Dépannage STP sur les commutateurs Catalyst exécutant le logiciel système Cisco IOS

Contenu

Introduction

Ce document fournit des instructions pour employer le logiciel Cisco IOS® pour dépanner des problèmes avec le protocole Spanning-Tree (STP). Il y a des commandes spécifiques qui s'appliquent au Catalyst 6500/6000 seulement; cependant, vous pouvez appliquer la plupart des principes à n'importe quel commutateur Cisco Catalyst qui exécute le logiciel Cisco IOS.

La plupart de dépannage STP tourne environ trois questions :

- boucles de transfert
- inondation excessive due à un haut débit de changements de topologie STP (comité technique)
- problème lié au temps de convergence

Puisque la transition n'a aucun mécanisme à dépister si un certain paquet est expédié de plusieurs périodes (par exemple, un Time to Live IP [TTL] est utilisée pour jeter le trafic qui circule trop long dans le réseau), seulement un chemin peut exister entre deux périphériques dans le même domaine de la couche 2 (L2).

Le but de STP est de bloquer les ports redondants basés sur un algorithme STP, pour résoudre la topologie physique redondante dans une topologie comme une arborescence. Une boucle de transfert (telle qu'une boucle STP) se produit quand aucun port en topologie redondante n'est bloqué, et le trafic est expédiée en cercles indéfiniment.

Une fois que les débuts de boucle de transfert, il congestionneront vraisemblablement les liens de bas-bande passante le long de son chemin — si tous les liens sont de la même bande passante,

tous les liens sera vraisemblablement congestionnée. Cet encombrement entraînera la perte de paquets et mènera à une situation de réseau vers le bas dans le domaine L2 affecté.

Avec l'inondation excessive, les symptômes ne pourraient pas être comme évidents. Quelques liens lents pourraient devenir congestionnés par le trafic propagé, et les périphériques ou les utilisateurs derrière ces liaisons encombrées pourraient éprouver la lenteur ou la perte de connectivité totale.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Divers types de spanning-tree et comment les configurer. Référez-vous à configurer le pour en savoir plus STP et d'IEEE 802.1s MST.
- Diverses caractéristiques de spanning-tree et comment les configurer. Référez-vous à configurer le pour en savoir plus de caractéristiques STP.

Composants utilisés

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

- Catalyst 6500 avec l'engine du superviseur 2
- Logiciel Cisco IOS Version 12.1(13)E

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.

Pourquoi STP échoue

STP assure des suppositions au sujet de son environnement d'exploitation. Ce sont les suppositions les plus concernant ce document :

- Chaque lien entre les deux passerelles est bidirectionnel. Ceci signifie que, si A se connecte directement à B, alors A recevra ce que B a envoyé et B recevra ce qu'A a envoyé, tant que le lien est en hausse entre elles.
- Chaque passerelle qui exécute STP peut régulièrement recevoir, traiter, et transmettre les Bridges Protocol Data Unit STP (BPDU), également connus sous le nom de paquets STP.

Tandis que ces suppositions semblent logiques et évidentes, il y a des situations quand elles ne sont pas rencontrées. La plupart de ces situations impliquent un certain tri de problème de

matériel ; cependant, les erreurs de logiciel peuvent également mener aux pannes STP. Diverses défaillances matérielles, mauvaises configurations, ou cause miscabling la majorité de pannes STP, alors que les pannes de logiciel expliquent la minorité. Les pannes STP peuvent également se produire en raison des connexions supplémentaires inutiles qui existent entre les Commutateurs. Les VLAN entrent dans un état d'indisponibilité en raison de ces connexions supplémentaires. Pour résoudre ce problème, enlevez toutes les connexions non désirées entre les Commutateurs.

Quand une de ces suppositions n'est pas rencontrée, un ou plusieurs passerelles pourraient plus recevoir ou ne traiter les BPDU. Ceci signifie que la passerelle (ou les passerelles) ne pourra pas découvrir la topologie du réseau. Sans connaissance de la topologie correcte, le commutateur ne peut pas bloquer les boucles. Par conséquent, le trafic propagé circulera au-dessus de la topologie faite une boucle, consommera toute la bande passante, et réduira le réseau.

Les exemples de pourquoi les Commutateurs peuvent ne pas recevoir des BPDU incluent de mauvais émetteurs-récepteurs ou convertisseurs d'interface de gigabit (GBIC), problèmes de câblage, ou défaillances matérielles sur le port, le linecard, ou l'engine de superviseur. Une raison fréquente pour des pannes STP est un lien unidirectionnel entre les passerelles. En une telle condition, une passerelle envoie des BPDU, mais la passerelle en aval ne les reçoit jamais. Le traitement STP peut également être perturbé par une CPU surchargée (99 pour cent ou plus), parce que le commutateur ne peut pas traiter des BPDU reçus. Des BPDU peuvent être corrompus le long du chemin d'une passerelle à l'autre, qui empêche également le comportement approprié STP.

Hormis les boucles de transfert, quand aucun port n'est bloqué, il y a des situations quand seulement certains paquets sont inexactement expédiés par les ports de blocage. Dans la plupart des cas, ceci est provoqué par par des problèmes logiciels. Un tel comportement pourrait entraîner des « lent-boucles. » Ceci signifie que quelques paquets sont faits une boucle, mais la majorité du trafic traverse toujours le réseau, parce que les liens ne sont pas probablement congestionnés.

Les sections restantes dans ce document fournissent des instructions pour dépanner les questions liées STP les plus communes.

Dépannage des boucles de transfert

Les boucles de transfert varient considérablement chacun des deux dans leur origine (cause) et les effectuent. En raison de la large variété de questions qui peuvent affecter STP, ce document peut seulement fournir des directives générales au sujet de la façon dépanner des boucles de transfert.

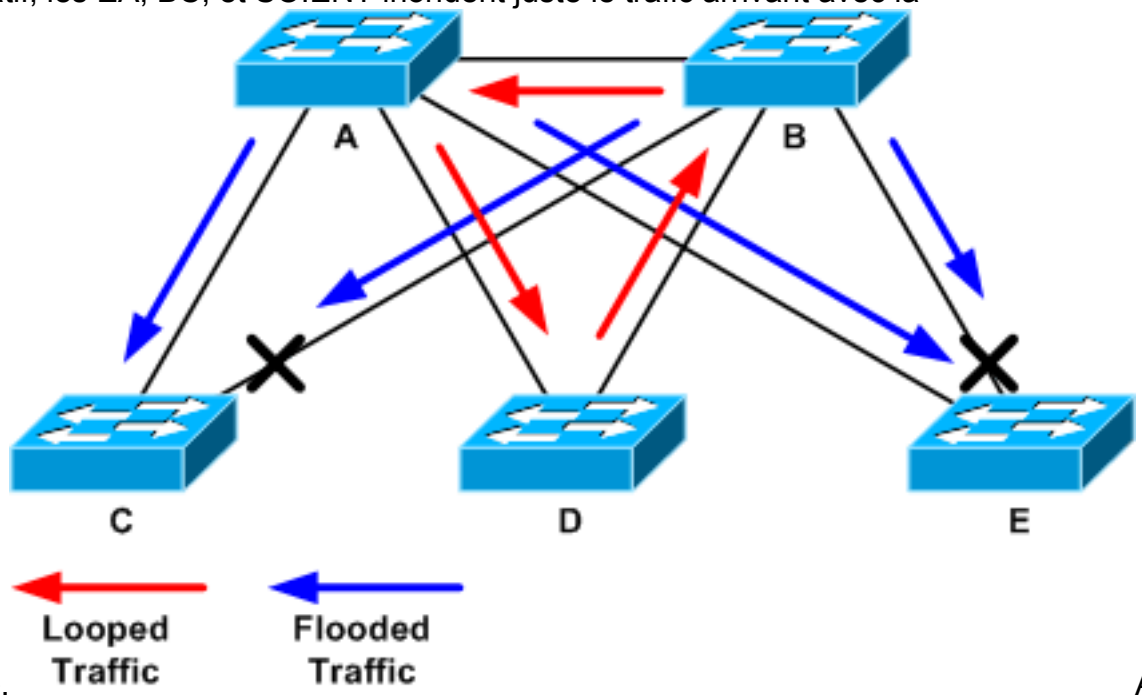
Avant que vous commenciez à dépanner, vous devez obtenir ces informations :

- Un diagramme de topologie réel qui détaille tous les Commutateurs et passerelles
- Leurs numéros de port (de interconnexion) correspondants
- Détails de configuration STP, tels que lesquels le commutateur est la racine et la racine de sauvegarde, que les liens ont un coût ou une priorité de non-par défaut, et l'emplacement des ports de blocage

Généralement, le dépannage implique ces étapes (selon la situation, quelques étapes peuvent ne pas être nécessaires) :

1. Identifiez la boucle.Quand une boucle de transfert s'est développée dans le réseau, ce sont les symptômes habituels :Perte de connectivité, et par derrière les régions affectées de réseauL'utilisation du CPU élevé sur des Routeurs s'est connectée aux segments affectés ou aux VLAN qui peuvent mener à de divers symptômes, tels que le lien instable voisin de lien instable de protocole de routage ou de routeur actif de Protocole HSRP (Hot Standby Router Protocol)Utilisation élevée de lien (souvent 100 pour cent)Utilisation du fond de panier élevée de commutateur (comparée à l'utilisation de spécification de base)Messages de Syslog qui indiquent le paquet faisant une boucle dans le réseau (par exemple les messages d'adresse IP en double de HSRP)Messages de Syslog qui indiquent réapprendre constant d'adresse ou les messages instables d'adresse MACUn nombre croissant de suppressions de sortie sur beaucoup d'interfacesRemarque: L'un de ces seules raisons peuvent ne pas indiquer différentes questions (ou aucune question du tout). Cependant, quand beaucoup de ces derniers sont observés en même temps, il est fortement probable qu'une boucle de transfert se soit développée dans le réseau.Remarque: Le moyen le plus rapide de vérifier ceci est de vérifier l'utilisation du trafic du fond de panier de commutateur :`cat# **show catalyst6000 traffic-meter traffic meter = 13%** Never cleared **peak = 14%** reached at 12:08:57 CET Fri Oct 4 2002` Remarque: Le Catalyst 4000 avec le logiciel de Cisco IOS ne prend en charge pas actuellement cette commande.Si le niveau en cours du trafic est bien au-dessus de normale ou si le niveau de spécification de base n'est pas connu, vérifiez si le niveau maximal a été réalisé récemment et s'il est proche du niveau en cours du trafic. Par exemple, si le niveau du trafic maximal est de 15 pour cent et il était atteint il y a juste deux minutes et le niveau en cours du trafic est de 14 pour cent, puis qui signifierait que le commutateur fonctionne sous exceptionnellement une charge élevée.Si la charge de la circulation est à un niveau normal, alors ce signifie probablement qu'il n'y a ou aucune boucle ou que ce périphérique n'est pas impliqué dans la boucle. Cependant, il pourrait encore être impliqué dans une boucle lente.
2. Découvrez la topologie (portée) de la boucle.Une fois qu'on l'a établi que la raison pour la panne de réseau est une boucle de transfert, le plus prioritaire est d'arrêter la boucle et de restaurer l'exploitation réseau. Afin d'arrêter la boucle, vous devez connaître quels ports sont impliqués dans la boucle : regardez les ports avec l'utilisation de lien la plus élevée (paquets par seconde). La commande de logiciel de Cisco IOS d'**interface d'exposition** affiche l'utilisation pour chaque interface.Afin d'afficher seulement les informations d'utilisation et le nom d'interface (pour une analyse rapide), vous pourriez utiliser le filtrage sorti par expression régulière de logiciel de Cisco IOS. Émettez l'**interface d'exposition | incluez la ligne|\ /sec** commande d'afficher seulement le paquet par deuxièmes statistiques et nom d'interface :`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`** Prêtez une attention particulière aux interfaces avec l'utilisation de lien la plus élevée. Dans cet exemple, ce sont les interfaces g2/3, g2/4, et g2/8 ; ils sont probablement les ports qui sont impliqués dans la boucle.

3. Cassez la boucle.Pour casser la boucle, vous devez arrêter ou déconnecter les ports impliqués. Il est très important non seulement d'arrêter la boucle mais aussi de trouver et réparer la cause principale de la boucle. Il est relativement plus facile de casser la boucle.**Remarque:** Afin d'aider l'analyse ultérieure de cause, vous n'avez pas besoin arrêté ou déconnectez tous les ports immédiatement ; au lieu de cela, fermez-les un par un. Il vaut généralement mieux d'arrêter des ports au point d'agrégation concerné par la boucle, telle qu'un commutateur de distribution ou de noyau. Si vous arrêtez tous les ports immédiatement et les activez ou rebranchez un par un, il ne pourrait pas fonctionner ; la boucle sera arrêtée et ne pourrait pas commencer juste après que le port offensant est rebranché. Par conséquent, il serait difficile de corréler la panne à n'importe quel port particulier.**Remarque:** Il est recommandé que vous collectez des informations avant que vous redémarriez les Commutateurs pour casser la boucle. Autrement, l'analyse ultérieure de cause principale sera très difficile.Après que vous désactiviez ou déconnectiez chaque port, vous devez vérifier si l'utilisation du fond de panier de commutateur est de nouveau à un niveau normal.**Remarque:** Maintenez dans l'esprit que, habituellement, quelques ports ne soutiennent pas la boucle mais, plutôt, inondez le trafic arrivant avec la boucle. Quand vous arrêtez de tels ports d'inondation, vous réduirez seulement l'utilisation du fond de panier par un peu, mais vous n'arrêterez pas la boucle.Dans la topologie d'exemple suivant, la boucle est entre les commutateur A, B, et D. Par conséquent, les liens ab, l'AD, et le BD soutiennent. Si vous arrêtez l'un de ces liens, vous arrêterez la boucle. Les liens courant alternatif, les EA, BC, et SOIENT inondent juste le trafic arrivant avec la



boucle. Après que le port soutenant soit arrêté, l'utilisation du fond de panier descendra à une valeur normale. Il est très important de noter de quel port l'arrêt a apporté à l'utilisation du fond de panier (et à l'utilisation d'autres ports) à un niveau normal.En ce moment, la boucle sera arrêtée et l'exploitation réseau devrait s'améliorer ; cependant, parce que la cause d'origine de la boucle n'a pas été probablement réparée, il pourrait encore y avoir quelques questions en suspens.
4. Trouvez et réparez la cause de la boucle.Une fois que la boucle a été arrêtée, vous devez déterminer la raison pour laquelle la boucle a commencé. C'est souvent la partie la plus difficile du processus, parce que les raisons peuvent varier. Il est également difficile de formaliser une procédure précise qui fonctionne dans tous les cas. Cependant, ce sont

quelques directives générales :Étudiez le diagramme de topologie, pour trouver un chemin redondant. Ceci inclut le port soutenant trouvé dans l'étape précédente qui revient au même commutateur (les paquets de chemin prenaient pendant la boucle). Dans la topologie d'exemple précédent, ce chemin est AD-DB-BA.Pour chaque commutateur sur le chemin redondant, vérifiez ces questions :Le commutateur connaît-il la racine correcte STP ?Tous les Commutateurs dans un réseau L2 devraient convenir sur une racine commune STP. C'est un symptôme clair des problèmes quand les passerelles affichent uniformément un ID différent pour la racine STP dans un exemple particulier VLAN ou STP. Émettez la commande de VLAN-*id de* **show spanning-tree vlan** d'afficher l'ID de passerelle de racine pour un VLAN donné :`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 nombre VLAN peut être trouvé du port, parce que des ports impliqués dans la boucle ont été établis dans les étapes précédentes. Si les ports en question sont des joncteurs réseau, souvent tous les VLAN sur le joncteur réseau sont impliqués. Si ce n'est pas le cas (par exemple, s'il s'avère que la boucle s'est produite sur un VLAN simple) puis vous pouvez essayer d'émettre les **interfaces d'exposition | incluez la** commande **L2|line|broadcast** (seulement sur superviseur 2 et engines postérieures sur des Commutateurs de gamme Catalyst 6500/6000, parce que le superviseur 1 ne fournit pas des statistiques de la commutation par-VLAN). Regardez les interfaces VLAN seulement. Le VLAN avec le montant le plus élevé de paquets commutés sera le plus souvent celui où la boucle s'est produite :`cat# **show int | 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 explique le nombre le plus élevé d'émissions et de trafic L2-switched.Le port de racine est-il identifié correctement ?Le port de racine devrait avoir le plus peu coûteux à la passerelle de racine (parfois un chemin est plus court en termes de sauts mais plus long en termes de coût, en tant que ports à vitesse réduite ayez des coûts plus élevés).Pour déterminer quel port est considéré la racine pour un VLAN donné, émettez la commande de *VLAN de* **show spanning-tree vlan** :`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`Est-ce que BPDU reçus régulièrement sur le port de racine et sur les ports qui sont censés être bloquent ?Des BPDU sont envoyés par la passerelle de racine à chaque `intervalle entre deux paquets Hello` (deux secondes par défaut). Les ponts en non-racine reçoivent, traitent, modifient, et propagent les BPDU qui sont reçus de la racine.Émettez la commande de **détail d'***interface de* **show spanning-tree interface** de voir si les BPDU sont reçus :`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:** Un BPDU a été reçu entre les deux sorties de la commande (le compteur a disparu de 53 à 54).Les compteurs affichés sont réellement des compteurs mis à jour par le processus STP lui-même. Ceci signifie qui, si les compteurs de réception incrémentés, étaient non seulement BPDU reçu par un port physique mais il était également reçu par le processus STP.Si le compteur reçu BPDU n'incrémente pas sur le port qui est censé être le remplaçant ou le port de sauvegarde de racine, alors le chèque si le port reçoit n'importe quelles Multidiffusions du tout (des BPDU sont envoyés comme Multidiffusion). Émettez la commande de **compteurs d'interface interface d'exposition** :cat# **show interface g3/2 counters** Port InOctets InUcastPkts **InMcastPkts** InBcastPkts Gi3/2 14873036 2 **89387** 0 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 **89391** 0 Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts Gi3/2 114366106 83776 732087 19 (La brève description A pour des rôles de port STP peut être trouvée dans le résumé rapide de la section de rôles de port STP d'améliorations de protocole spanning-tree utilisant le fonctionnalités de protection contre les boucles et de détection des différences de temps de propagation des BPDU.)Si aucun BPDU n'est reçu, vérifiez si le port ne compte pas des erreurs. Émettez la commande d'**erreurs de compteurs d'interface interface d'exposition** :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 reçus par le port physique mais n'atteint pas toujours le processus STP. Si les commandes utilisées dans les deux exemples précédents prouvent que quelques Multidiffusions sont reçues, et les erreurs n'incrémentent pas, alors vérifiez si les BPDU sont relâchés au niveau de processus STP. Émettez les processus-**stats de spanning-tree de test de commutateur de remote command** commandent sur le Catalyst 6500 :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 des statistiques de processus STP. Il est important de vérifier que les compteurs de baisse n'augmentent pas et que les paquets reçus augmentent.Si les paquets reçus n'augmentent pas mais le port physique reçoit des Multidiffusions, vérifiez que les paquets sont reçus par l'interface d'intrabande de commutateur (l'interface de la CPU). Émettez l'**ibc d'exposition de commutateur de remote command | commande du rx_input i** sur le Catalyst 6500/6000 :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 prouve que, entre les sorties, le port d'intrabande a reçu 23 paquets.**Remarque:** Ces 23 paquets sont non seulement des paquets BPDU ; c'est un compteur global pour tous les paquets reçus par le

port d'intrabande.S'il n'y a aucune indication que des BPDU sont relâchés sur le commutateur local ou le port, vous devez se déplacer au commutateur de l'autre côté du lien et vérifier si ce commutateur envoie des BPDU.Est-ce que BPDU sont envoyés régulièrement sur la non-racine, des ports désignés ?Si, selon le rôle de port, le port envoie des BPDU — mais le voisin ne les reçoit pas — vérifient si des BPDU sont envoyés réellement. Émettez la commande de **détail d'***interface de* **show spanning-tree interface** :`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 **BPDU: 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 **BPDU: sent 1776**, received 1` Dans cet exemple, deux BPDU ont été envoyés entre les sorties.**Remarque:** Le processus STP met à jour le `BPDU` : compteur `envoyé`. Ceci signifie que le compteur indique que le BPDU a été envoyé vers le port physique, pour être par la suite envoyé. Vérifiez si les compteurs de port augmentent pour les paquets de multidiffusion transmis. Émettez la commande de **compteurs d'interface interface d'exposition**. Ceci peut aider à déterminer si les BPDU sortent ou pas :`cat# **show interface g3/1 counters** Port InOctets InUcastPkts InMcastPkts InBcastPkts Gi3/1 127985312 83776 812319 19 Port OutOctets OutUcastPkts **OutMcastPkts** OutBcastPkts 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** OutBcastPkts Gi3/1 131826447 3442 **872346** 386` Avec toutes ces étapes, l'idée est de trouver le commutateur ou de joindre où des BPDU ne sont pas reçus, sont envoyés, ou traités.Il est possible, néanmoins peu probable, que le STP a calculé l'état correct pour le port, mais en raison d'une question d'avion de contrôle, il ne pouvait pas placer cet état sur le matériel d'expédition. Une boucle peut être créée, si le port de blocage supposé n'est pas bloqué au niveau matériel. Si vous suspectez une telle question dans votre réseau, entrez en contact avec le support technique de Cisco pour davantage d'assistance.
5. Restaurez la Redondance.Une fois que le périphérique ou joignent qui entraîne la boucle a été trouvé, ce périphérique doit être isolé dans le réseau, ou des mesures doivent être prises pour résoudre le problème (comme remplacez la fibre ou le GBIC). Les liens redondants, déconnectés dans l'étape 3, doivent être restaurés.Il est important de faire en tant que peu de manipulation comme possible au périphérique ou de joindre qui entraîne la boucle, parce que beaucoup de conditions qui mènent à une boucle peuvent être très passagères, intermittentes, et instables. Ceci signifie que, si la condition est effacée pendant ou après le dépannage, il peut prendre un moment avant qu'une telle condition se produise de nouveau. Il est possible que la condition puisse ne pas se produire de nouveau du tout. Tout effort devrait être fait pour préserver la condition, de sorte qu'il puisse plus plus loin être étudié par le support technique de Cisco. Il est important que vous collectiez des informations au sujet de la condition avant que vous remettiez à l'état initial les Commutateurs. Si une condition est allée, il est souvent impossible de déterminer la cause principale de la boucle. Pour trouver le périphérique ou joindre que déclenche la boucle est une réalisation importante, mais vous doit s'assurer qu'une autre panne de la même sorte n'entraîne pas la boucle de nouveau. Le pour en savoir plus, se rapportent à sécuriser le réseau contre la section de boucles de transfert de ce document.

Dépannage des modifications excessives de topologie entraînant l'inondation

Le rôle du mécanisme comité technique est de corriger des tables de l'expédition L2 après que la topologie d'expédition ait changé. C'est nécessaire pour éviter une panne de Connectivité parce que, après un comité technique, les ports particuliers par précédemment accessibles de quelques adresses MAC pourraient devenir accessibles par différents ports. Le comité technique raccourcit la durée de vieillissement de table d'expédition sur tous les Commutateurs dans le VLAN où le comité technique se produit ; ainsi, si l'adresse n'est pas réapprise, il expiration et l'inondation se produira pour assurer à portée de paquets l'adresse MAC de destination.

Le comité technique est déclenché par la modification de l'état STP d'un port à ou de l'état d'`expédition` STP. Après comité technique, même si l'adresse MAC de destination particulière a vieilli-, l'inondation ne devrait pas continuer pour long. L'adresse sera réapprise par le premier paquet qui provient l'hôte dont l'adresse MAC est devenue obsolet. La question pourrait surgir quand le TCs se produisent à plusieurs reprises, avec des intervalles courts. Les Commutateurs seront constamment fast-aging leurs tables d'expédition, ainsi l'inondation sera presque constante.

Remarque: Avec STP rapide ou multiple STP (IEEE 802.1w et IEEE 802.1s), le comité technique est déclenché par une modification de l'État du port à la `transmission`, aussi bien que la modification de rôle de `indiquer pour s'enraciner`. Avec STP rapide, la table de l'expédition L2 est immédiatement vidée, par opposition à 802.1d, qui raccourcit la durée de vieillissement. Vider immédiat de la table d'expédition restaure la Connectivité plus rapide, mais entraînera plus d'inondation.

Le comité technique devrait être un événement rare dans un réseau bien-configuré. Quand un lien sur un port de commutateur va en haut ou en bas, il y a par la suite un comité technique, une fois l'état STP du port change à ou de l'`expédition`. Quand le port s'agite, ceci entraînerait le TCs et l'inondation répétitifs.

Les ports avec la fonctionnalité PortFast STP activée n'entraîneront pas le TCs quand allant à ou de l'état d'`expédition`. La configuration du portfast sur tous les ports de fin-périphérique (tels que des imprimantes, des PC, et des serveurs) devrait limiter le TCs à une basse quantité et est fortement recommandée. Pour plus d'informations sur le TCs, référez-vous compréhension derrière des modifications de topologie de protocole spanning-tree.

S'il y a TCs répétitif sur le réseau, vous devez identifier la source des ces TCs et agir de les réduire, pour apporter l'inondation à un minimum.

Avec 802.1d, des informations STP sur un événement comité technique sont propagées parmi les passerelles par une notification comité technique (TCN), qui est un type particulier de BPDU. Si vous suivez les ports qui reçoivent TCN BPDU, vous pouvez trouver le périphérique qui lance le TCs.

Établissez si l'inondation est provoqué par par le TCs STP

Normalement, vous pouvez déterminer que là inonde de la représentation lente, les pertes de paquets sur les liens qui ne sont pas censés être congestionnés, et l'analyseur de paquet affichant de plusieurs paquets monodiffusions à la même destination qui n'est pas sur le segment local.

Pour plus d'informations sur l'inondation d'unicast, référez-vous à l'inondation d'Unicast dans les réseaux campus commutés.

Sur un Catalyst que 6500/6000 cela exécute le Cisco IOS logiciel, vous peut vérifier le compteur d'engine d'expédition (seulement sur l'engine de superviseur 2) pour estimer la quantité d'inondation. Émettez les **statistiques de comte d'exposition de commutateur de remote command | i MISS_DA|**Commande **ST_FR** :

```
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 affiche que la modification depuis la dernière époque cette commande a été exécutée, et la deuxième colonne affiche la valeur cumulative depuis la dernière réinitialisation. La première ligne affiche la quantité de trames inondées, et la deuxième ligne affiche la quantité de trames traitées. Si les deux valeurs sont étroites ensemble, ou la première valeur augmente à un haut débit, il pourrait être que le commutateur inonde le trafic. Cependant, ceci peut seulement être utilisé en même temps que d'autres manières de vérifier l'inondation, car les compteurs ne sont pas granulaires. Il y a un compteur par commutateur, pas par port ou VLAN. Il est normal de voir quelques paquets d'inondation, car le commutateur inondera toujours si l'adresse MAC de destination n'est pas dans la table d'expédition. Ce sera le cas quand le commutateur reçoit un paquet avec une adresse de destination qui n'a pas été encore apprise.

Dépistez la source de TCs

Si le nombre VLAN est connu pour le VLAN où excessif inondation se produit, vérifiez les compteurs STP pour voir si le nombre de TCs est élevé ou incrémentant régulièrement. Émettez la commande de **détail de VLAN-*id de* show spanning-tree vlan** (dans cet exemple, le VLAN 1 est utilisé) :

```
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 nombre VLAN n'est pas connu, vous pouvez utiliser l'analyseur de paquet ou vérifier les compteurs comité technique pour tous les VLAN.

Prenez les mesures pour empêcher le TCs excessif

Vous pouvez surveiller le `nombre de modifications de topologie` à l'opposé de voyez s'il augmente régulièrement. Puis, mouvement à la passerelle qui est connectée au port qui est affiché, de recevoir le dernier comité technique (dans l'exemple précédent, le port GigabitEthernet1/1) et de voir d'où le comité technique a été livré pour cette passerelle. Ce processus doit être répété jusqu'à ce que le port de station d'extrémité sans portfast STP activé soit trouvé, ou jusqu'au lien instable est trouvé qui doit être réparé. La procédure entière doit être répétée si le TCs proviennent toujours d'autres sources. Si le lien appartient à un fin-hôte, vous devriez configurer la fonctionnalité PortFast pour empêcher la génération du TCs.

Remarque: Dans l'implémentation du logiciel STP de Cisco IOS, le compteur pour le TCs incrémentera seulement si un TCN BPDU est reçu par un port dans un VLAN. Si une configuration normale BPDU avec un indicateur comité technique de positionnement est reçue alors le

compteur comité technique n'est pas incrémenté. Ceci signifie que, si vous suspectez un comité technique pour être la raison pour l'inondation, il est le meilleur de commencer dépister les sources pour le comité technique de la passerelle de racine STP dans ce VLAN. Il aura la plupart d'informations précises concernant la quantité et la source de TCs.

Dépannage des questions relatives au temps de convergence

Il y a des situations quand l'exécution réelle de STP n'apparie pas le comportement prévu. Ce sont les deux questions les plus fréquentes :

- La convergence STP ou la reconvergence prend plus long que prévu.
- La topologie en résultant est différente que prévue.

Le plus souvent, ce sont les raisons pour ce comportement :

- Une non-concordance entre la vraie et documentée topologie
- Mauvaise configuration, telle qu'une configuration contradictoire des temporisateurs STP, dépassant le diamètre STP, ou la mauvaise configuration de portfast
- CPU surchargée de commutateur pendant la convergence ou la reconvergence
- Erreur de logiciel

Comme cité précédemment, ce document peut seulement fournir des directives générales pour dépanner, dues à la large variété de questions qui pourraient affecter STP.

Pour comprendre pourquoi la convergence prend plus long que prévu, regardez l'ordre des événements STP pour découvrir ce qui se produisait et dans les quels commande. Puisque l'implémentation STP en logiciel de Cisco IOS n'a pas l'offre spéciale se connectant (excepté des événements spécifiques, tels que des incohérences de port), vous pouvez utiliser des fonctionnalités de débogage du logiciel STP de Cisco IOS de comprendre ce qui se produit.

Pour STP, avec du Catalyst 6500/6000 cela exécute le Cisco IOS logiciel, le traitement est fait sur le processeur de commutateur (fournisseur de services) (ou le superviseur), ainsi met au point le besoin d'être activé sur le fournisseur de services. Pour des groupes de passerelle de logiciel de Cisco IOS, le traitement est fait sur le processeur d'artère (RP), ainsi met au point les besoins d'être activé sur le RP (MSFC).

Commandes de débogage STP

Beaucoup de commandes de **débogage** STP sont destinées pour l'usage d'ingénierie de développement. Ils ne fournissent aucune sortie qui est signicative à quelqu'un sans connaissance détaillée de l'implémentation STP en logiciel de Cisco IOS. Une partie met au point peut fournir la sortie qui est immédiatement accessible en lecture, comme des modifications d'état de port, des modifications de rôle, événement tels que le TCs, et un vidage mémoire des BPDU reçus et transmis. Cette section ne fournit pas une description complète de tout les met au point, mais introduit plutôt brièvement le plus souvent utilisés.

Remarque: Quand vous utilisez des commandes de **débogage**, activez le nécessaire de minimum met au point. Si le temps réel met au point ne sont pas nécessaire, enregistrent la sortie au log plutôt que l'impriment à la console. Excessif met au point peut surcharger la CPU et perturber l'exécution de commutateur. Pour diriger la sortie de débogage vers le log au lieu de vers la console ou vers des sessions de telnet, n'émettez le **logging console informationnel** et **aucune** commande de **moniteur se connectante** en mode de configuration globale.

Pour voir le journal d'événements général, émettez la commande d'**événement de debug spanning-tree** pour par le spanning-tree VLAN (PVST) et rapide-PVST. C'est le premier mettent au point qui donne une idée générale de ce qui se produit avec STP.

En plusieurs mode du spanning-tree (MST), cela ne fonctionne pas pour émettre la commande d'**événement de debug spanning-tree**. , Émettez par conséquent les **rôles de debug spanning-tree mstp** commandent de voir les modifications de rôle de port.

Pour voir les modifications d'état STP de port, émettez la commande d'**état de debug spanning-tree switch** ainsi que la commande de **vp de debug pm** :

```
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 STP se comporte d'une certaine manière, il est souvent utile de voir les BPDU qui sont reçus et envoyés par le commutateur :

```
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 00
06 52 5F 0E 50 00 26 42 42 03 Nov 6 11:44:27: SP: STP: Data
00000000000000074F1CE847000000138048000 6525F0E4 08010010014000 2000F00 Nov 6 11:44:27: SP: STP:
VLAN1 Gi2/1:0000 00 00 00 000000074F1CE847 00000013 80480006525F0E40 8010 0100 1400 0200 0F00
```

Ceci mettent au point des travaux pour des modes PVST, rapides-PVST, et MST ; mais il ne décode pas le contenu des BPDU. Cependant, vous pouvez l'employer pour s'assurer que des BPDU sont reçus.

Pour voir le contenu du BPDU, émettez le **rx de debug spanning-tree switch décodent la** commande ainsi que la commande de **processus de rx de debug spanning-tree switch** pour PVST et rapide-PVST. Émettez la commande de **bpdu-rx de debug spanning-tree mstp** de voir le contenu du BPDU pour MST :

```
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 BPDU détaillé décodez avec cette commande de **débogage** :

```
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 la version du logiciel Cisco IOS 12.1.13E et plus tard, conditionnel met au point pour STP sont pris en charge. Ceci signifie que vous pouvez mettre au point les BPDU qui sont reçus ou transmis sur un par-port ou une base par-VLAN.

Émettez les *commandes d'interface de vlan_num* ou de **debug condition interface de debug condition vlan**, de limiter la portée de la par-interface de sortie de débogage ou du par-VLAN.

Sécuriser le réseau contre des boucles de transfert

Pour manipuler l'incapacité de STP de traiter correctement certaines pannes, Cisco a développé un certain nombre de fonctionnalités et améliorations pour protéger les réseaux contre des boucles de transfert.

Dépannage des aides STP pour isoler et trouver probablement la cause pour une panne particulière, alors que l'implémentation de ces améliorations est la seule manière de sécuriser le réseau contre des boucles de transfert.

Ce sont des méthodes pour protéger votre réseau contre des boucles de transfert :

1. Protocole UDLD (UniDirectional Link Detection) d'enable sur tous les liens de commutateur à commutateur. Pour plus d'informations sur UDLD, référez-vous à comprendre et à configurer la caractéristique de protocole Unidirectional Link Detection.
2. Loop Guard d'enable sur tous les Commutateurs. Pour plus d'informations sur le Loop Guard, référez-vous aux améliorations de protocole spanning-tree utilisant le fonctionnalités de protection contre les boucles et de détection des différences de temps de propagation des BPDU.Une fois activés, UDLD et Loop Guard éliminent la majorité des causes possibles pour des boucles de transfert. Plutôt que créent une boucle de transfert, le lien offensant (ou tous joint la personne à charge sur le matériel manquant) est arrêté ou

bloqué.**Remarque:** Tandis que ces deux caractéristiques semblent quelque peu redondantes, chacune a ses seules capacités. , Employez par conséquent les deux caractéristiques en même temps pour fournir le de plus haut niveau de la protection. Pour une comparaison détaillée d'UDLD et de Loop Guard, référez-vous au Loop Guard contre la détection unidirectionnelle de lien.Il y a différents avis au sujet de si vous devez utiliser UDLD agressif ou normal. Il convient noter que l'UDLD agressif n'assurera pas plus de protection contre des boucles comparées au mode normal UDLD. L'UDLD agressif détecte les scénarios port-collés (quand le lien est en hausse, mais là ne sont aucun blackholes associé du trafic). Le du côté incliné de cette fonctionnalité ajoutée est que l'UDLD agressif peut potentiellement désactiver des liens quand aucune à panne cohérente n'est présente. Souvent les gens confondent la modification de l'`intervalle entre deux paquets Hello` UDLD avec la configuration d'UDLD agressif. C'est incorrect. Des temporisateurs peuvent être modifiés en les deux modes UDLD.**Remarque:** Dans de rares cas, l'UDLD agressif peut arrêter tous les ports uplinks, qui isole essentiellement le commutateur du reste du réseau. Par exemple, ceci pourrait se produire quand les deux Commutateurs en amont éprouvent très l'utilisation du CPU élevé et la détection UDLD en mode agressif est utilisée. Par conséquent, il est recommandé que vous configurez des errordisable-délais d'attente, si le commutateur n'a pas la gestion hors bande en place.

3. Portfast d'enable sur tous les ports de station d'extrémité.Vous devez permettre au portfast de limiter la quantité de TCs et d'inondation ultérieure, qui peut affecter la performance du réseau. Utilisez seulement cette commande avec les ports qui se connectent pour finir des stations. Autrement, une boucle accidentelle de topologie peut entraîner une boucle de paquet de données et perturber le commutateur et l'exploitation réseau.**Attention :** Exercez l'attention quand vous n'utilisez l'**aucune** commande de **spanning-tree portfast**. Cette commande retire seulement toutes les commandes spécifiques de portfast de port. Cette commande active implicitement le portfast si vous définissez la commande de **spanning-tree portfast default** en mode de configuration globale et si le port n'est pas un port de joncteur réseau. Si vous ne configurez pas le portfast globalement, l'**aucune** commande de **spanning-tree portfast** n'est équivalente à la commande de **débronchement de spanning-tree portfast**.
4. Placez les EtherChannels au mode `desirable` en des côtés (où pris en charge) et l'option non-`silente`.Le mode `desirable` permettra au Protocole PAgP (Port Aggregation Protocol) d'assurer la cohérence d'exécution entre les pairs de acheminement. Ceci donne un degré supplémentaire de protection contre des boucles, particulièrement pendant les reconfigurations de canal (comme quand joindre ou quitter de liens le canal, et détection de panne de lien). Il y a une protection intégrée de mauvaise configuration de la Manche, qui est activée par défaut et qui empêche des boucles de transfert devant creuser des rigoles la mauvaise configuration ou d'autres conditions. Pour plus d'informations sur cette caractéristique, référez-vous compréhension derrière la détection d'incohérence d'EtherChannel.
5. Ne désactivez pas l'automatique-négociation (si pris en charge) sur des liens de commutateur à commutateur.les mécanismes d'Automatique-négociation peuvent donner les informations sur une panne à distance, qui sont la façon la plus rapide de détecter la panne au côté distant. Si la panne est détectée au côté distant, le côté local réduit le lien même si le lien reçoit toujours des impulsions. Comparé aux mécanismes de haut niveau de détection tels qu'UDLD, l'automatique-négociation est très rapide (dans des microsecondes) mais manque de la couverture de bout en bout d'UDLD (tel que le datapath entier : CPU — logique d'expédition — port1 — port2 — logique d'expédition — CPU contre port1 — port2). Le mode d'UDLD agressif fournit la fonctionnalité semblable à celle de l'automatique-

négociation quant à la détection de panne. Quand la négociation est prise en charge des deux côtés du lien, il n'y a aucun besoin d'activer la détection UDLD en mode agressif.

6. Précaution d'usage quand vous accordez les temporisateurs STP.Les temporisateurs STP dépendent de l'un l'autre et de la topologie du réseau. STP peut ne pas fonctionner correctement avec des modifications arbitraires apportées aux temporisateurs. Pour plus d'informations sur des temporisateurs STP, référez-vous aux temporisateurs de compréhension et de accord de Protocole Spanning Tree.
7. Si les attaques par déni de service sont possibles, sécurisez le périmètre du réseau STP avec la protection de racine.La protection de racine et la protection BPDU te permettent pour sécuriser STP contre l'influence de l'extérieur. Si une telle attaque est une possibilité, la protection de racine et la protection BPDU doivent être utilisées pour protéger le réseau. Pour plus d'informations sur la protection de racine et la protection BPDU, référez-vous à ces documents :Perfectionnement de la protection de la racine du protocole Spanning TreeAmélioration de la protection des BPDU en PortFast pour le spanning tree
8. Protection de l'enable BPDU sur des ports en Portfast, pour empêcher STP d'être affectée par les périphériques non autorisés de réseau (tels que des Concentrateurs, des Commutateurs, et des pont-routeurs) qui sont connectés aux ports.Si la protection de racine est correctement configurée, il empêchera déjà le STP d'être influencée de l'extérieur. Si la protection BPDU est activée, il arrêtera les ports qui reçoivent tous les BPDU (non seulement BPDU supérieurs). Ceci peut être utile si de tels incidents doit être étudiés, parce que la protection BPDU produit le message de Syslog et a arrêté le port. Il convient noter que des boucles de court-séjour ne sont pas empêchées par la racine ou les protections BPDU, si deux ports en Portfast sont connectés directement ou par le hub.
9. Évitez le trafic d'utilisateur sur le VLAN de gestion. Le VLAN de gestion n'est contenu à un module, pas le tout le réseau.L'interface de gestion de la commutation reçoit des paquets d'émission sur le VLAN de gestion. Si les émissions excessives se produisent (comme une saturation de diffusion ou une application de défaut de fonctionnement), la CPU de commutateur pourrait devenir surchargée, qui pourrait probablement tordre l'exécution STP.
10. Une racine (codée en dur) prévisible STP et un STP de sauvegarde enracinent le placement.La racine STP et la racine de sauvegarde STP doivent être configurées de sorte que la convergence, dans le cas des pannes, se produise d'une manière prévisible et établisse la topologie optimale dans chaque scénario. Ne laissez pas la priorité STP à la valeur par défaut, pour empêcher la sélection imprévisible de commutateur de racine.

Informations connexes

- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems