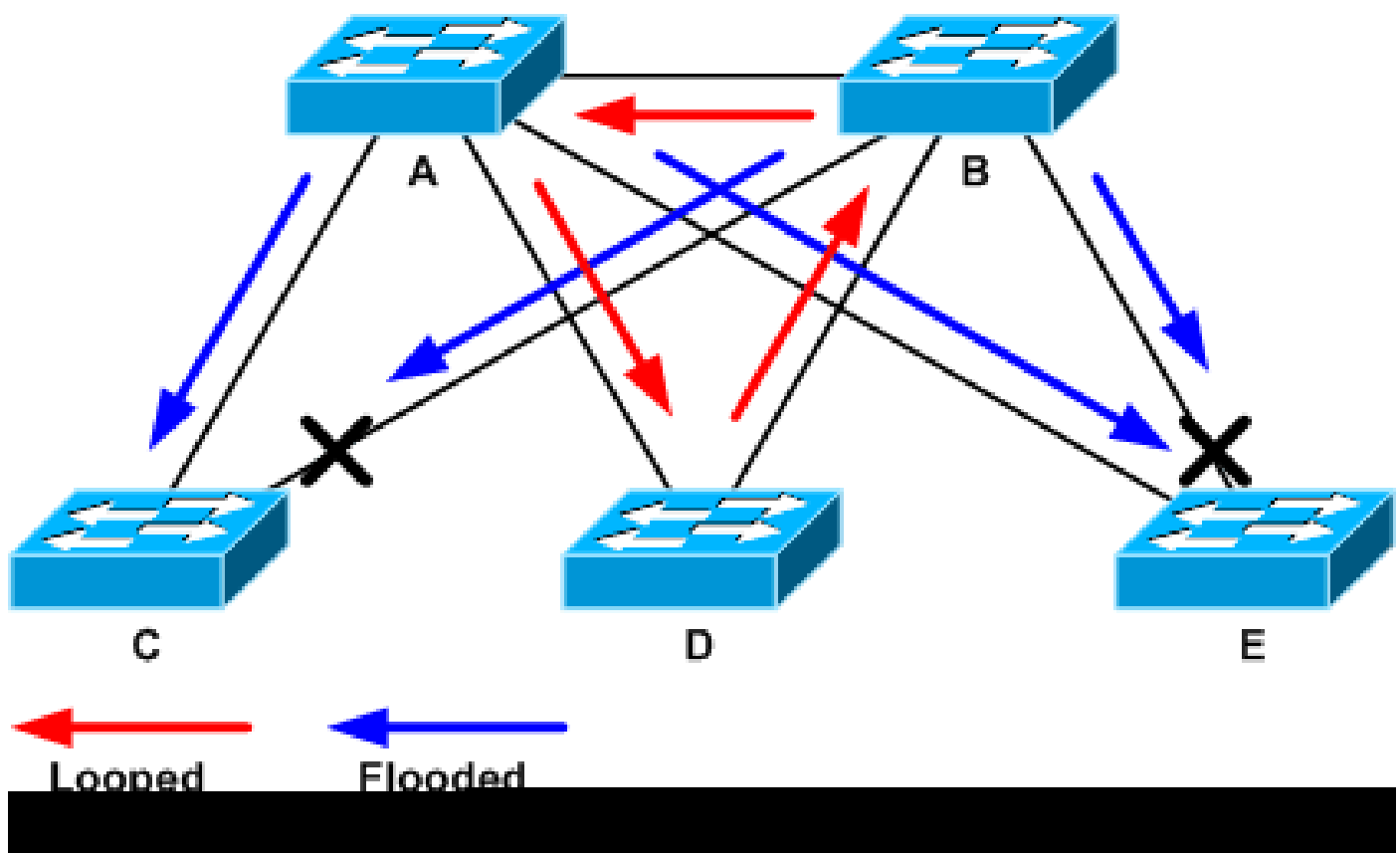
 Remarque : vous n'avez pas besoin d'arrêter ou de déconnecter tous les ports en même temps. Vous pouvez les éteindre une par une. Il est préférable d'arrêter les ports au point

 d'agrégation affecté par la boucle, comme un commutateur de distribution ou de coeur de réseau. Si vous arrêtez tous les ports à la fois et que vous les activez ou les reconnectez un par un, cela ne fonctionne pas ; la boucle est arrêtée et ne peut pas démarrer immédiatement après la reconnexion du port défectueux. Par conséquent, il est difficile de corrélérer la défaillance à un port particulier.

 Remarque : pour rompre la boucle, il est recommandé de collecter des informations avant de redémarrer les commutateurs. Sinon, il sera difficile d'analyser les causes profondes. Après avoir désactivé ou déconnecté chaque port, vous devez vérifier si l'utilisation du fond de panier du commutateur est revenue à un niveau normal.

 Remarque : gardez à l'esprit que les ports ne supportent pas la boucle, mais inondent le trafic qui arrive avec la boucle. Lorsque vous arrêtez de tels ports d'inondation, vous réduisez seulement l'utilisation du fond de panier, mais vous n'arrêtez pas la boucle.

Dans l'exemple de topologie suivant, la boucle est établie entre les commutateurs A, B et D. Par conséquent, les liaisons AB, AD et BD sont maintenues. Si vous arrêtez l'une de ces liaisons, vous arrêtez la boucle. Les liaisons AC, AE, BC et BE inondent simplement le trafic qui arrive avec la boucle.



Trafic en boucle et inondé

Une fois le port de support arrêté, l'utilisation du fond de panier passe à une valeur normale. Vous devez savoir quel port a été arrêté pour que l'utilisation du fond de panier (et celle des autres ports) atteigne un niveau normal. À ce stade, la boucle est arrêtée et le fonctionnement du réseau

s'améliore. Cependant, comme la cause initiale de la boucle n'a pas été corrigée, d'autres problèmes subsistent.

4. Trouver et corriger la cause de la boucle

Une fois la boucle arrêtée, vous devez déterminer la raison pour laquelle elle a commencé. Il s'agit de la partie difficile du processus, car les raisons peuvent varier. Il est également difficile de formaliser une procédure exacte qui fonctionne dans tous les cas.

Directives :

- Examinez le schéma de topologie pour trouver un chemin redondant. Cela inclut le port de support trouvé à l'étape précédente qui revient au même commutateur (les paquets de chemin parlés pendant la boucle). Dans l'exemple de topologie précédent, ce chemin est AD-DB-BA.
- Pour chaque commutateur sur le chemin redondant, vérifiez si le commutateur connaît la racine STP correcte.

Tous les commutateurs d'un réseau L2 doivent s'entendre sur une racine STP commune. Il s'agit d'un symptôme clair de problèmes lorsque les ponts affichent systématiquement un ID différent pour la racine STP dans un VLAN ou une instance STP spécifique. Émettez la commande `show spanning-tree vlan vlan-id` pour afficher l'ID de pont racine pour un VLAN donné :

```
<#root>
```

```
cat#
```

```
show spanning-tree vlan 333
```

```
MST03
```

```
Spanning tree enabled protocol mstp
```

```
Root ID          Priority      32771
  Address        0050.14bb.6000
  Cost           20000
  Port          136 (GigabitEthernet3/8)
  Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID        Priority      32771 (priority 32768 sys-id-ext 3)
  Address        00d0.003f.8800
  Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Interface          Role Sts Cost          Prio.Nbr Status
-----
Gi3/8              Root FWD 20000         128.136 P2p
Po1                Desg FWD 20000         128.833 P2p
```

Le numéro de VLAN peut être trouvé à partir du port, car les ports impliqués dans la boucle ont

été établis dans les étapes précédentes. Si les ports en question sont des agrégations, souvent tous les VLAN sur l'agrégation sont impliqués. Si ce n'est pas le cas (par exemple, s'il apparaît que la boucle s'est produite sur un seul VLAN), vous pouvez essayer d'émettre les interfaces `show | include L2|line|broadcast` command (uniquement sur les moteurs Supervisor 2 et ultérieurs sur les commutateurs de la gamme Catalyst 6500/6000, car Supervisor 1 ne fournit pas de statistiques de commutation par VLAN). Examinez uniquement les interfaces VLAN. Le VLAN avec le plus grand nombre de paquets commutés est souvent celui où la boucle s'est produite :

```
<#root>
```

```
cat#
```

```
show interface | include L2|line|broadcast
```

```
Vlan1 is up, line protocol is up
  L2 Switched: ucast: 653704527 pkt, 124614363025 bytes - mcast:
    23036247 pkt, 1748707536 bytes
    Received 23201637 broadcasts, 0 runts, 0 giants, 0 throttles

Vlan10 is up, line protocol is up
  L2 Switched: ucast: 2510912 pkt, 137067402 bytes - mcast:
    41608705 pkt, 1931758378 bytes
    Received 1321246 broadcasts, 0 runts, 0 giants, 0 throttles

Vlan11 is up, line protocol is up
  L2 Switched: ucast: 73125 pkt, 2242976 bytes - mcast:
    3191097 pkt, 173652249 bytes
    Received 1440503 broadcasts, 0 runts, 0 giants, 0 throttles

Vlan100 is up, line protocol is up
  L2 Switched: ucast: 458110 pkt, 21858256 bytes - mcast:
    64534391 pkt, 2977052824 bytes
    Received 1176671 broadcasts, 0 runts, 0 giants, 0 throttles

Vlan101 is up, line protocol is up
  L2 Switched: ucast: 70649 pkt, 2124024 bytes - mcast:
    2175964 pkt, 108413700 bytes
    Received 1104890 broadcasts, 0 runts, 0 giants, 0 throttles
```

Dans cet exemple, le VLAN 1 représente le plus grand nombre de diffusions et de trafic commuté de couche 2. Assurez-vous que le port racine est correctement identifié.

Le port racine doit avoir le coût le plus faible vers le pont racine (parfois un chemin est plus court en termes de sauts, mais plus long en termes de coût, car les ports à faible vitesse ont des coûts plus élevés). Pour déterminer quel port est considéré comme la racine pour un VLAN donné, émettez la commande `show spanning-tree vlan` :

```
<#root>
```

```
cat#
```

```
show spanning-tree vlan 333
```

MST03

```
Spanning tree enabled protocol mstp
Root ID    Priority    32771
          Address    0050.14bb.6000
          Cost      20000
```

```
Port      136 (GigabitEthernet3/8)
```

```
    Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID Priority    32771 (priority 32768 sys-id-ext 3)
Address    00d0.003f.8800
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Interface	Role	Sts	Cost	Prio.Nbr	Status
-----	----	---	-----	-----	-----
Gi3/8	Root	FWD	20000	128.136	P2p
Po1	Desg	FWD	20000	128.833	P2p

Assurez-vous que les unités BPDU sont reçues régulièrement sur le port racine et sur les ports qui sont censés bloquer.

Les BPDU sont envoyées par le pont racine à chaque intervalle HELLO (deux secondes par défaut). Les ponts non racine reçoivent, traitent, modifient et propagent les unités BPDU reçues de la racine. Émettez la commande `show spanning-tree interface detail` pour voir si les BPDU sont reçues :

```
<#root>
```

```
cat#
```

```
show spanning-tree interface g3/2 detail
```

```
Port 130 (GigabitEthernet3/2) of MST00 is backup blocking
  Port path cost 20000, Port priority 128, Port Identifier 128.130.
  Designated root has priority 0, address 0007.4f1c.e847
  Designated bridge has priority 32768, address 00d0.003f.8800
  Designated port id is 128.129, designated path cost 2000019
  Timers: message age 4, forward delay 0, hold 0
```

```
Number of transitions to forwarding state: 0
```

```
  Link type is point-to-point by default, Internal
  Loop guard is enabled by default on the port
  BPDU: sent 3,
```

```
received 53
```


```
cat#
```

```
show spanning-tree interface g3/2 detail
```

```
Port 130 (GigabitEthernet3/2) of MST00 is backup blocking
  Port path cost 20000, Port priority 128, Port Identifier 128.130.
```

```
Designated root has priority 0, address 0007.4f1c.e847
Designated bridge has priority 32768, address 00d0.003f.8800
Designated port id is 128.129, designated path cost 2000019
Timers: message age 5, forward delay 0, hold 0
Number of transitions to forwarding state: 0
Link type is point-to-point by default, Internal
Loop guard is enabled by default on the port
BPDU: sent 3,
```

received 54

 Remarque : une unité BPDU a été reçue entre les deux sorties de la commande (le compteur est passé de 53 à 54).

Les compteurs représentés sont en fait des compteurs gérés par le processus STP lui-même. Cela signifie que, si les compteurs de réception ont été incrémentés, non seulement la trame BPDU a été reçue par un port physique, mais elle a également été reçue par le processus STP. Si le compteur `received BPDU` n'incrémente pas sur le port qui est censé être le port de secours ou de remplacement racine, vérifiez si le port reçoit des multidiffusions (les BPDU sont envoyées en multidiffusion). Exécutez la commande `show interface interface counters` :

```
<#root>
```

```
cat#
```

```
show interface g3/2 counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi3/2	14873036	2		

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
Gi3/2	114365997	83776	732086	19

```
cat#
```

```
show interface g3/2 counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi3/2	14873677	2		

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
Gi3/2	114365997	83776	732086	19

```
89391
```

0

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
Gi3/2	114366106	83776	732087	19

Une brève description des rôles des ports STP est disponible dans [la section Enhance STP with Loop Guard and BPDU Skew Detection](#) de la section [Spanning-Tree Protocol Enhancements using Loop Guard and BPDU Skew Detection Features](#). Si aucune trame BPDU n'est reçue, vérifiez si le port compte les erreurs. Exécutez la commande `show interface interface counters errors` :

```
<#root>
```

```
cat#
```

```
show interface g4/3 counters errors
```

Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize	OutDiscards
Gi4/3	0	0	0	0	0	0

Port	Single-Col	Multi-Col	Late-Col	Excess-Col	Carri-Sen	Runts	Giants
Gi4/3	0	0	0	0	0	0	0

Il est possible que les BPDU soient reçues par le port physique, mais n'atteignent toujours pas le processus STP. Si les commandes utilisées dans les deux exemples précédents montrent que certaines multidiffusions sont reçues et que les erreurs ne sont pas comptées, vérifiez si les BPDU sont abandonnées au niveau du processus STP. Exécutez la commande à distance `switch test spanning-tree process-stats` sur le Catalyst 6500 :

```
<#root>
```

```
cat#
```

```
remote command switch test spanning-tree process-stats
```

```
-----TX STATS-----
transmission rate/sec      = 2
paks transmitted           = 5011226
paks transmitted (opt)     = 0
opt chunk alloc failures  = 0
max opt chunk allocated    = 0
-----RX STATS-----
```

```
receive rate/sec          = 1
```

```
paks received at stp isr  = 3947627
paks queued at stp isr    = 3947627
```

```
paks dropped at stp isr   = 0
drop rate/sec             = 0
```

```
paks dequeued at stp proc = 3947627
```

```
paks waiting in queue      = 0
queue depth                = 7(max) 12288(total)
-----PROCESSING STATS-----
queue wait time (in ms)   = 0(avg) 540(max)
processing time (in ms)   = 0(avg) 4(max)
proc switch count         = 100
add vlan ports            = 20
time since last clearing   = 2087269 sec
```

La commande utilisée dans cet exemple affiche les statistiques de processus STP. Il est important de vérifier que les compteurs d'abandon n'augmentent pas et que les paquets reçus augmentent. Si les paquets reçus ne sont pas augmentés mais que le port physique ne reçoit pas de multidiffusions, vérifiez que les paquets sont reçus par l'interface intrabande du commutateur (l'interface du processeur). Exécutez la commande à distance `switch show ibc | i rx_input` sur Catalyst 6500/6000 :

```
<#root>
```

```
cat#
```

```
remote command switch show ibc | i rx_input
```

```
rx_inputs=
```

```
5626468
```

```
, rx_cumbytes=859971138
```

```
cat#
```

```
remote command switch show ibc | i rx_input
```

```
rx_inputs=
```

```
5626471
```

```
, rx_cumbytes=859971539
```

Cet exemple montre qu'entre les sorties, le port intrabande a reçu 23 paquets.



Remarque : ces 23 paquets ne sont pas seulement des paquets BPDU ; il s'agit d'un compteur global pour tous les paquets reçus par le port intrabande.

S'il n'y a aucune indication que les BPDU sont abandonnées sur le commutateur ou le port local, vous devez vous déplacer vers le commutateur de l'autre côté de la liaison et vérifier si ce commutateur envoie les BPDU. Vérifiez si les unités BPDU sont envoyées régulièrement sur des ports désignés non racine. Si le rôle de port est identique, le port envoie des BPDU, mais le voisin ne les reçoit pas. Vérifiez si des BPDU sont envoyées. Exécutez la commande `show spanning-tree interface detail` :

<#root>

cat#

```
show spanning-tree interface g3/1 detail
```

Port 129 (GigabitEthernet3/1) of MST00 is

designated

forwarding

Port path cost 20000, Port priority 128, Port Identifier 128.129.
Designated root has priority 0, address 0007.4f1c.e847
Designated bridge has priority 32768, address 00d0.003f.8800
Designated port id is 128.129, designated path cost 2000019
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 0
Link type is point-to-point by default, Internal
Loop guard is enabled by default on the port

BPDUs: sent 1774

, received 1

cat#

```
show spanning-tree interface g3/1 detail
```

Port 129 (GigabitEthernet3/1) of MST00 is

designated


forwarding

Port path cost 20000, Port priority 128, Port Identifier 128.129.
Designated root has priority 0, address 0007.4f1c.e847
Designated bridge has priority 32768, address 00d0.003f.8800
Designated port id is 128.129, designated path cost 2000019
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 0
Link type is point-to-point by default, Internal
Loop guard is enabled by default on the port

BPDUs: sent 1776

, received 1

Dans cet exemple, deux unités BPDUs sont envoyées entre les sorties.

 Remarque : le processus STP gère 1e BPDUs : sentcounter. Cela signifie que le compteur indique que la trame BPDUs a été envoyée vers le port physique et est envoyée. Vérifiez si les compteurs de port augmentent pour les paquets de multidiffusion transmis. Émettez la commande show interface interface counters. Cela peut aider à déterminer le flux de trafic des unités BPDUs.

<#root>

cat#

```
show interface g3/1 counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi3/1	127985312	83776	812319	19

Port	OutOctets	OutUcastPkts
------	-----------	--------------

OutMcastPkts

Port	OutBcastPkts	OutMcastPkts
Gi3/1	131825915	3442

872342

386

cat#

```
show interface g3/1 counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi3/1	127985312	83776	812319	19

Port	OutOctets	OutUcastPkts
------	-----------	--------------

OutMcastPkts

Port	OutBcastPkts	OutMcastPkts
Gi3/1	131826447	3442

872346

386

Avec toutes ces étapes, l'idée est de trouver le commutateur ou la liaison où les BPDU ne sont pas reçues, envoyées ou traitées. Il est possible que le STP ait calculé l'état correct pour le port, mais en raison d'un problème de plan de contrôle, il ne peut pas définir cet état sur le matériel de transfert. Une boucle peut être créée si le port n'est pas bloqué au niveau matériel. Si vous pensez qu'il s'agit d'un problème dans votre réseau, [contactez le support technique Cisco](#) pour obtenir de l'aide.

5. Restaurer la redondance

Une fois le périphérique ou la liaison à l'origine de la boucle détecté, ce périphérique doit être isolé du réseau ou le problème doit être résolu (par exemple, remplacer la fibre optique ou le GBIC). Les liaisons redondantes, déconnectées à l'étape 3, doivent être restaurées.


Il est important de ne pas manipuler le périphérique ou la liaison à l'origine de la boucle, car de nombreuses conditions conduisant à une boucle sont transitoires, intermittentes et instables. Cela signifie que, si la condition est effacée dans ou après l'enquête, la condition ne se produit pas pendant un certain temps ne se produit pas ou pas du tout. La condition doit être enregistrée afin que l'[assistance technique Cisco](#) puisse l'étudier plus en détail. Il est important de collecter des informations sur la condition avant de réinitialiser les commutateurs. Si une condition n'est plus

présente, il est impossible de déterminer la cause première de la boucle. Si vous collectez les informations, vous vous assurez que ce problème ne provoque pas à nouveau la boucle. Pour plus d'informations, référez-vous à [Sécurisation du réseau contre les boucles de transfert](#).

Examen des modifications topologiques

Le rôle du mécanisme de modification de topologie (TC) est de corriger les tables de transfert L2 après la modification de la topologie. Cela est nécessaire pour éviter une panne de connectivité, car les adresses MAC précédemment accessibles via des ports particuliers peuvent changer et devenir accessibles via différents ports. TC raccourcit l'âge de la table de transfert sur tous les commutateurs du VLAN où le TC se produit. Ainsi, si l'adresse n'est pas réapprise, elle expire et une inondation se produit pour garantir que les paquets atteignent l'adresse MAC de destination.

Le TC est déclenché par le changement de l'état STP d'un port à ou de l'état STP forwarding state. Après TC, même si l'adresse MAC de destination particulière a expiré, l'inondation ne se poursuit pas longtemps. L'adresse est réapprise par le premier paquet provenant de l'hôte dont l'adresse MAC a expiré. Le problème peut survenir lorsque TC se produit de façon répétée, avec de courts intervalles. Les commutateurs vieillissent constamment et rapidement leurs tables de transfert, de sorte que l'inondation peut être presque constante.

 Remarque : avec le protocole Rapid STP ou Multiple STP (IEEE 802.1w et IEEE 802.1s), TC est déclenché par un changement de l'état du port vers forwarding, ainsi que par le changement de rôle de designated root. Avec le protocole STP rapide, la table de transfert L2 est immédiatement vidée, contrairement à la norme 802.1d, qui réduit le temps de vieillissement. Le vidage immédiat de la table de transfert restaure la connectivité plus rapidement, mais peut provoquer davantage de diffusion

TC est un événement rare dans un réseau bien configuré. Lorsqu'une liaison sur un port de commutateur est activée ou désactivée, il y a finalement un TC, une fois que l'état STP du port est changé en forwarding ou from forwarding. Lorsque le port est instable, cela peut provoquer des CT répétitifs et une inondation.

Les ports avec la fonctionnalité STP portfast activée ne peuvent pas provoquer de TC lorsqu'ils passent à ou à partir de l'état forwarding. La configuration de portfast sur tous les ports des périphériques finaux (tels que les imprimantes, les PC et les serveurs) peut limiter les TC à une faible quantité et est fortement recommandée.

S'il y a des CT répétitifs sur le réseau, vous devez identifier la source de ces CT et prendre des mesures pour les réduire, afin de réduire au minimum l'inondation.

Avec la norme 802.1d, les informations STP relatives à un événement TC sont propagées entre les ponts via une notification TC (TCN), qui est un type spécial de BPDU. Si vous suivez les ports qui reçoivent les BPDU TCN, vous pouvez trouver le périphérique à l'origine des TC.

Trouver la cause de l'inondation

Vous pouvez déterminer qu'il y a inondation en raison de performances lentes, abandons de paquets sur des liaisons qui ne sont pas censées être encombrées et l'analyseur de paquets affiche plusieurs paquets de monodiffusion vers la même destination qui ne se trouve pas sur le segment local. Pour plus d'informations sur l'inondation de monodiffusion, référez-vous à [Inondation de monodiffusion dans les réseaux de campus commutés](#).

Sur un Catalyst 6500/6000 qui exécute le logiciel Cisco IOS, vous pouvez vérifier le compteur du moteur de transfert (uniquement sur le moteur Supervisor 2) pour estimer la quantité d'inondation. Exécutez la commande à distance switch show earl statistics | i MISS_DA|ST_FRcommand:

```
<#root>
```

```
cat#
```

```
remote command switch show earl statistics | i MISS_DA|ST_FR
```

```
ST_MISS_DA      =      18          530308834
ST_FRMS         =      97          969084354
```

```
cat#
```

```
remote command switch show earl statistics | i MISS_DA|ST_FR
```

```
ST_MISS_DA      =       4          530308838
ST_FRMS         =      23          969084377
```

Dans cet exemple, la première colonne indique la modification depuis la dernière exécution de cette commande et la seconde la valeur cumulée depuis le dernier redémarrage. La première ligne indique la quantité de trames inondées et la seconde, la quantité de trames traitées. Si les deux valeurs sont proches l'une de l'autre, ou si la première valeur augmente à un taux élevé, il est possible que le commutateur inonde le trafic. Cependant, cela ne peut être utilisé qu'en conjonction avec d'autres moyens de vérifier l'inondation, car les compteurs ne sont pas granulaires. Il y a un compteur par commutateur, et non par port ou VLAN. Il est normal de voir certains paquets inondés, car le commutateur peut toujours inonder si l'adresse MAC de destination ne figure pas dans la table de transfert. Cela peut être le cas lorsque le commutateur reçoit un paquet avec une adresse de destination qui n'a pas encore été apprise.

Trouver la source des CT

Si le numéro de VLAN est connu pour le VLAN où une inondation excessive se produit, vérifiez les compteurs STP pour voir si le nombre de TC est élevé ou augmente régulièrement. Émettez la commande show spanning-tree vlan id-vlan detail (dans cet exemple, VLAN 1 est utilisé) :

```
<#root>
```

```
cat#
```

```
show spanning-tree vlan 1 detail
```

```
VLAN0001 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 0007.0e8f.04c0
Configured hello time 2, max age 20, forward delay 15
Current root has priority 0, address 0007.4f1c.e847
Root port is 65 (GigabitEthernet2/1), cost of root path is 119
Topology change flag not set, detected flag not set
```


```
Number of topology changes 1 last change occurred 00:00:35 ago
from GigabitEthernet1/1
```

```
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300
```

Si le numéro de VLAN est inconnu, vous pouvez utiliser l'analyseur de paquets ou vérifier les compteurs TC pour tous les VLAN.

Prendre des mesures pour prévenir les TC excessifs

Vous pouvez surveiller le nombre de compteurs de modifications de topologie pour voir s'il augmente régulièrement. Ensuite, passez au pont qui est connecté au port qui est représenté, pour recevoir le dernier TC (dans l'exemple précédent, le port GigabitEthernet1/1) et voir d'où vient le TC pour ce pont. Ce processus doit être répété jusqu'à ce que le port de la station d'extrémité sans STP portfast activé soit trouvé, ou jusqu'à ce que la liaison instable qui doit être corrigée soit trouvée. Toute la procédure doit être répétée si les CT proviennent d'autres sources. Si la liaison appartient à un hôte d'extrémité, vous pouvez configurer la fonctionnalité portfast pour empêcher la génération de TC.

 Remarque : dans l'implémentation STP du logiciel Cisco IOS, le compteur pour les TC ne peut s'incrémenter que si une BPDU TCN est reçue par un port dans un VLAN. Si une BPDU de configuration normale avec un indicateur TC défini est reçue, alors le compteur TC n'est pas incrémenté. Cela signifie que, si vous suspectez un TC d'être la raison de l'inondation, commencez à rechercher les sources pour le TC à partir du pont racine STP dans ce VLAN. Il peut contenir les renseignements les plus précis sur le nombre et la source des CT.

Résolution des problèmes liés au temps de convergence

Dans certains cas, le fonctionnement réel du protocole STP ne correspond pas au comportement attendu. Voici les deux problèmes les plus fréquents :

- La convergence ou la reconvergence STP prend plus de temps que prévu.
- Le résultat de la topologie est différent de celui attendu.


Le plus souvent, voici les raisons de ce comportement :

- Non-concordance entre la topologie réelle et la topologie documentée.
- Mauvaise configuration, telle qu'une configuration incohérente des compteurs STP, un diamètre STP qui augmente ou une mauvaise configuration de portfast.
- CPU de commutateur surchargé pendant la convergence ou la reconvergence.
- Défaut logiciel.

Comme mentionné précédemment, ce document ne peut fournir que des directives générales pour le dépannage, en raison de la grande variété de problèmes qui pourraient affecter le STP. Pour comprendre pourquoi la convergence prend plus de temps que prévu, examinez la séquence des événements STP pour savoir ce qui se passe et dans quel ordre. Étant donné que l'implémentation STP dans le logiciel Cisco IOS ne consigne pas les résultats (à l'exception d'événements spécifiques, tels que des incohérences de port), vous pouvez utiliser le logiciel Cisco IOS pour déboguer STP afin d'obtenir une vue plus claire. Pour STP, avec un Catalyst 6500/6000 qui exécute le logiciel Cisco IOS, le traitement est effectué sur le processeur de commutation (SP) (ou Supervisor), de sorte que les débogages doivent être activés sur le SP. Pour les groupes de ponts de la plate-forme logicielle Cisco IOS, le traitement est effectué sur le processeur de routage (RP), de sorte que les débogages doivent être activés sur le RP (MSFC).

Utiliser les commandes de débogage STP

De nombreuses commandes STPdebug sont destinées à l'ingénierie du développement. Ils ne fournissent aucun résultat significatif pour une personne sans connaissance détaillée de l'implémentation STP dans le logiciel Cisco IOS. Certains débogages peuvent fournir une sortie qui est instantanément lisible, comme des changements d'état de port, des changements de rôle, des événements tels que des TC, et un vidage des BPDU reçues et transmises. Cette section ne fournit pas une description complète de tous les débogages, mais présente plutôt brièvement les plus fréquemment utilisés.

 Remarque : lorsque vous utilisez des commandes debug, activez le minimum de débogages nécessaires. Si les débogages en temps réel ne sont pas nécessaires, enregistrez le résultat dans le journal plutôt que de l'imprimer sur la console. Des débogages excessifs peuvent surcharger le processeur et perturber le fonctionnement du commutateur.

Pour diriger la sortie de débogage vers le journal plutôt que vers la console ou vers les sessions Telnet, émettez les commandes `logging console information` et `no logging monitor` en mode de configuration globale. Pour voir le journal des événements généraux, émettez la commande `debug spanning-tree event` pour Per VLAN Spanning-Tree (PVST) et Rapid-PVST. C'est le premier débogage qui donne des informations sur ce qui s'est passé avec le STP. En mode Multiple Spanning-Tree (MST), il n'est pas possible d'émettre la commande `debug spanning-tree event`. Par conséquent, émettez la commande `debug spanning-tree mstp roles` pour voir les changements de rôle de port. Pour voir les changements d'état STP du port, émettez la commande `debug spanning-tree switch state` avec la commande `debug pm vp`:

<#root>

cat-sp#

debug spanning-tree switch state

Spanning Tree Port state changes debugging is on

cat-sp#

debug pm vp

Virtual port events debugging is on

Nov 19 14:03:37: SP: pm_vp 3/1(333): during state forwarding, got event 4(remove)

Nov 19 14:03:37: SP:

@@@

pm_vp 3/1(333):

forwarding -> notforwarding

port 3/1 (was forwarding) goes down in vlan 333

Nov 19 14:03:37: SP: *** vp_fwdchange: single: notfwd: 3/1(333)

Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): notforwarding -> present

Nov 19 14:03:37: SP: *** vp_linkchange: single: down: 3/1(333)

Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): present -> not_present

Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/1(333)

Nov 19 14:03:37: SP: pm_vp 3/2(333): during state notforwarding,
got event 4(remove)

Nov 19 14:03:37: SP:

@@@

pm_vp 3/2(333): notforwarding -> present

Nov 19 14:03:37: SP: *** vp_linkchange: single: down: 3/2(333)

Port 3/2 (was not forwarding) in vlan 333 goes down

Nov 19 14:03:37: SP: @@@ pm_vp 3/2(333): present -> not_present

Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/2(333)

Nov 19 14:03:53: SP: pm_vp 3/1(333): during state not_present,
got event 0(add)

Nov 19 14:03:53: SP: @@@ pm_vp 3/1(333): not_present -> present

Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/1(333)

Nov 19 14:03:53: SP: pm_vp 3/1(333): during state present,
got event 8(linkup)

Nov 19 14:03:53: SP:

@@@

pm_vp 3/1(333): present ->

notforwarding

Nov 19 14:03:53: SP: STP SW: Gi3/1 new blocking req for 0 vlans

Nov 19 14:03:53: SP: *** vp_linkchange: single: up: 3/1(333)

Port 3/1 link goes up and blocking in vlan 333

```
Nov 19 14:03:53: SP: pm_vp 3/2(333): during state not_present,  
got event 0(add)  
Nov 19 14:03:53: SP: @@@ pm_vp 3/2(333): not_present -> present  
Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/2(333)
```

```
Nov 19 14:03:53: SP: pm_vp 3/2(333): during state present,  
got event 8(linkup)  
Nov 19 14:03:53: SP:
```

@@@

```
pm_vp 3/2(333): present ->  
notforwarding
```

```
Nov 19 14:03:53: SP: STP SW: Gi3/2 new blocking req for 0 vlans  
Nov 19 14:03:53: SP: *** vp_linkchange: single: up: 3/2(333)
```

Port 3/2 goes up and blocking in vlan 333

```
Nov 19 14:04:08: SP: STP SW: Gi3/1 new learning req for 1 vlans  
Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 0 vlans  
Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 1 vlans  
Nov 19 14:04:23: SP: pm_vp 3/1(333): during state notforwarding,  
got event 14(forward_notnotify)  
Nov 19 14:04:23: SP:
```

```
@@@ pm_vp 3/1(333): notforwarding ->  
forwarding
```

```
Nov 19 14:04:23: SP: *** vp_list_fwdchange: forward: 3/1(333)
```

Port 3/1 goes via learning to forwarding in vlan 333

Pour comprendre pourquoi le protocole STP se comporte d'une certaine manière, il est souvent utile de voir les BPDU qui sont reçues et envoyées par le commutateur :

```
<#root>
```

```
cat-sp#
```

```
debug spanning-tree bpdu receive
```

Spanning Tree BPDU Received debugging is on

```
Nov 6 11:44:27: SP: STP: VLAN1 rx BPDU: config protocol = ieee,  
packet from GigabitEthernet2/1 , linktype IEEE_SPANNING ,  
enctype 2, encsize 17
```

```
Nov 6 11:44:27: SP: STP: enc 01 80 C2 00 00 00 06 52 5F 0E 50 00 26 42 42 03
```

```
Nov 6 11:44:27: SP: STP: Data 000000000000000074F1CE8470000001380480006525F0E4  
080100100140002000F00
```

```
Nov 6 11:44:27: SP: STP: VLAN1 Gi2/1:0000 00 00 00 000000074F1CE847 00000013  
80480006525F0E40 8010 0100 1400 0200 0F00
```

Ce débogage fonctionne pour les modes PVST, Rapid-PVST et MST ; mais il ne décode pas le contenu des BPDU. Cependant, vous pouvez l'utiliser pour vous assurer que les BPDU sont

reçues. Pour voir le contenu de la BPDU, émettez la commande debug spanning-tree switch rx decodecmd avec la commande debug spanning-tree switch rx process pour PVST et Rapid-PVST. Émettez la commande debug spanning-tree mstp bpdu-rx pour voir le contenu de la BPDU pour MST :

```
<#root>
```

```
cat-sp#
```

```
debug spanning-tree switch rx decode
```

```
Spanning Tree Switch Shim decode received packets debugging is on
```

```
cat-sp#
```

```
debug spanning-tree switch rx process
```

```
Spanning Tree Switch Shim process receive bpdu debugging is on
```

```
Nov 6 12:23:20: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026
Nov 6 12:23:20: SP:      encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1
Nov 6 12:23:20: SP:      42 42 03 SPAN
Nov 6 12:23:20: SP:      CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013
Nov 6 12:23:20: SP:      B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00

Nov 6 12:23:22: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026
Nov 6 12:23:22: SP:      encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1
Nov 6 12:23:22: SP:      42 42 03 SPAN
Nov 6 12:23:22: SP:      CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013
Nov 6 12:23:22: SP:      B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00
```

Pour le mode MST, vous pouvez activer le décodage BPDU détaillé avec cette commande debug:

```
<#root>
```

```
cat-sp#
```

```
debug spanning-tree mstp bpdu-rx
```

```
Multiple Spanning Tree Received BPDUs debugging is on
```

```
Nov 19 14:37:43: SP: MST:BPDU DUMP [
```


```
rcvd_bpdu Gi3/2
```

```
Repeated]
```

```
Nov 19 14:37:43: SP: MST:   Proto:0 Version:3 Type:2 Role: DesgFlags[   F   ]
Nov 19 14:37:43: SP: MST:   Port_id:32897 cost:2000019
Nov 19 14:37:43: SP: MST:   root_id   :0007.4f1c.e847 Prio:0
Nov 19 14:37:43: SP: MST:   br_id    :00d0.003f.8800 Prio:32768
Nov 19 14:37:43: SP: MST:   age:2 max_age:20 hello:2 fwdelay:15
Nov 19 14:37:43: SP: MST:   V3_len:90 PathCost:30000 region:STATIC rev:1
Nov 19 14:37:43: SP: MST:   ist_m_id :0005.74
Nov 19 14:37:43: SP: MST:BPDU DUMP [
```

```
rcvd_bpdu Gi3/2
```

```
Repeated]
Nov 19 14:37:43: SP: MST: Proto:0 Version:3 Type:2 Role: DesgFlags[ F ]
Nov 19 14:37:43: SP: MST: Port_id:32897 cost:2000019
Nov 19 14:37:43: SP: MST: root_id :0007.4f1c.e847 Prio:0
Nov 19 14:37:43: SP: MST: br_id :00d0.003f.8800 Prio:32768
Nov 19 14:37:43: SP: MST: age:2 max_age:20 hello:2 fwdelay:15
Nov 19 14:37:43: SP: MST: V3_len:90 PathCost:30000 region:STATIC rev:1
Nov 19 14:37:43: SP: MST: ist_m_id :0005.7428.1440 Prio:32768 Hops:18
Num Mrec: 1
Nov 19 14:37:43: SP: MST: stci=3 Flags[ F ] Hop:19 Role:Desg [Repeated]
Nov 19 14:37:43: SP: MST: br_id:00d0.003f.8800 Prio:32771 Port_id:32897
Cost:2000028.1440 Prio:32768 Hops:18 Num Mrec: 1
Nov 19 14:37:43: SP: MST: stci=3 Flags[ F ] Hop:19 Role:Desg [Repeated]
Nov 19 14:37:43: SP: MST: br_id:00d0.003f.8800 Prio:32771 Port_id:32897
Cost:20000
```

 Remarque : pour le logiciel Cisco IOS version 12.1.13E et ultérieure, les débogages conditionnels pour STP sont pris en charge. Cela signifie que vous pouvez déboguer les BPDU qui sont reçues ou transmises par port ou par VLAN.

Émettez les commandes `debug condition vlan vlan_num` ou `debug condition interface interface` pour limiter l'étendue de la sortie de débogage à per-interface ou per-VLAN.

Sécurisation du réseau contre les boucles de transfert

Cisco a développé un certain nombre de fonctionnalités et d'améliorations pour protéger les réseaux contre les boucles de transfert lorsqu'un STP ne peut pas gérer certaines pannes.

Lorsque vous dépannez le STP, il permet d'isoler et éventuellement de trouver la cause d'une défaillance particulière, tandis que la mise en oeuvre de ces améliorations est la seule façon de sécuriser le réseau contre les boucles de transfert.

Voici quelques méthodes de protection de votre réseau contre les boucles de transfert :


1. Activez la détection de liaison unidirectionnelle (UDLD) sur toutes les liaisons de commutateur à commutateur

Pour plus d'informations sur UDLD, référez-vous [à Compréhension et configuration de la fonctionnalité de protocole de détection de liaison unidirectionnelle](#).


2. Activez la protection contre les boucles sur tous les commutateurs

Pour plus d'informations sur la protection contre les boucles, référez-vous [à Améliorations du protocole Spanning Tree à l'aide de la protection contre les boucles et des fonctions de détection de distorsion BPDU](#).

Lorsqu'elles sont activées, UDLD et Loop Guard éliminent la majorité des causes des boucles de transfert. Plutôt que de créer une boucle de transfert, la liaison défectueuse (ou toutes les liaisons dépendant du matériel défectueux) est arrêtée ou bloquée.


 Remarque : bien que ces deux fonctionnalités semblent quelque peu redondantes, chacune possède ses propres fonctionnalités. Par conséquent, utilisez les deux fonctions en même temps pour fournir le niveau de protection le plus élevé. Pour une comparaison détaillée de UDLD et Loop Guard, référez-vous [à Loop Guard vs. Unidirectional Link Detection](#).

Il y a différentes opinions quant à savoir si vous devez utiliser UDLD agressif ou normal. L'UDLD agressif ne peut pas fournir une protection plus grande contre les boucles par rapport à l'UDLD en mode normal. UDLD agressif détecte les scénarios de blocage de port (lorsque la liaison est active, mais qu'il n'y a pas de trous noirs associés au trafic). L'inconvénient de cette fonctionnalité supplémentaire est qu'UDLD agressif peut potentiellement désactiver des liaisons lorsqu'aucune défaillance cohérente n'est présente. Souvent, les gens confondent la modification de l'intervalle UDLDhellointerval avec la fonctionnalité UDLD agressive. C'est incorrect. Les minuteurs peuvent être modifiés dans les deux modes UDLD.

 Remarque : dans de rares cas, UDLD agressif peut arrêter tous les ports de liaison ascendante, ce qui isole essentiellement le commutateur du reste du réseau. Par exemple, cela peut se produire lorsque les deux commutateurs en amont connaissent une utilisation extrêmement élevée du CPU et que le mode agressif UDLD est utilisé. Par conséquent, il est recommandé de configurer des délais d'attente qui ne peuvent pas s'éroder, si le commutateur n'a pas de gestion hors bande en place.

3. Activez Portfast sur tous les ports des stations d'extrémité

Vous devez activer portfast pour limiter la quantité de TC et l'inondation subséquente, ce qui peut affecter les performances du réseau. Utilisez cette commande uniquement avec les ports qui se connectent aux stations d'extrémité. Sinon, une boucle topologique accidentelle peut provoquer une boucle de paquets de données et perturber le fonctionnement du commutateur et du réseau.

 Attention : soyez prudent lorsque vous utilisez la commande no spanning-tree portfast. Cette commande supprime uniquement les commandes portfast spécifiques à un port. Cette commande active implicitement portfast si vous définissez la commande spanning-tree portfast default en mode de configuration globale et si le port n'est pas un port trunk. Si vous ne configurez pas portfast globalement, la commande no spanning-tree portfast est équivalente à la commande spanning-tree portfast disable.

4. Définissez EtherChannels sur `Desirable` Mode on Both Sides (where supported) et `Non-silent` Option

Le mode souhaitable peut activer le protocole PAgP (Port Aggregation Protocol) pour assurer la cohérence du temps d'exécution entre les homologues de canalisation. Cela offre un degré supplémentaire de protection contre les boucles, en particulier lors des reconfigurations de canaux (par exemple, lorsque des liaisons rejoignent ou quittent le canal, et lors de la détection d'une défaillance de liaison). Il existe une fonction intégrée de protection contre les erreurs de configuration des canaux, activée par défaut, qui empêche les boucles de transfert en raison d'une

mauvaise configuration des canaux ou d'autres conditions. Pour plus d'informations sur cette fonctionnalité, référez-vous [à Présentation de la détection d'incohérence EtherChannel](#).

5. Ne désactivez pas la négociation automatique (si elle est prise en charge) sur les liaisons commutateur à commutateur

Les mécanismes de négociation automatique peuvent transmettre des informations sur les pannes à distance, ce qui constitue le moyen le plus rapide de détecter les pannes du côté distant. Si une défaillance est détectée sur le côté distant, le côté local désactive la liaison même si celle-ci reçoit des impulsions. Par rapport aux mécanismes de détection de haut niveau tels qu'UDLD, la négociation automatique est extrêmement rapide (en quelques microsecondes), mais elle n'offre pas la couverture de bout en bout d'UDLD (comme le chemin de données complet : CPU - logique de transfert - port1 - port2 - logique de transfert - CPU contre port1 - port2). Le mode UDLD agressif fournit des fonctionnalités similaires à celles de la négociation automatique en ce qui concerne la détection de défaillance. Lorsque la négociation est prise en charge des deux côtés de la liaison, il n'est pas nécessaire d'activer le mode agressif UDLD.

6. Faites attention lorsque vous réglez les compteurs STP

Les compteurs STP dépendent les uns des autres et de la topologie du réseau. Le protocole STP ne fonctionne pas correctement avec les modifications arbitraires apportées aux minuteurs. Pour plus d'informations sur les compteurs STP, référez-vous [à Présentation et réglage des compteurs du protocole Spanning Tree](#).

7. Si des attaques par déni de service sont possibles, sécurisez le périmètre STP du réseau avec Root Guard

Root Guard et BPDU Guard vous permettent de sécuriser le protocole STP contre toute influence extérieure. Si une telle attaque est possible, la protection de la racine et la protection BPDU doivent être utilisées pour protéger le réseau. Pour plus d'informations sur Root Guard et BPDU Guard, reportez-vous aux documents suivants :

- [Amélioration de la protection de la racine du protocole Spanning Tree](#)
- [Amélioration de la protection des BPDU en PortFast pour le spanning tree](#)

8. Activez la protection BPDU sur les ports compatibles Portfast, pour empêcher le protocole STP d'être affecté par des périphériques réseau non autorisés (tels que des concentrateurs, des commutateurs et des routeurs de pontage) connectés aux ports

Si vous configurez Root Guard correctement, cela empêche le STP d'avoir une influence de l'extérieur. Si la protection BPDU est activée, elle arrête les ports qui reçoivent des BPDU. Cela est utile pour enquêter sur les incidents, car BPDU Guard produit le message syslog et arrête le port. Si les protections de la racine ou des unités BPDU n'empêchent pas les boucles de cycle court, deux ports activés rapidement se connectent directement ou via le concentrateur.

9. Éviter le trafic utilisateur sur le VLAN de gestion

Le VLAN de gestion est confiné à un bloc de construction, pas à l'ensemble du réseau.

L'interface de gestion du commutateur reçoit des paquets de diffusion sur le VLAN de gestion. Si des diffusions excessives se produisent (telles qu'une tempête de diffusion ou une application défailante), le processeur du commutateur peut devenir surchargé, ce qui pourrait éventuellement perturber le fonctionnement du protocole STP.

10. Un emplacement racine STP prédictible (codé en dur) et racine STP de secours

La racine STP et la racine STP de sauvegarde doivent être configurées de sorte que la convergence, en cas de panne, se produise de manière prévisible et crée une topologie optimale dans chaque scénario. Ne laissez pas la priorité STP à la valeur par défaut, pour éviter la sélection imprévisible du commutateur racine.

Informations connexes

- [Support pour les produits LAN](#)
- [Prise en charge de la technologie de commutation LAN](#)

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.