Dépannage des problèmes STP et considérations de conception associées

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Échec du protocole Spanning Tree
  - Convergence Spanning Tree
  - Non-correspondance de mode duplex
    - Logiciel Cisco IOS
  - Liaison Unidirectionnelle
  - Corruption de paquet
  - Erreurs de ressource
  - Erreur de configuration PortFast
  - Problèmes de réglage et de diamètre des paramètres STP gênants
  - Erreurs logicielles
- Dépannage d'une défaillance
  - Utiliser le schéma du réseau
  - Identifier une boucle de pontage
  - Restaurez rapidement la connectivité et préparez-vous pour une autre fois
    - Désactiver les ports pour rompre la boucle
    - Consigner les événements STP sur les périphériques qui hébergent des ports bloqués
  - Vérifier les ports
    - Vérifiez que les ports bloqués reçoivent des BPDU
    - Rechercher une non-concordance de mode duplex
    - Vérifier l'utilisation des ports
    - Vérifier la corruption des paquets
  - Rechercher les erreurs de ressource
  - Commandes utiles
    - Commandes du logiciel Cisco IOS
- Conception STP pour éviter les problèmes
  - Savoir où se trouve la racine
  - Savoir où se situe la redondance
  - Réduction du nombre de ports bloqués
    - Élaguer les VLAN que vous n'utilisez pas
    - Utiliser la commutation de couche 3
  - Conservez STP même si cela n'est pas nécessaire
  - Maintenez le trafic hors du VLAN d'administration et n'avez pas de VLAN unique sur l'ensemble du réseau

Informations connexes

Introduction

Ce document décrit comment dépanner et empêcher les pannes du protocole STP (Spanning Tree Protocol) dans les réseaux Cisco Catalyst pontés.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document se concentre sur le comportement STP classique et les commandes du logiciel Cisco IOS.

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.

Informations générales

Ce document discute certaines des raisons courantes pour lesquelles le STP peut échouer et les informations à rechercher pour identifier la source du problème. Elle indique également le type de conception qui minimise les problèmes liés au Spanning Tree et qui est facile à dépanner.

Ce document ne traite pas du fonctionnement de base du protocole STP. Pour savoir comment fonctionne le protocole STP, reportez-vous à ce document :

- Comprendre et configurer le protocole STP sur les commutateurs Catalyst

Ce document ne traite pas du protocole Rapid STP (RSTP), défini dans la norme IEEE 802.1w. En outre, ce document ne traite pas du protocole MST (Multiple Spanning Tree), défini dans la norme IEEE 802.1s. Sauf indication contraire, les descriptions de minuteur et de convergence de

ce document s'appliquent au comportement STP IEEE 802.1D classique.

Pour plus d'informations sur les protocoles RSTP et MST, reportez-vous aux documents suivants :

- Comprendre le protocole STP (Multiple Spanning Tree Protocol) (802.1s)
- Comprendre le protocole Spanning Tree rapide (802.1w)

Pour un document de dépannage STP plus spécifique pour les commutateurs Catalyst qui exécutent le logiciel Cisco IOS, référez-vous au document Dépannage des problèmes STP sur les commutateurs Catalyst.



Remarque : Ce document préserve les informations STP existantes pour fournir des connaissances de base sur le comportement STP IEEE 802.1D classique. Le protocole STP classique n'est pas recommandé pour les environnements de production. Pour les réseaux de production, utilisez une conception routée de couche 3 si possible et déployez un protocole ou un mode Spanning Tree plus récent, tel que le protocole RSTP (Rapid Spanning Tree Protocol), le protocole Rapid PVST+ ou le protocole MST (Multiple Spanning Tree), en fonction de la prise en charge de la plate-forme et des exigences de conception du réseau

---

Échec du protocole Spanning Tree

La fonction principale de l’algorithme Spanning Tree (STA) est de couper les boucles créées par les liaisons redondantes dans les réseaux en pont. Le protocole STP fonctionne au niveau de la couche 2 du modèle OSI (Open Systems Interconnection). À l’aide d’unités BPDU (Bridge Protocol Data Unit) qui échangent entre les ponts, le protocole STP sélectionne les ports qui acheminent ou bloquent le trafic. Ce protocole peut échouer dans certains cas spécifiques, et de dépanner la situation qui en résulte peut être très difficile, ce qui dépend de la conception du réseau. Dans cette zone particulière, vous effectuez la partie la plus importante du processus de dépannage avant que le problème ne se produise.

Une défaillance dans le STA entraîne généralement une boucle de pontage. La plupart des clients qui appellent le support technique Cisco pour des problèmes de Spanning Tree suspectent un bogue, mais un bogue en est rarement la cause. Même si le logiciel est le problème, une boucle de pontage dans un environnement STP provient toujours d'un port qui peut bloquer, mais qui transfère le trafic.

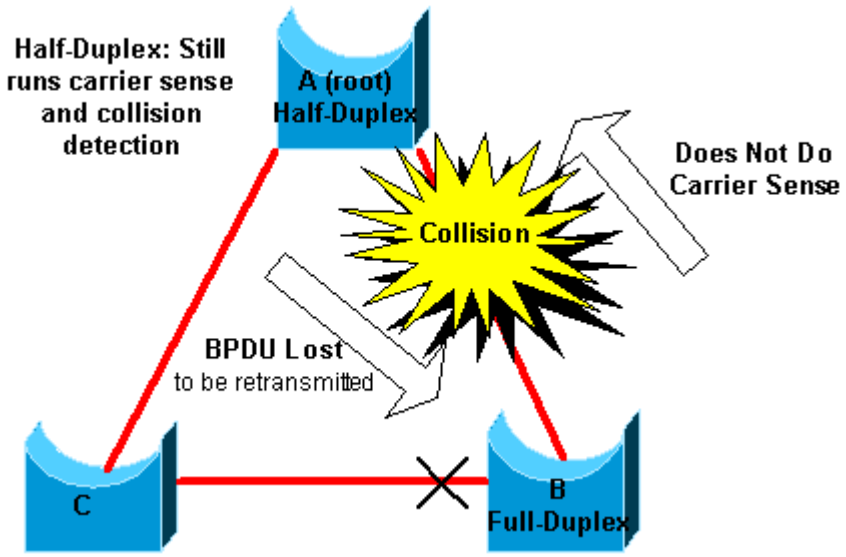
Convergence Spanning Tree

Reportez-vous à la vidéo sur le protocole Spanning Tree pour un exemple de la façon dont le protocole converge au départ. L'exemple explique également pourquoi un port bloqué passe en mode de transmission en raison d'une perte excessive de BPDU, ce qui entraîne une défaillance de STA.

Le reste de ce document liste les différentes situations qui peuvent causer l'échec de STA. La plupart de ces défaillances sont liées à une perte massive de BPDU. La perte entraîne le passage des ports bloqués en mode de transmission.

Non-correspondance de mode duplex

La non-concordance de mode bidirectionnel sur une liaison point à point est une erreur de configuration très courante. Sur les liaisons Ethernet 10/100 Mbits/s traditionnelles, si vous définissez manuellement le mode duplex sur Full d'un côté de la liaison et laissez l'autre côté en mode de négociation automatique, la liaison se termine en mode half-duplex. (Un port dont le mode duplex est défini sur Full ne négocie plus.)



Dans le pire des cas, un pont qui envoie des trames BPDU a le mode duplex défini sur half-duplex sur un port, alors que le mode duplex est défini sur full duplex sur le port homologue à l'autre extrémité de la liaison. Dans l'exemple précédent, la non-correspondance de mode duplex sur la liaison entre les ponts A et B peut facilement conduire à une boucle de pontage. Le pont B étant configuré pour le mode bidirectionnel simultané, il n'effectue pas de détection de porteuse avant l'accès à la liaison. Le pont B commence à envoyer des trames même si le pont A utilise déjà la liaison. Cette situation est un problème pour A ; Le pont A détecte une collision et exécute l'algorithme de réémission temporisée avant que le pont ne tente une autre transmission de la trame. S'il y a suffisamment de trafic de B vers A, chaque paquet que A envoie, qui inclut les BPDU, subit un report ou une collision et finit par être abandonné. D'un point de vue STP, comme le pont B ne reçoit plus de BPDU de A, le pont B a perdu le pont racine. Cela conduit B à débloquer le port connecté au pont C, ce qui crée la boucle.

Chaque fois qu'il y a une non-correspondance de mode duplex, ce message d'erreur peut être vu sur les consoles de commutateur des commutateurs Catalyst qui exécutent le logiciel Cisco IOS :

Logiciel Cisco IOS

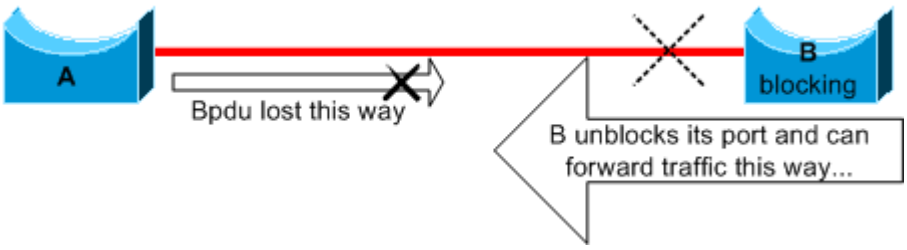
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half duplex), with TBA050714
```

Vérifiez les paramètres duplex et, si la configuration duplex ne correspond pas, définissez la configuration de manière appropriée.

Pour plus d'informations sur la façon de dépanner une non-correspondance de mode duplex, référez-vous au document Configure and Verify Ethernet 10/100/1000Mb Half/Full Duplex Auto-Negotiation.

Liaison Unidirectionnelle

Les liaisons unidirectionnelles sont une cause courante de boucle de pontage. Sur les liaisons à fibre optique, une défaillance qui se produit sans détection entraîne souvent des liaisons unidirectionnelles. Une autre cause est un problème avec un émetteur-récepteur. Tout ce qui peut amener une liaison à rester active et à fournir une communication unidirectionnelle est très dangereux en ce qui concerne le protocole STP. Cet exemple clarifie :



Supposons ici que la liaison entre A et B soit unidirectionnelle. La liaison rejette le trafic de A à B, tandis que la liaison transmet le trafic de B à A. Supposons que le pont B faisait obstacle avant que la liaison ne devienne unidirectionnelle. Cependant, un port ne peut bloquer que s'il reçoit des BPDU d'un pont qui a une priorité plus élevée. Puisque, dans ce cas, toutes les BPDU qui proviennent de A sont perdues, le pont B fait éventuellement passer son port vers A à l'état de transmission et transfère le trafic. Cela crée une boucle. Si cette défaillance existe au démarrage, le protocole STP ne converge pas correctement. Dans le cas d'une non-correspondance de mode duplex, un redémarrage aide temporairement ; mais dans ce cas, un redémarrage des ponts n'a absolument aucun effet.

Afin de détecter les liaisons unidirectionnelles avant la création de la boucle de transfert, Cisco a conçu et mis en oeuvre le protocole UDLD (UniDirectional Link Detection). UDLD détecte les conditions unidirectionnelles sur les liaisons de couche 2 prises en charge. Configurez le mode UDLD agressif sur les liaisons point à point prises en charge où la désactivation automatique des ports est requise après la détection d'une condition unidirectionnelle.

Pour plus d'informations sur l'utilisation d'UDLD, référez-vous au document Configurer la fonctionnalité de protocole UDLD.

Corruption de paquet

La corruption des paquets peut également entraîner le même type de défaillance. Si une liaison présente un taux élevé d'erreurs physiques, vous pouvez perdre un certain nombre de BPDU consécutives. Cette perte peut amener un port de blocage à passer à l'état de transmission. Vous ne voyez pas ce cas très souvent parce que les paramètres STP par défaut sont très conservateurs. Avec les minuteurs par défaut IEEE 802.1D classiques, un port bloqué peut prendre environ 50 secondes à partir de la perte de la dernière unité BPDU supérieure pour atteindre l'état de transmission : 20 secondes d'âge maximum, 15 secondes d'écoute et 15 secondes d'apprentissage. La transmission réussie d'une seule unité BPDU rompt la boucle. Ce cas se produit généralement avec l'ajustement négligent des paramètres STP. La réduction de l'âge maximal est un exemple d'ajustement.

Une non-correspondance de mode bidirectionnel, des câbles défectueux ou une longueur de câble incorrecte peuvent endommager les paquets. Référez-vous au document Dépannage des problèmes de port et d'interface de commutateur pour une explication du compteur d'erreurs du logiciel Cisco IOS.

Erreurs de ressource

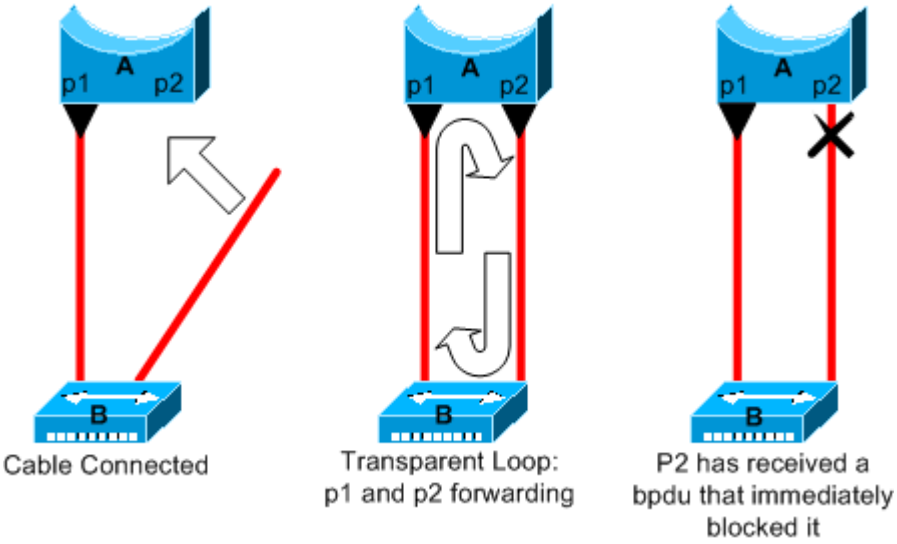
Le protocole STP est mis en oeuvre dans le logiciel, même sur les commutateurs haut de gamme qui remplissent la plupart des fonctions de commutation dans le matériel avec des circuits intégrés spécialisés à application spécifique (ASIC). Si, pour une raison quelconque, il y a une surutilisation du CPU du pont, les ressources peuvent être inadéquates pour la transmission des BPDU. Le STA n'est généralement pas gourmand en processeur et a la priorité sur les autres processus. La section Rechercher les erreurs de ressource de ce document fournit quelques directives sur le nombre d'instances de STP qu'une plate-forme particulière peut traiter.

Erreur de configuration PortFast

PortFast est une fonctionnalité que vous activez généralement uniquement pour un port ou une interface qui se connecte à un hôte. Lorsque la liaison est établie sur ce port, le pont ignore les

premières étapes du STA et passe directement en mode de transmission.

⚠ Mise en garde : Activez PortFast uniquement sur les interfaces de périphérie qui ne se connectent pas à un périphérique de pontage de couche 2. N'activez pas PortFast sur une interface qui peut recevoir des BPDU ou créer une boucle de couche 2.



Dans cet exemple, le périphérique A est un pont avec le port p1 déjà en transmission. Le port p2 a une configuration PortFast. Le périphérique B est un concentrateur. Dès que vous branchez le second câble sur A, le port p2 passe en mode de transmission et crée une boucle entre p1 et p2. Cette boucle s'arrête dès que p1 ou p2 reçoit une trame BPDU qui met l'un de ces deux ports en mode de blocage. Mais il y a un problème avec ce genre de boucle transitoire. Si le trafic en boucle est très intense, le pont peut rencontrer des problèmes avec la transmission réussie de la trame BPDU qui arrête la boucle. Ce problème peut retarder considérablement la convergence ou provoquer l'arrêt du réseau dans des cas extrêmes.

Pour plus d'informations sur l'utilisation correcte de PortFast sur les commutateurs qui exécutent le logiciel Cisco IOS, référez-vous au document Utilisation de PortFast et d'autres commandes pour corriger les retards de connectivité de démarrage de station de travail.

Même avec la configuration PortFast, le port ou l'interface participe toujours au protocole STP. Si un commutateur avec une priorité de pont inférieure à celle du pont racine actif actuel se connecte à un port ou une interface configuré(e) PortFast, il peut être sélectionné comme pont racine. Ce changement de pont racine peut affecter la topologie STP active et peut rendre le réseau sous-optimal. Pour éviter cette situation, la plupart des commutateurs Catalyst qui exécutent le logiciel Cisco IOS ont une fonction nommée BPDU Guard. La protection BPDU désactive un port ou une interface configuré(e) PortFast si le port ou l'interface reçoit une BPDU.

Pour plus d'informations sur l'utilisation de la fonctionnalité BPDU Guard sur les commutateurs qui exécutent le logiciel Cisco IOS, référez-vous au document Comprendre l'amélioration de la

protection BPDU PortFast du Spanning Tree.

Problèmes de réglage et de diamètre des paramètres STP gênants

Une valeur agressive pour le paramètre max-age et le délai de transmission peuvent conduire à une topologie STP très instable. Dans ce cas, la perte de certaines unités BPDU peut provoquer l'apparition d'une boucle. Un autre problème qui n'est pas bien connu concerne le diamètre du réseau en pont. Les valeurs par défaut conservatrices des compteurs STP imposent un diamètre de réseau maximal de sept. Ce diamètre de réseau maximal limite la distance entre les ponts du réseau. Dans ce cas, deux ponts distincts ne peuvent pas se trouver à plus de sept sauts l'un de l'autre. Une partie de cette restriction provient du champ d'âge que les unités BPDU transportent.

Lorsqu'une trame BPDU se propage du pont racine vers les feuilles de l'arbre, le champ d'âge s'incrémente chaque fois que la trame BPDU passe par un pont. Finalement, le pont rejette la BPDU lorsque le champ d'âge dépasse l'âge maximal. Si la racine est trop éloignée de certains ponts du réseau, ce problème peut se produire. Ce problème affecte la convergence du Spanning Tree.

Faites particulièrement attention si vous prévoyez de modifier les compteurs STP à partir de la valeur par défaut. Il y a danger si vous essayez d'obtenir une reconvergence plus rapide de cette façon. Un changement de minuteur STP a un impact sur le diamètre du réseau et la stabilité du STP. Vous pouvez modifier la priorité du pont pour sélectionner le pont racine et modifier le coût ou le paramètre de priorité du port pour contrôler la redondance et l'équilibrage de charge.

Le logiciel Cisco Catalyst vous fournit des macros qui ajustent finement les paramètres STP les plus importants pour vous :

- La commande spanning-tree vlan number root { primary | secondary } diminue la priorité du pont de sorte qu'il devienne racine (ou racine alternative). Une option supplémentaire est disponible pour cette commande qui permet de régler les compteurs STP en spécifiant le diamètre de votre réseau. Même lorsqu'il est correctement effectué, le réglage du minuteur n'améliore pas de manière significative le temps de convergence et introduit certains risques d'instabilité dans le réseau. En outre, ce type de réglage doit être mis à jour chaque fois qu'un périphérique est ajouté au réseau. Conservez les valeurs par défaut, qui sont familières aux ingénieurs réseau.
- La commande spanning-tree uplinkfast pour le logiciel Cisco IOS augmente la priorité du commutateur afin que le commutateur ne devienne pas le pont racine. La commande réduit le temps de convergence STP après une défaillance de liaison montante directe. Utilisez cette fonctionnalité héritée sur un commutateur de couche d'accès avec des liaisons ascendantes redondantes vers la couche de distribution lorsque la plate-forme et le mode STP le prennent en charge. Reportez-vous au document Comprendre et configurer la fonctionnalité Cisco UplinkFast.

- La commande spanning-tree backbonefast pour le logiciel Cisco IOS peut réduire le temps de convergence STP du commutateur en cas de défaillance d'une liaison indirecte. BackboneFast est une fonctionnalité propriétaire de Cisco. Reportez-vous au document Comprendre et configurer Backbone Fast sur les commutateurs Catalyst.

Pour plus d'informations sur les compteurs STP et les règles pour les régler quand c'est absolument nécessaire, référez-vous au document Comprendre et régler les compteurs de protocole Spanning Tree.

Erreurs logicielles

Comme indiqué dans l'introduction, le protocole STP est l'une des premières fonctionnalités mises en oeuvre dans les produits Cisco. Vous pouvez vous attendre à ce que cette fonctionnalité soit très stable. Seule l'interaction avec des fonctionnalités plus récentes, telles qu'EtherChannel, a entraîné l'échec du protocole STP dans certains cas très spécifiques qui ont maintenant été traités. Un certain nombre de facteurs différents peuvent causer un bogue logiciel et peuvent avoir un certain nombre d'effets différents. Il n'y a aucun moyen de décrire correctement les problèmes qu'un bogue peut introduire. La situation la plus dangereuse qui résulte d'erreurs logicielles est si vous ignorez certaines unités BPDU ou si vous avez une transition de port de blocage vers le transfert.

Dépannage d'une défaillance

Malheureusement, il n'existe pas de procédure systématique de dépannage d'un problème STP. Cependant, cette section résume certaines des actions qui sont à votre disposition. La plupart des étapes de cette section s’appliquent au dépannage des boucles de pontage en général. Vous pouvez utiliser une approche plus conventionnelle pour identifier d'autres défaillances du protocole STP qui entraînent une perte de connectivité. Par exemple, vous pouvez explorer le chemin emprunté par le trafic qui rencontre un problème.

Remarque : La plupart de ces étapes de dépannage supposent une connectivité aux différents périphériques du réseau en pont. Cette connectivité signifie que vous avez accès à la console. Pendant une boucle de pontage, par exemple, vous ne pouvez probablement pas établir de connexion à distance.

Si vous disposez de la sortie d'une **show tech-support** commande de votre périphérique Cisco, vous pouvez utiliser Cisco CLI Analyzer.

Remarque : Seuls les utilisateurs Cisco enregistrés ont accès aux informations et aux outils internes de Cisco.

Utiliser le schéma du réseau

Avant de dépanner une boucle de pontage, vous devez connaître au moins les éléments suivants :

- La topologie du réseau en pont
- L'emplacement du pont racine
- L'emplacement des ports bloqués et des liaisons redondantes

Ces connaissances sont essentielles pour au moins les deux raisons suivantes :

- Pour savoir ce qu'il faut réparer sur le réseau, vous devez savoir à quoi ressemble le réseau lorsqu'il fonctionne correctement.
- La plupart des étapes de dépannage utilisent simplement les commandes show pour essayer d'identifier les conditions d'erreur. La connaissance du réseau vous permet de vous concentrer sur les ports critiques des périphériques clés.

Identifier une boucle de pontage

Auparavant, une tempête de diffusion pouvait avoir un effet désastreux sur le réseau. Aujourd'hui, avec des liaisons haut débit et des périphériques qui assurent la commutation au niveau matériel, il est peu probable qu'un hôte unique, par exemple un serveur, fasse tomber un réseau en panne par le biais de diffusions. La meilleure façon d'identifier une boucle de pontage est de capturer le trafic sur une liaison saturée et de vérifier que vous voyez des paquets similaires plusieurs fois. Toutefois, si tous les utilisateurs d'un domaine de pont donné rencontrent des problèmes de connectivité en même temps, vous pouvez déjà suspecter une boucle de pontage.

Vérifiez l'utilisation des ports sur vos périphériques et recherchez les valeurs anormales. Reportez-vous à la section Vérifier l'utilisation des ports de ce document.

Restaurez rapidement la connectivité et préparez-vous pour une autre fois

Désactiver les ports pour rompre la boucle

Les boucles de pontage ont des conséquences extrêmement graves sur un réseau de pontage. Les administrateurs n'ont généralement pas le temps de rechercher la cause de la boucle et préfèrent restaurer la connectivité dès que possible. Afin d'arrêter une boucle active, utilisez la console ou l'accès hors bande pour désactiver un chemin redondant suspecté à la fois, et vérifiez la connectivité après chaque modification. Évitez de désactiver les liaisons qui fournissent le seul chemin de gestion ou de transfert vers un segment de réseau. Si vous pouvez identifier une partie du réseau qui est la plus affectée, commencez à désactiver les ports dans cette zone. Ou, si possible, désactivez initialement les ports qui peuvent être bloquants. Chaque fois que vous désactivez un port, vérifiez si vous avez restauré la connectivité sur le réseau. En identifiant le port désactivé qui arrête la boucle, vous identifiez également le chemin redondant où se trouve ce port. Si ce port a été bloqué, vous avez probablement trouvé la liaison sur laquelle la panne est apparue.

Consigner les événements STP sur les périphériques qui hébergent des ports bloqués

Si vous ne parvenez pas à identifier précisément la source du problème, ou si le problème est temporaire, activez la journalisation des événements STP sur les ponts et les commutateurs du réseau qui subit la panne. Si vous voulez limiter le nombre de périphériques à configurer, activez au moins cette journalisation sur les périphériques qui hébergent des ports bloqués ; la transition d'un port bloqué est ce qui crée une boucle.

⚠ Mise en garde : Les commandes de débogage peuvent ajouter une charge de plan de contrôle pendant une boucle de pontage. Exécutez-les uniquement avec un accès par console ou hors bande, surveillez l'utilisation du processeur et désactivez le débogage après la collecte des données.

- Exécutez la commande EXEC debug spanning-tree events pour activer le débogage des événements STP. Configurez logging buffered pour capturer les messages dans la mémoire tampon de journalisation.

Vous pouvez également essayer d'envoyer la sortie de débogage à un périphérique syslog. Malheureusement, lorsqu'une boucle de pontage se produit, vous maintenez rarement la connectivité à un serveur syslog.

Vérifier les ports

Les ports critiques à examiner en premier sont les ports de blocage. Cette section fournit une liste

des éléments à rechercher sur les différents ports, avec une description rapide des commandes à émettre pour les commutateurs qui exécutent le logiciel Cisco IOS.

Vérifiez que les ports bloqués reçoivent des BPDU

En particulier sur les ports bloqués et les ports racine, vérifiez que vous recevez régulièrement des BPDU. Plusieurs problèmes peuvent entraîner une défaillance du port lors de la réception de paquets ou de BPDU.

- Logiciel Cisco IOS - Dans le logiciel Cisco IOS version 12.0 ou ultérieure, la sortie de la commande show spanning-tree vlan <vlan-id>detail comporte un champ `BPDU`. Le champ indique le nombre de BPDU reçues pour chaque interface. Exécutez la commande une ou deux fois de plus pour déterminer si le périphérique reçoit des unités BPDU. Une autre option est d'activer le débogage STP avec la commande debug spanning-tree bpdu pour vérifier la réception des BPDU.

Rechercher une non-concordance de mode duplex

Pour rechercher une non-correspondance de mode duplex, vous devez vérifier chaque côté de la liaison point à point.

- Logiciel Cisco IOS : exécutez la **show interfaces [interface-number] status** commande permettant de vérifier la vitesse et l'état duplex du port spécifique.

Vérifier l'utilisation des ports

Une interface avec surcharge de trafic peut ne pas transmettre les BPDU vitales. Une surcharge de liaison indique également une boucle de pontage possible.

- Logiciel Cisco IOS : utilisez la commande **show interfaces** pour déterminer l'utilisation sur une interface. Plusieurs champs vous aident dans cette détermination, tels que `load` et `packets input/output`. Reportez-vous au document Troubleshoot Switch Port and Interface Problems pour une explication du résultat de la **show interfaces** commande.

Vérifier la corruption des paquets

- Logiciel Cisco IOS : recherchez les incréments d'erreur dans le compteur d'erreurs d'entrée (`input errors counter`) de la commande show interfaces . Les compteurs d'erreurs incluent les `trames incomplètes, les trames géantes, l'absence de tampon, le CRC, la trame`, le

`dépassement` et les `nombres ignorés`.

Référez-vous au document Dépannage des problèmes de port et d'interface de commutateur pour une explication de la **show interfaces** command output.

Rechercher les erreurs de ressource

Une utilisation CPU élevée peut être dangereuse pour un système qui exécute le STA. Utilisez cette méthode pour vérifier que la ressource CPU est adéquate pour un périphérique :

- Logiciel Cisco IOS : exécutez la commande show processes cpu . Vérifiez que l'utilisation du processeur n'est pas trop élevée.

Il y a une limitation sur le nombre d'instances différentes de STP qu'un Supervisor Engine peut traiter. Assurez-vous que le nombre total de ports logiques sur toutes les instances de STP pour différents VLAN ne dépasse pas le nombre maximal pris en charge pour chaque type de Supervisor Engine et configuration de mémoire.

Émettez la **show spanning-tree summary totals** commande pour les commutateurs, cette commande affiche le nombre de ports logiques ou d'interfaces par VLAN dans la colonne `STP Active`. Le total apparaît au bas de cette colonne. Le total représente la somme de tous les ports logiques sur toutes les instances de STP pour les différents VLAN. Assurez-vous que ce nombre ne dépasse pas le nombre maximal pris en charge pour chaque type de Supervisor Engine.

 Remarque : La formule permettant de calculer la somme des ports logiques sur le commutateur est la suivante :

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

Pour un résumé des restrictions STP qui s'appliquent aux commutateurs Catalyst, référez-vous à ces documents :

Plateforme	Restrictions STP du logiciel Cisco IOS
Supervisor Engine 720 Catalyst 6500/6000	Notes de version de Cisco IOS version 12.2SXF et reconstructions
Catalyst 4500/4000	Notes de version du commutateur de la gamme Catalyst 4500, Cisco IOS, 12.1EW
Catalyst 3750	Guide de configuration du logiciel du commutateur Catalyst

	3750, Rél. 12.1(19)EA1

Commandes utiles

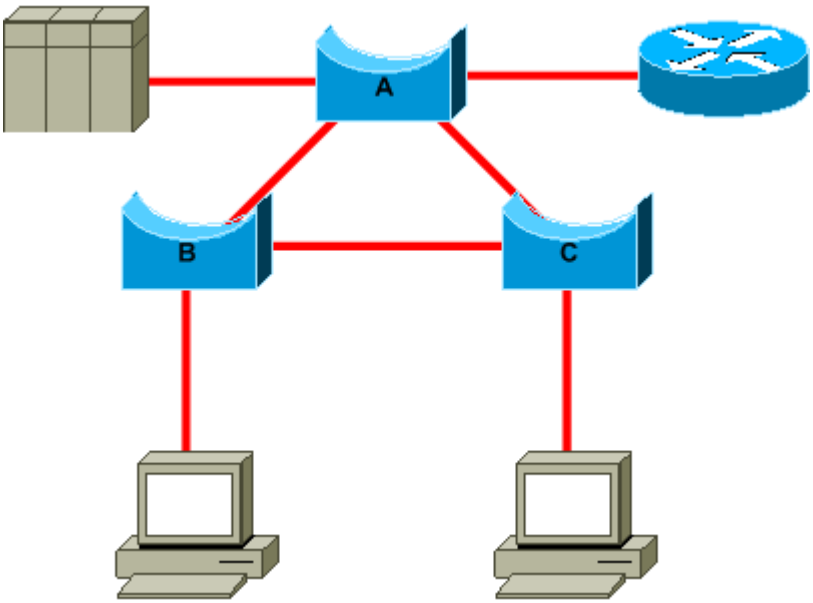
Commandes du logiciel Cisco IOS

- **show interfaces**
- **show spanning-tree**
- **show processes cpu**
- **debug spanning-tree**
- **logging buffered**

Conception STP pour éviter les problèmes

Savoir où se trouve la racine

Très souvent, les informations sur l'emplacement de la racine ne sont pas disponibles au moment du dépannage. Ne laissez pas le STP décider quel pont est racine. Pour chaque VLAN, vous pouvez généralement identifier le commutateur qui peut le mieux servir de racine. Cela dépend de la conception du réseau. En règle générale, choisissez un pont puissant au milieu du réseau. Si vous placez le pont racine au centre du réseau avec une connexion directe aux serveurs et aux routeurs, vous réduisez généralement la distance moyenne entre les clients et les serveurs et les routeurs.



Ce schéma montre :

- Si le pont B est racine, la liaison A vers C est bloquée sur le pont A ou le pont C. Dans ce cas-là, les hôtes qui se connectent au commutateur B peuvent accéder au serveur et au routeur en deux sauts. Les hôtes qui se connectent au pont C peuvent accéder au serveur et au routeur en trois sauts. La distance moyenne est de deux sauts et demi.
- Si le pont A est la racine, le routeur et le serveur sont accessibles en deux sauts pour les deux hôtes qui se connectent sur B et C. La distance moyenne est maintenant de deux sauts.

La logique de cet exemple simple est transférée vers des topologies plus complexes.

Remarque : Pour chaque VLAN, configurez le pont racine et le pont racine de secours en réduisant la valeur de priorité du pont STP. Vous pouvez également utiliser les commandes spanning-tree vlan <vlan-id> root primary et spanning-tree vlan <vlan-id> root secondary.

Savoir où se situe la redondance

Planifiez l'organisation de vos liaisons redondantes. Oubliez la fonctionnalité plug-and-play du protocole STP. Réglez le paramètre de coût STP pour décider quels ports bloquent. Ce réglage n'est généralement pas nécessaire si vous disposez d'une conception hiérarchique et d'un pont racine dans un bon emplacement.

Remarque : Pour chaque VLAN, identifiez les ports qui peuvent bloquer le réseau stable. Avoir un schéma de réseau qui montre clairement chaque boucle physique dans le réseau dont les ports bloqués cassent les boucles.

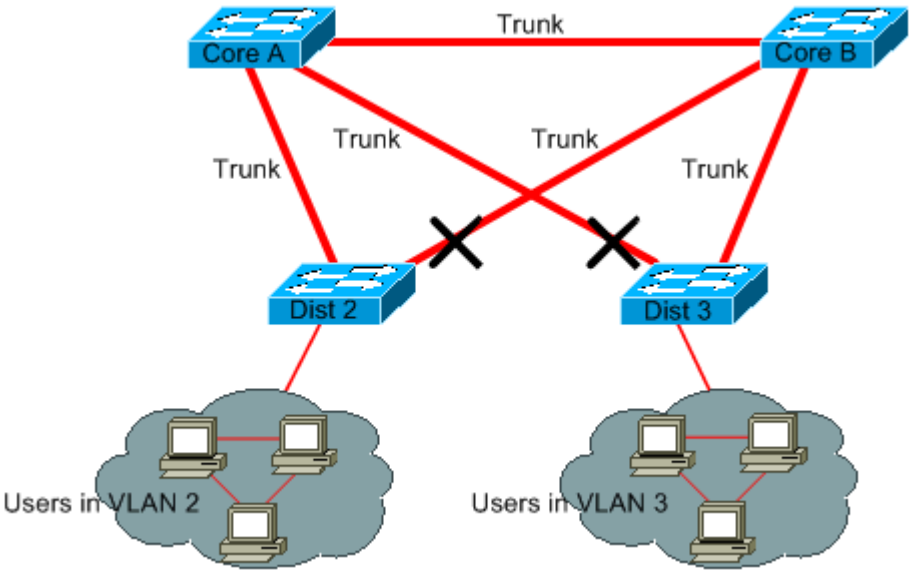
La connaissance de l’emplacement des liaisons redondantes vous aide à identifier une boucle de pontage accidentelle et la cause. En outre, la connaissance de l'emplacement des ports bloqués vous permet de déterminer l'emplacement de l'erreur.

Réduction du nombre de ports bloqués

La seule action critique que le protocole STP effectue est le blocage des ports. Un seul port de blocage qui passe par erreur à l’acheminement peut faire fondre une grande partie du réseau. Une bonne façon de limiter le risque inhérent à l'utilisation du STP est de réduire autant que possible le nombre de ports bloqués.

Élaguer les VLAN que vous n’utilisez pas

Évitez les chemins indépendants inutiles de couche 2 entre deux noeuds de commutation. Grouper des liaisons parallèles dans un EtherChannel lorsque la conception et la plate-forme le prennent en charge :

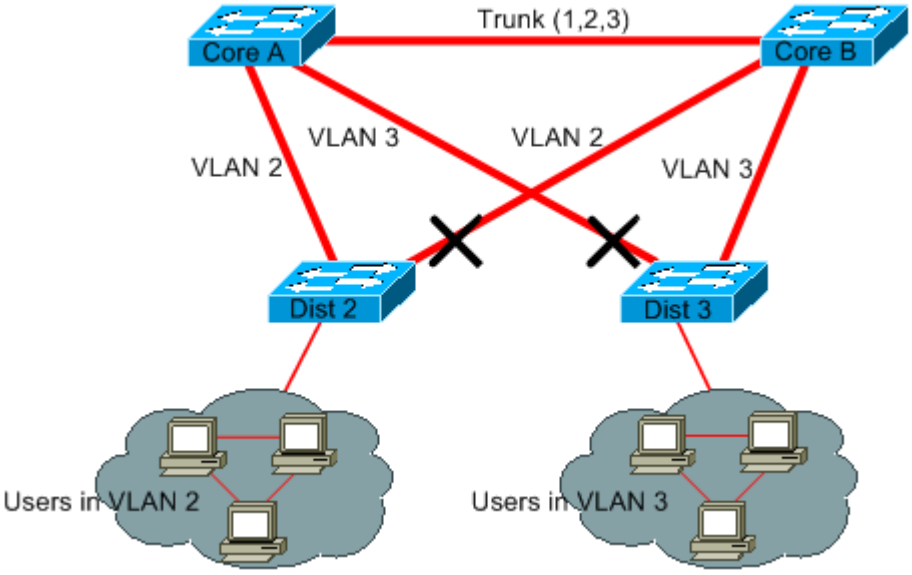


Les commutateurs de distribution sont à connexion double à deux commutateurs principaux. Les utilisateurs qui se connectent sur des commutateurs de distribution ne se trouvent que dans un sous-ensemble des VLAN disponibles sur le réseau. Dans cet exemple, les utilisateurs qui se connectent sur le Dist 2 sont tous dans le VLAN 2 ; Dist 3 connecte uniquement les utilisateurs dans VLAN 3. Par défaut, les agrégations transportent tous les VLAN définis dans le domaine VTP (VLAN Trunk Protocol). Seul Dist 2 reçoit le trafic de diffusion et de multidiffusion inutile pour VLAN 3, mais il bloque également l’un de ses ports pour VLAN 3. Il en résulte trois chemins redondants entre Core A et Core B. Cette redondance entraîne un plus grand nombre de ports bloqués et une probabilité plus élevée de bouclage.

Remarque : Éliminez les VLAN dont vous n’avez pas besoin de vos trunks.

L’élagage VTP réduit le trafic inondé inutile pour les VLAN éligibles, mais la configuration explicite trunk allowed-VLAN fournit un positionnement VLAN déterministe. Ne considérez pas l’élagage VTP comme un remplacement pour la suppression des VLAN inutilisés des listes d’agrégation autorisées.

Dans cet exemple, seul un VLAN d'accès est utilisé pour connecter les commutateurs de distribution au coeur :



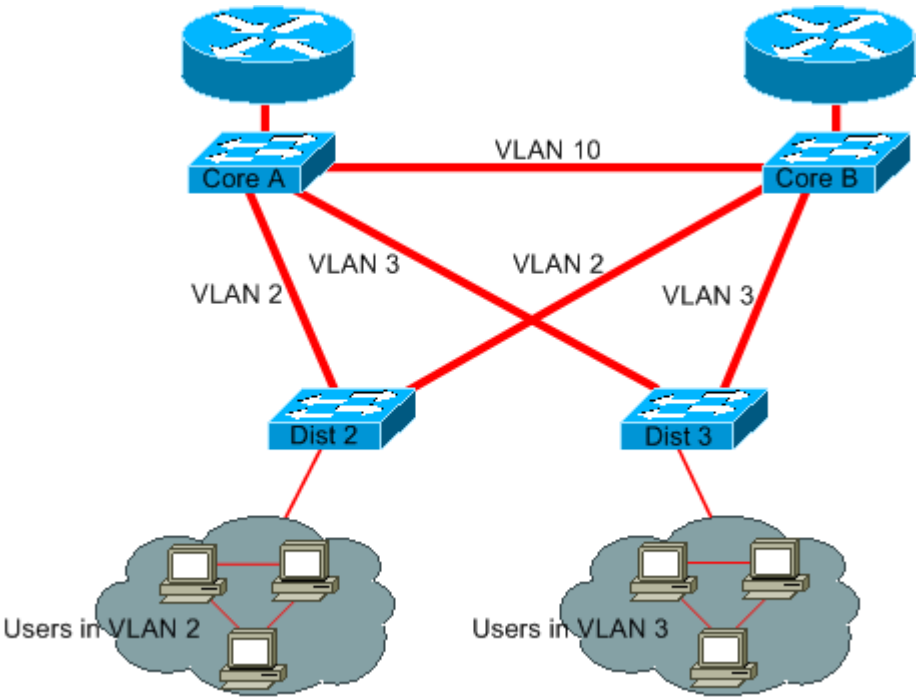
Dans cette conception, un seul port est bloqué par VLAN. En outre, avec cette conception, vous pouvez supprimer toutes les liaisons redondantes en une seule étape si vous arrêtez le coeur A ou le coeur B.

Utiliser la commutation de couche 3

La commutation de couche 3 signifie un routage approximativement à la vitesse de la commutation. Un routeur remplit deux fonctions principales :

- Un routeur crée une table de transfert. Le routeur échange généralement des informations avec des homologues via des protocoles de routage.
- Un routeur reçoit des paquets et les transmet à l'interface appropriée en fonction de l'adresse de destination.

Les commutateurs haut de gamme Cisco de couche 3 sont en mesure d'exécuter cette fonction, à la même vitesse que la fonction de commutation de couche 2. Si vous introduisez un saut de routage et créez une segmentation supplémentaire du réseau, il n'y a aucune pénalité de vitesse. Ce schéma utilise l'exemple dans la section Élaguer les VLAN que vous n'utilisez pas comme base :



Le coeur A et le coeur B sont désormais des commutateurs de couche 3. VLAN 2 et VLAN 3 ne sont plus pontés entre Core A et Core B, de sorte qu'une boucle STP ne peut pas traverser cette frontière routée. Les boucles de couche 2 restent possibles dans chaque VLAN ponté.

- La redondance est toujours présente et repose sur les protocoles de routage de couche 3. La conception utilise le routage de couche 3 pour la redondance des chemins. Le temps de convergence dépend du protocole de routage, du mécanisme de détection des défaillances, des minuteurs, de la topologie et de la plate-forme.
- Il n'y a plus de port unique que le STP bloque. Par conséquent, il n'y a pas de potentiel pour une boucle de pontage.
- Il n'y a aucune pénalité de vitesse, car quitter le VLAN par la commutation de couche 3 est aussi rapide que le pontage à l'intérieur du VLAN.

Il y a un seul inconvénient avec cette conception. La migration vers ce type de conception implique généralement une refonte du schéma d’adressage.

Conservez STP même si cela n'est pas nécessaire

Même si vous avez réussi à supprimer tous les ports bloqués de votre réseau et que vous n'avez aucune redondance physique, ne désactivez pas STP. Le protocole STP ne sollicite généralement pas beaucoup le processeur ; la commutation de paquets n'implique pas le processeur dans la plupart des commutateurs Cisco. En outre, les quelques BPDU qui sont envoyées sur chaque liaison ne réduisent pas de manière significative la bande passante disponible. Cependant, un réseau en pont sans STP peut fondre en une fraction de seconde si un opérateur fait une erreur

sur un tableau de connexions, par exemple. En général, la désactivation du protocole STP dans un réseau en pont ne vaut pas le coup.

Maintenez le trafic hors du VLAN d'administration et n'avez pas de VLAN unique sur l'ensemble du réseau

Un commutateur Cisco possède généralement une adresse IP unique qui se lie à un VLAN, appelé VLAN d’administration. Dans ce VLAN, le commutateur se comporte comme un hôte IP générique. Le trafic de diffusion, de multidiffusion et de plan de contrôle dans le VLAN d'administration peut consommer des ressources CPU, selon le type de trafic, la plate-forme, la version du logiciel et la configuration du plan de contrôle. Un taux élevé de trafic de diffusion ou de multidiffusion sur le VLAN d'administration peut avoir un impact négatif sur le CPU et sur sa capacité à traiter des BPDU vitales. Par conséquent, éloignez le trafic utilisateur du VLAN d'administration.

Dans les versions précédentes, il n'y avait aucun moyen de supprimer VLAN 1 d'une agrégation dans l'implémentation Cisco. Le VLAN 1 sert généralement de VLAN administratif, où tous les commutateurs sont accessibles dans le même sous-réseau IP. Bien qu'utile, cette configuration peut être dangereuse car une boucle de pontage sur VLAN 1 affecte toutes les agrégations, ce qui peut mettre hors service l'ensemble du réseau. Bien sûr, le même problème existe quel que soit le VLAN que vous utilisez. Essayez de segmenter les domaines de pontage en utilisant des commutateurs de couche 3 haut débit.

Depuis la version 12.1(11b)E du logiciel Cisco IOS, vous pouvez supprimer VLAN 1 des agrégations. Le VLAN 1 reste présent, mais il peut améliorer la sécurité et réduire le trafic inutile de couche 2.

Informations connexes

- Catalogue des outils d'assistance Cisco
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.