Problèmes liés au protocole STP (Spanning Tree Protocol) et considérations de conception

Contenu

Introduction

Ce document présente une liste de recommandations qui aident à mettre en application un réseau sécurisé en ce qui concerne le pontage pour des commutateurs Cisco Catalyst exécutant Catalyst OS (CatOS) et le logiciel Cisco IOS®. Ce document évoque certaines des raisons courantes pour

lesquelles le Protocole Spanning Tree (STP) peut échouer et les informations qu'il faut rechercher pour identifier la source du problème. Le document montre également le type de conception qui réduit au minimum les problèmes liés au spanning tree et qui est facile à dépanner.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Ce document n'évoque pas le fonctionnement de base de STP. Pour apprendre comment le STP fonctionne, référez-vous à ce document :

- Présentation et configuration du protocole Spanning Tree (STP) sur les commutateurs Catalyst

Ce document n'évoque pas le STP rapide (RSTP) défini dans IEEE 802.1w. En outre, ce document n'évoque pas le protocole MSTP (Multiple Spanning Tree Protocol), défini dans IEEE 802.1s. Pour plus d'informations sur RSTP et MST, référez-vous à ces documents :

- Présentation du protocole Multiple Spanning Tree (MSTP) (802.1s)
- Présentation du protocole Rapid Spanning Tree (STP) (802.1w)

Pour un document de dépannage de STP spécifique pour les commutateurs Catalyst exécutant le logiciel Cisco IOS, se référez au document Dépannage de STP sur un commutateur Catalyst exécutant Cisco IOS intégré (mode natif).

Panne de Protocole Spanning Tree

La fonction principale de l'algorithme Spanning Tree (STA) est de couper les boucles créées par des liens redondants dans des réseaux pontés. Le STP fonctionne sur la couche 2 du modèle d'Open System Interconnection (OSI). À l'aide d'unités de données de protocole de pont (BPDU) qui s'échangent entre les ponts, le STP choisit les ports qui par la suite expédient ou bloquent le trafic. Ce protocole peut échouer dans certains cas spécifiques et le dépannage de la situation en résultant peut être très difficile, cela dépend de la conception du réseau. Dans cette zone particulière, vous effectuez la partie la plus importante du dépannage avant que le problème ne se pose.

Une panne dans le STA mène généralement à 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 est rarement la cause. Même si le logiciel est le problème, une boucle de pontage dans un environnement STP vient toujours d'un port qui devrait bloquer le trafic, mais à la place le transmet.

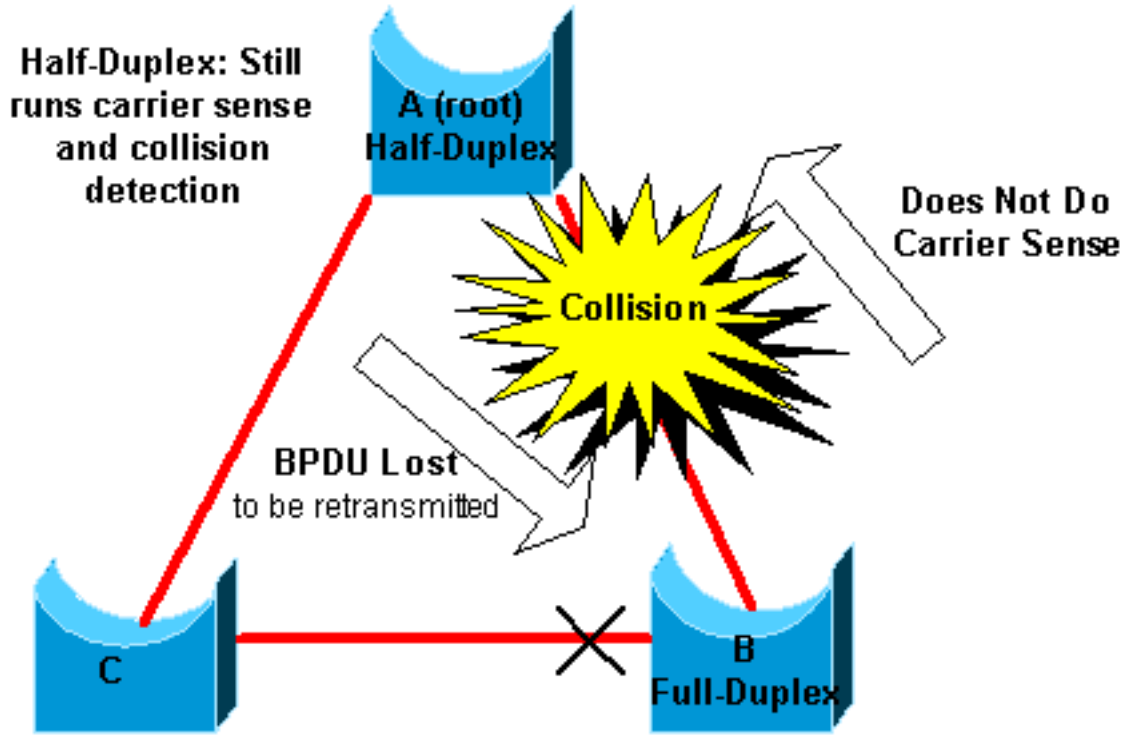
Convergence du spanning tree

Référez-vous à l'animation Flash sur le spanning tree pour voir un exemple expliquant comment le spanning tree converge au début. L'exemple explique également pourquoi un port bloqué passe en mode de transmission en raison d'une perte excessive de BPDU, ayant pour résultat la panne STA.

Le reste de ce document mentionne les différentes situations qui peuvent faire échouer le STA. La plupart de ces pannes sont associées à une perte massive de BPDU. La perte entraîne la transition des ports bloqués en mode de transmission.

Non-correspondance de mode duplex

L'erreur de correspondance de duplex sur une liaison point à point est une erreur de configuration très courante. Si vous paramétré manuellement le mode duplex sur Intégral d'un côté de la liaison et que vous laissez l'autre côté en mode autonégociation, la liaison finit par être en semi-duplex. (Un port en mode duplex paramétré sur Intégral ne négocie plus.)



Le pire scénario est quand un pont qui envoie des BPDU a le mode duplex paramétré sur semi-duplex sur un port, mais que le port pair à l'autre extrémité de la liaison a le mode duplex paramétré sur duplex intégral. Dans l'exemple ci-dessus, l'erreur de correspondance de duplex sur la liaison entre les ponts A et B peut facilement mener à une boucle de pontage. Puisque le pont B a une configuration pour le duplex intégral, il n'exécute pas la 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 d'attente avant que le pont n'essaye une autre transmission de la trame. S'il y a assez de trafic de B à A, chaque paquet que A envoie, qui inclut les BPDU, subit le renvoi ou la collision

et finalement est supprimé. Du point de vue du STP, comme le pont B ne reçoit plus de BPDU de A, le pont B a perdu le pont racine. Ceci mène B à débloquer le port connecté au pont C, ce qui crée la boucle.

Chaque fois qu'il y a une erreur de correspondance de duplex, ces messages d'erreur sont sur les consoles des commutateurs Catalyst qui exécutent CatOS et le logiciel Cisco IOS :

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

Logiciel Cisco IOS

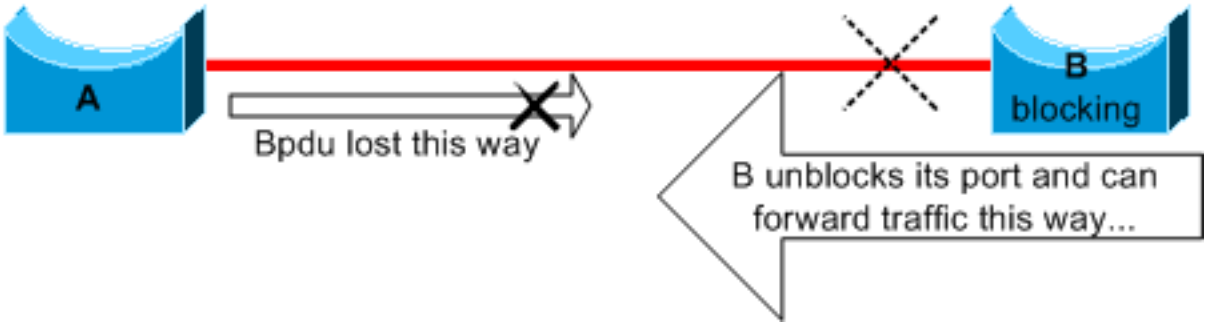
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

Contrôlez les paramètres de duplex et, s'il n'y a pas correspondance dans la configuration de duplex, paramétrez la configuration convenablement.

Pour plus d'informations sur la façon de dépanner une erreur de correspondance de duplex, référez-vous au document Configuration et dépannage de la négociation automatique semi-duplex/duplex intégral pour Ethernet 10/100/1 000 Mb.

Liaison unidirectionnelle

Les liaisons unidirectionnelles sont une cause classique d'une boucle de pontage. Sur des liaisons par fibre, une panne sans détection entraîne souvent des liaisons unidirectionnelles. Une autre cause est un problème avec un transmetteur. Tout ce qui peut mener une liaison à se maintenir et à fournir une communication à sens unique est très dangereux en ce qui concerne le STP. Cet exemple l'illustre :



Ici, supposez que la liaison entre A et B est unidirectionnelle. Les baisses de lien trafiquent d'A à B tandis que le lien communique le trafic de B à A. Assume qui jettent un pont sur B bloquaient avant que le lien soit devenu unidirectionnel. Cependant, un port peut seulement bloquer s'il reçoit des BPDU du pont qui a une plus grande priorité. Puisque, dans ce cas, toutes les BPDU qui viennent de A sont perdues, le pont B fait passer son port vers A à l'état de transmission et transmet le trafic. Ceci crée une boucle. Si cette panne existe au démarrage, le STP ne converge pas correctement. Dans le cas d'une erreur de correspondance de duplex, une 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 mise en application le protocole UniDirectional Link Detection (UDLD). Cette fonctionnalité peut détecter un câblage incorrect ou des liaisons unidirectionnelles sur la couche 2 et automatiquement casser les boucles en résultant en désactivant certains ports. Exécutez

l'UDLD partout où c'est possible dans un environnement ponté.

Pour plus d'informations sur l'utilisation de l'UDLD, référez-vous au document Compréhension et configuration de la fonctionnalité du protocole UDLD (Unidirectional Link Detection).

Corruption de paquet

La corruption de paquet peut également mener au même genre de panne. Si une liaison à un taux élevé d'erreurs physiques, vous pouvez perdre un certain nombre de BPDU consécutives. Cette perte peut mener un port bloquant à passer à l'état de transmission. Vous ne voyez pas ce cas très souvent parce que les paramètres par défaut du STP sont très conservateurs. Le port bloquant doit manquer des BPDU pendant 50 secondes avant la transition vers la transmission. La transmission réussie d'une seule BPDU casse la boucle. Ce cas se produit généralement avec le réglage négligent des paramètres du STP. Un exemple de réglage est la réduction de l'âge maximum.

Une erreur de correspondance de duplex, de mauvais câbles, ou une longueur de câble incorrecte peuvent entraîner la corruption de paquet. Référez-vous au document Dépannage du port de commutation et de l'interface pour une explication sur la sortie du compteur d'erreurs de CatOS et du logiciel Cisco IOS.

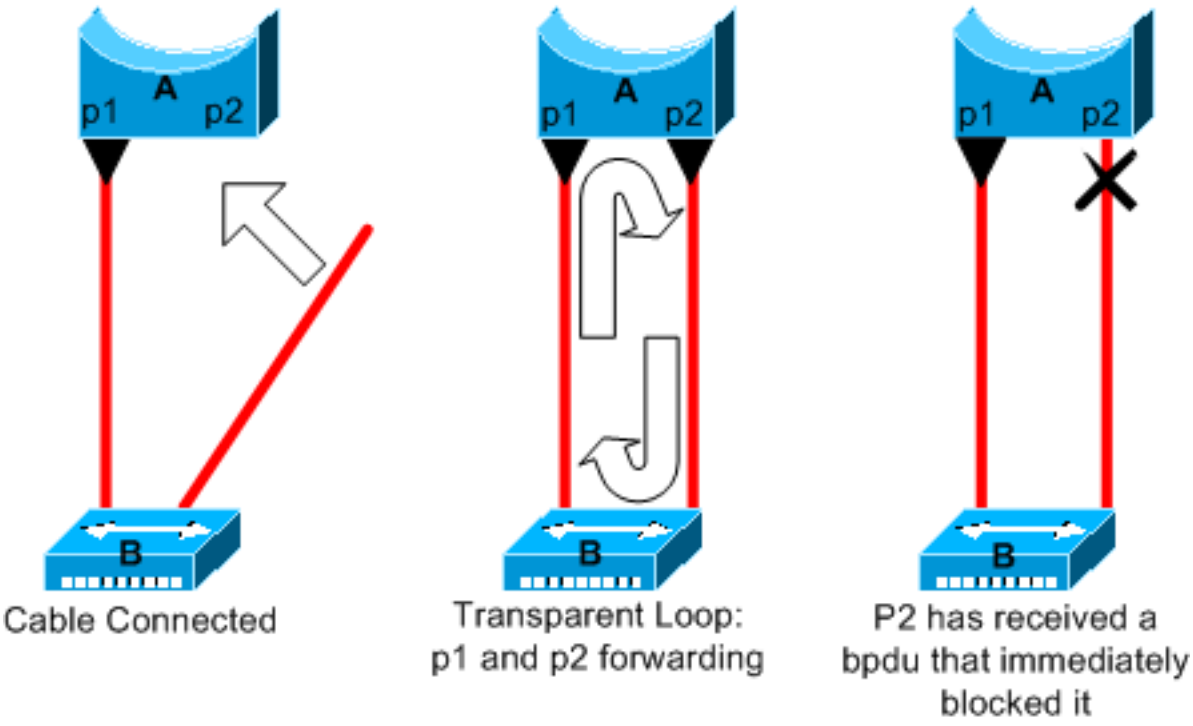
Erreurs de ressource

Le STP est mis en application dans le logiciel, même sur des commutateurs de pointe qui remplissent la plupart des fonctions de commutation dans le matériel avec des circuits intégrés spécifiques à l'application spécialisés (ASIC). Si pour une raison quelconque il y a un surutilisation du CPU du pont, les ressources peuvent être insuffisantes pour la transmission de BPDU. Le STA ne fait généralement pas un usage intensif du processeur et a la priorité sur les autres processus. La section Recherche des erreurs de ressource de ce document fournit quelques directives sur le nombre d'instances de STP qu'une plate-forme particulière peut gérer.

Erreur de configuration de PortFast

PortFast est une fonctionnalité que vous activez généralement seulement pour un port ou une interface qui se connecte à un hôte. Quand la liaison est établie sur ce port, le pont saute les premières étapes du STA et passe directement en mode de transmission.

Attention : N'utilisez pas la fonctionnalité PortFast sur des ports de commutation ou des interfaces qui se connectent à d'autres commutateurs, concentrateurs ou routeurs. Sinon, vous risquez de créer une boucle dans le réseau.



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 BPDU qui met un de ces deux ports en mode de blocage. Mais il y a un problème avec ce genre de boucle temporaire. Si le trafic dans la boucle est très intensif, le pont peut avoir des difficultés avec la bonne transmission de la BPDU qui va arrêter la boucle. Ce problème peut retarder considérablement la convergence ou mettre le réseau en panne dans des cas extrêmes.

Pour plus d'informations sur l'utilisation correcte PortFast sur des commutateurs exécutant CatOS et le logiciel Cisco IOS, référez-vous au document Utilisation de PortFast et d'autres commandes pour éliminer les retards de connectivité de démarrage du poste de travail.

Même avec une configuration PortFast, le port ou l'interface participe toujours dans le STP. Si un commutateur avec une priorité de pont inférieure à celle du pont racine actuellement actif se connecte à un port ou une interface configuré(e) pour PortFast, il peut être désigné comme pont racine. Cette modification du pont racine peut défavorablement affecter la topologie STP active et peut rendre le réseau non optimal. Pour empêcher cette situation, la plupart des commutateurs Catalyst exécutant CatOS et le logiciel Cisco IOS ont une fonctionnalité nommée BPDU Guard. Le BPDU Guard désactive un port ou une interface configuré(e) pour PortFast si le port ou l'interface reçoit une BPDU.

Pour plus d'informations sur l'utilisation de la fonctionnalité BPDU Guard sur des commutateurs exécutant CatOS et le logiciel Cisco IOS, référez-vous au document Amélioration du BPDU Guard de Portfast pour spanning tree.

Problèmes difficiles d'optimisation de paramètre et de diamètre STP

Une valeur agressive pour le paramètre d'âge maximum et le retard de transmission peut mener à une topologie STP très instable. En pareil cas, la perte de certaines BPDU peut faire apparaître une boucle. Un autre problème qui n'est pas bien connu est associé au diamètre du réseau ponté. Les valeurs par défaut conservatrices pour les temporisateurs STP imposent un diamètre de réseau maximal de sept. Ce diamètre de réseau maximal limite la distance à laquelle les ponts

peuvent être les uns par rapport aux autres dans le réseau. Dans ce cas, deux ponts distincts ne peuvent pas être à plus de sept sauts l'un de l'autre. Une partie de cette restriction vient du champ d'âge que les BPDU portent.

Quand une BPDU se propage du pont racine vers les terminaux de l'arborescence, le champ d'âge s'incrémente chaque fois que la BPDU passe par un pont. Finalement, le pont rejette la BPDU quand le champ d'âge dépasse l'âge maximum. Si la racine est trop loin de certains ponts du réseau, ce problème peut se produire. Ce problème affecte la convergence du spanning tree.

Faites particulièrement attention si vous prévoyez d'utiliser une valeur autre que la valeur par défaut pour les temporisateurs STP. Il y a danger si vous essayez d'obtenir un reconvergence plus rapide de cette façon. Une modification de temporisateur STP a une incidence sur le diamètre du réseau et la stabilité du STP. Vous pouvez changer la priorité du pont pour sélectionner le pont racine et changer le coût de transmission ou le paramètre de priorité pour contrôler la redondance et l'équilibrage de charge.

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

- La macro-commande **set spantree root [secondary]** réduit la priorité du pont de sorte qu'il devienne la racine (ou une racine alternative). Une option supplémentaire est disponible pour cette commande, permettant d'ajuster les temporisateurs STP en spécifiant le diamètre de votre réseau. Même lorsque c'est correctement fait, l'ajustement des temporisateurs n'améliore pas de manière significative le temps de convergence et introduit certains risques d'instabilité dans le réseau. En outre, ce genre d'ajustement doit être mis à jour à chaque fois qu'un périphérique est ajouté au réseau. Gardez les valeurs par défaut conservatrices qui sont bien connues des ingénieurs réseau.
- La commande **set spantree uplinkfast** pour CatOS ou la commande **spanning-tree uplinkfast** pour le logiciel Cisco IOS augmente la priorité du commutateur de sorte que le commutateur ne puisse pas être la racine. La commande augmente le temps de convergence STP en cas de défaillance de la liaison ascendante. Utilisez cette commande sur un commutateur de distribution avec double connexion à certains commutateurs principaux. Référez-vous au document Compréhension et configuration de la fonctionnalité Cisco UplinkFast.
- La commande **set spantree backbonefast enable** pour CatOS ou la commande **spanning-tree backbonefast** pour le logiciel Cisco IOS peut augmenter le temps de convergence STP du commutateur en cas de défaillance d'une liaison indirecte. BackboneFast est une fonctionnalité propriétaire de Cisco. Référez-vous au document Compréhension et configuration de Backbone Fast sur des commutateurs Catalyst.

Pour plus d'informations sur les temporisateurs STP et les règles pour les ajuster quand c'est absolument nécessaire, référez-vous au document Compréhension et ajustement des temporisateurs du Protocole Spanning Tree.

Erreurs logicielles

Comme mentionné dans l'introduction, le STP est l'une des premières fonctionnalités qui a été mise en application dans des produits Cisco. Vous pouvez attendre de cette fonctionnalité qu'elle soit très stable. Seule l'interaction avec de nouvelles configurations, telles que l'EtherChannel, a entraîné l'échec de STP dans quelques cas très spécifiques qui ont été maintenant résolus. Un certain nombre de facteurs différents peuvent entraîner un bogue logiciel et peuvent avoir un certain nombre d'effets différents. Il n'y a aucune façon de décrire convenablement les problèmes

qu'un bogue peut introduire. La situation la plus dangereuse qui résulte d'erreurs logicielles est si vous ignorez certaines BPDU ou, d'une façon générale, si vous avez une transition de port bloquant à transférer.

Résoudre une panne

Malheureusement, il n'y a aucune procédure systématique pour résoudre 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 employer une approche plus conventionnelle pour identifier d'autres pannes du STP qui mènent à une perte de connectivité. Par exemple, vous pouvez explorer le chemin que prend le trafic qui a un problème.

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

Si vous disposez de la sortie d'une commande **show-tech support** de votre dispositif Cisco, vous pouvez utiliser l'outil Output Interpreter (clients enregistrés uniquement) pour afficher les problèmes potentiels ainsi que les correctifs.

Utiliser le schéma du réseau

Avant que vous dépanniez une boucle de pontage, vous devez connaître ces éléments, au minimum :

- La topologie du réseau ponté
- L'emplacement du pont racine
- L'emplacement des ports bloqués et des liens redondants

Cette connaissance est essentielle pour au moins ces deux raisons :

- Afin de savoir quoi dépanner dans le réseau, vous devez savoir comment le réseau se présente quand il fonctionne correctement.
- La majeure partie des étapes de dépannage utilisent simplement des commandes **show** pour essayer d'identifier des conditions d'erreur. La connaissance du réseau vous aide à vous concentrer sur les ports critiques sur les équipements clés.

Identifier une boucle de pontage

Auparavant, une saturation de diffusion pouvait avoir un effet désastreux sur le réseau. Aujourd'hui, avec les liaisons haut débit et les périphériques qui fournissent la commutation au niveau matériel, il est peu probable qu'un hôte simple, par exemple un serveur, mette en panne un réseau par des diffusions. La meilleure façon d'identifier une boucle de pontage est de saisir le trafic sur une liaison saturée et de vérifier que vous voyez des paquets semblables plusieurs fois. Normalement, cependant, si tous les utilisateurs dans un domaine de pont ont des problèmes de connectivité en même temps, vous pouvez déjà suspecter une boucle de pontage.

Contrôlez l'utilisation des ports sur vos périphériques et recherchez des valeurs anormales. Référez-vous à la section Contrôler l'utilisation des ports de ce document.

Sur les commutateurs Catalyst exécutant CatOS, vous pouvez facilement contrôler l'utilisation globale du fond de panier avec la commande show system. La commande indique l'utilisation actuelle du fond de panier du commutateur et spécifie également l'utilisation maximale et date de l'utilisation maximale. Une utilisation maximale inhabituelle vous montre s'il y a déjà eu une boucle de pontage sur ce périphérique.

Rétablir rapidement la connectivité et être prêt pour une autre fois

Désactiver les ports pour casser la boucle

Les boucles de pontage ont des conséquences extrêmement graves sur un réseau ponté. Les administrateurs n'ont généralement pas le temps pour rechercher la cause de la boucle et préfèrent rétablir la connectivité dès que possible. La façon de s'en sortir facilement dans ce cas est de désactiver manuellement chaque port qui fournit une redondance dans le réseau. Si vous pouvez identifier une partie du réseau qui est plus affectée, commencez à désactiver des ports dans cette zone. Ou, si possible, désactivez au début les ports qui devraient être bloquants. Chaque fois que vous désactivez un port, contrôlez pour voir si vous avez restauré la connectivité dans le réseau. En identifiant quel port désactivé arrête la boucle, vous identifiez également le chemin redondant où ce port est localisé. Si ce port devait être bloquant, vous avez probablement trouvé la liaison sur laquelle la panne est apparue.

Journaliser les événements STP sur les périphériques qui ont des ports bloqués

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

- La question de de de Softwareâ de Cisco IOS les événements de debug spanning-tree de commande EXEC pour activer STP mettent au point les informations. Émettez la commande de mode de configuration générale logging buffered pour saisir ces informations de débogage dans la mémoire tampon du périphérique.
- Le de de CatOSâ la commande par défaut du spantree 7 de set logging level augmente le niveau par défaut des événements qui associent à STP au niveau de débogage. Soyez sûr d'enregistrer un nombre maximal de messages dans la mémoire tampon du commutateur en utilisant la commande set logging buffer 500.

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

Contrôler les ports

Les ports critiques à étudier d'abord sont les ports de blocage. Cette section fournit une liste d'éléments à rechercher sur les différents ports, avec une description rapide des commandes à émettre pour les commutateurs exécutant CatOS et le logiciel Cisco IOS.

Vérifier que les ports bloqués reçoivent des BPDU

Particulièrement sur les ports bloqués et les ports à la racine, vérifiez que vous recevez des BPDU périodiquement. Plusieurs problèmes peuvent mener un port à ne pas recevoir de paquets ou de BPDU.

- Le de de Softwareâ de Cisco IOS dans Logiciel Cisco IOS version 12.0 ou plus tard, sortie du passerelle-*groupe # de la* commande de **show spanning-tree** a un champ BPDU. Le champ vous montre le nombre de BPDU reçues pour chaque interface. Émettez la commande une ou deux fois de plus pour déterminer si le périphérique reçoit des BPDU.Si vous n'avez pas le champ BPDU dans la sortie de la commande **show spanning-tree**, vous pouvez activer le débogage de STP avec la commande **debug spanning-tree** pour vérifier la réception de BPDU.
- Le de de CatOSâ la commande de *module/port de* **show mac** t'indique le nombre de paquets de multidiffusion qu'un port spécifique reçoit. Mais la commande la plus simple à utiliser est la commande **show spantree statistics modules#/port#/vlan#**. Cette commande affiche le nombre exact de BPDU de configuration qu'un port spécifique a reçu sur un VLAN spécifique. Un port peut appartenir à plusieurs VLAN en cas de liaison de jonction. Voyez la section Une commande supplémentaire de CatOS de ce document.

Vérifier s'il y a une erreur de correspondance de duplex

Pour rechercher une erreur de correspondance de duplex, vous devez contrôler chaque côté de la liaison point à point.

- La question de de de Softwareâ de Cisco IOS l'**exposition relie [la** commande d'**état d'interface-***nombre d'interface***]** de vérifier l'état de la vitesse et le duplex du port spécifique.
- Le de de CatOSâ les toutes premières lignes de la sortie de la commande du **show port** *module#/port#* te donnent le la vitesse et le duplex selon la configuration des ports.

Contrôler l'utilisation du port

Une interface avec une surcharge du trafic peut échouer dans la transmission de BPDU essentielles. Une surcharge de la liaison indique également une possible boucle de pontage.

- Utilisation de de de Softwareâ de Cisco IOS que l'**exposition de** commande **relie** pour déterminer l'utilisation sur une interface. Plusieurs champs vous aident dans cette détermination, tel que load et packets input/output. Référez-vous au document Dépannage du port de commutation et de l'interface pour une explication sur la sortie de la commande **show interfaces**.
- Le de de CatOSâ la commande du **show mac** *module#/port#* affiche des statistiques au sujet des paquets qu'un port reçoit et envoie. La commande **show top** évalue automatiquement l'utilisation du port sur une période de 30 secondes et affiche le résultat. La commande classe les résultats pourcentage d'utilisation de la bande passante, bien que d'autres options pour la classification de résultats soient disponibles. En outre, la commande **show system** donne une indication de l'utilisation du fond de panier, bien que la commande n'indique pas un port spécifique.

Contrôler la corruption de paquet

- Le de de Softwareâ de Cisco IOS recherchent des incréments d'erreur dans le `compteur input errors de la` commande d'interfaces d'exposition. Les compteurs d'erreurs incluent des trames incomplètes, des trames géantes, l'absence de mémoire tampon, le CRC, des trames erronées, le dépassement de capacité et des trames ignorées.Référez-vous au document Dépannage du port de commutation et de l'interface pour une explication sur la sortie de la commande **show interfaces**.
- Le de de CatOSâ le **show port** *module#/port# de* commande te fournit quelques détails avec l'Aligner-`errement, FCS-erre, Xmit-erre, Rcv-Err,` et les champs `trop petits`. La commande **show counters module#/port#** fournit des statistiques de manière encore plus détaillée.

Une commande supplémentaire de CatOS

La commande **show spantree statistics module#/port# vlan#** fournit des informations très précises au sujet d'un port spécifique. Émettez cette commande sur les ports que vous suspectez et prêtez une attention particulière à ces champs :

- Le `en avant de` de `countâ transport` ce compteur se souvient combien de fois des transitions d'un port d'apprendre à la transmission. Dans une topologie stable, ce compteur affiche toujours 1. Ce compteur se remet à 0 quand le port se désactive et s'active. Ainsi, une valeur supérieure à 1 indique que la transition effectuée par le port est le résultat d'un recalcul de STP. La transition n'est pas le résultat d'une défaillance de liaison directe.
- `L'échéance maximum` d'`âge de` de `countâ` ce compteur dépiste le nombre de fois que l'âge maximum a expirées sur ce lien. Fondamentalement, un port qui attend des BPDU attend l'âge maximum avant que le port ne considère le pont désigné comme perdu. L'âge maximum par défaut est de 20 secondes. Chaque fois que cet événement se produit, le compteur est incrémenté. Quand la valeur n'est pas 0, cela indique que le pont désigné pour ce LAN est instable ou a un problème avec la transmission de BPDU.

Rechercher des erreurs de ressource

Un utilisation élevée du CPU peut être dangereux pour un système qui exécute le STA. Employez cette méthode pour vérifier que la ressource CPU est adéquate pour un périphérique :

- Question de de de Softwareâ de Cisco IOS la commande de **show processes cpu**. Vérifiez que l'utilisation du CPU n'est pas trop élevée. Pour les commutateurs de la gamme Catalyst 4500/4000 exécutant CatOS ou le logiciel Cisco IOS, référez-vous au document Utilisation du CPU sur les commutateurs Catalyst 4500/4000, 2948G, 2980G et 4912G.
- Question de de de CatOSâ la commande **CPU de show proc** d'afficher les informations d'utilisation du processeur. Vérifiez que l'utilisation du CPU n'est pas trop élevée.

Il y a une limitation sur le nombre d'instances différentes de STP que le supervisor engine peut gérer. Assurez-vous que le nombre total de ports logiques à travers 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 mémoire.

Émettez la commande **show spantree summary** pour les commutateurs exécutant CatOS ou la commande **show spanning-tree summary totals** pour les commutateurs exécutant le logiciel Cisco IOS. Ces commandes affichent le nombre de ports logiques ou d'interfaces par VLAN dans la colonne STP Active. Le total apparaît en bas de cette colonne. Le total représente la somme de tous les ports logiques à travers toutes les instances de STP pour les différents VLAN. Assurez-

vous que ce numéro ne dépasse pas le nombre maximal pris en charge pour chaque type de Supervisor Engine.

Remarque: La formule pour calculer la somme des ports logiques sur le commutateur est :

```
(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 récapitulatif des restrictions pour STP qui s'appliquent aux commutateurs Catalyst, référez-vous à ces documents :

Plate-forme	Restrictions STP avec CatOS	Restrictions STP avec le logiciel Cisco IOS
Catalyst 6500/6000 Supervisor Engine I et II	Dépannage de STP	Dépannage du spanning tree
Supervisor Engine 720 Catalyst 6500/6000	Dépannage de STP	Dépannage du spanning tree
Catalyst 5500/5000	Spanning Tree	de d'â
Catalyst 4500/4000	Spanning Tree	Dépannage du spanning tree
Catalyst 3750	de d'â	Configuration de STP
Catalyst 3550	de d'â	Configuration de STP
Catalyst 2970	de d'â	Configuration de STP
Catalyst 2950/2955	de d'â	Configuration de STP
Catalyst 2940	de d'â	Configuration de STP
Catalyst 2900/3500XL	de d'â	Configuration de STP

Désactiver les fonctionnalités inutiles

Le dépannage est une question d'identification de ce qui est actuellement incorrect dans le réseau. Désactivez autant de fonctionnalités que possible. La désactivation aide à simplifier la structure du réseau et facilite l'identification du problème. Par exemple, EtherChanneling est une fonctionnalité qui exige que le STP regroupe au niveau logique plusieurs liaisons différentes en une seule ; la désactivation de cette fonctionnalité pendant le dépannage est utile. En règle générale, simplifier la configuration autant que possible rend le dépannage du problème plus facile.

Commandes utiles

Commandes du logiciel Cisco IOS

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

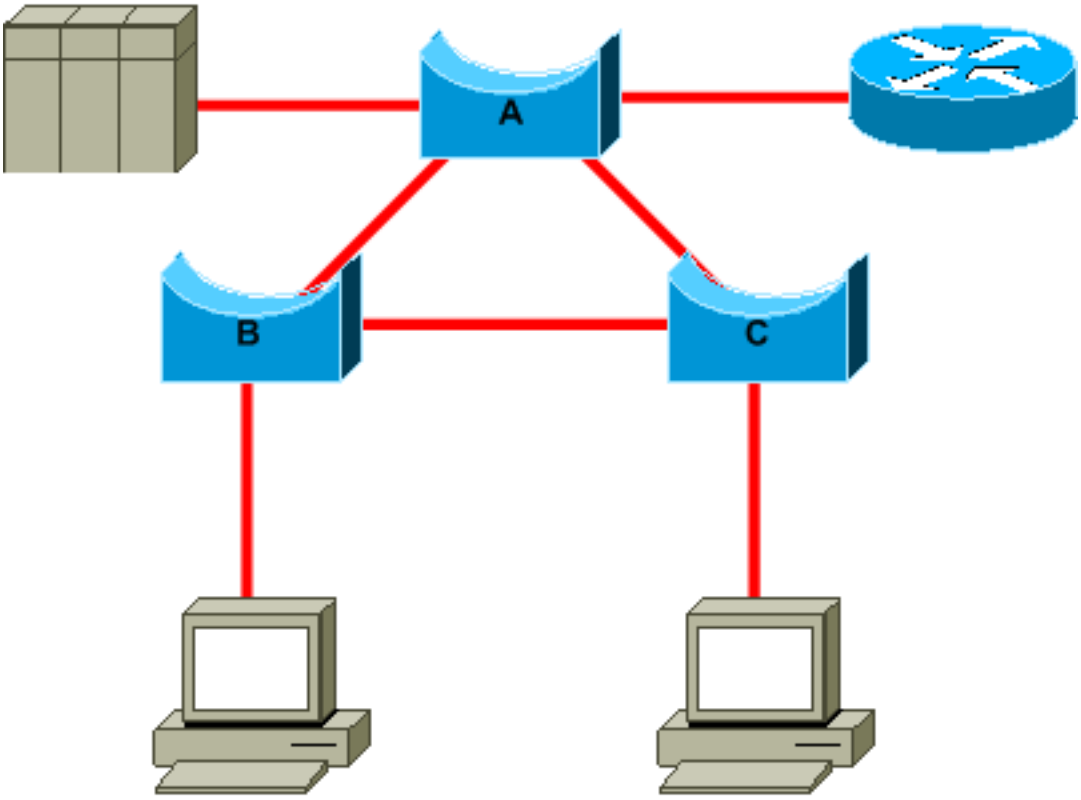
Commandes CatOS

- show port
- show mac
- show spantree
- show spantree statistics
- show spantree blockedports
- show spantree summary
- show top
- show proc cpu
- show system
- show counters
- set spantree root [secondary]
- set spantree uplinkfast
- set logging level
- set logging buffered

Concevoir le 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 quittez pas le STP pour décider quel pont est la racine. Pour chaque VLAN, vous pouvez habituellement identifier quel commutateur peut le mieux servir de racine. Ceci dépend de la conception du réseau. Généralement, choisissez un pont puissant au milieu du réseau. Si vous mettez le pont racine au centre du réseau avec connexion directe aux serveurs et aux routeurs, vous réduisez généralement la distance moyenne des clients aux serveurs et aux routeurs.



Ce diagramme montre :

- Si la passerelle B est racine, liez A au C est bloqué sur la passerelle A ou la passerelle C. dans ce cas, les hôtes qui se connectent au commutateur B peuvent accéder au serveur et le routeur en deux sauts. Les serveurs 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 derrière cet exemple s'applique aux topologies plus complexes.

Remarque importante : pour chaque VLAN, codez en dur le pont racine et le pont racine de secours avec une réduction de la valeur du paramètre de priorité de STP. Ou vous pouvez utiliser l'instruction-macro set spantree root.

Savoir où se trouve la redondance

Prévoyez l'organisation de vos liens redondants. Oubliez la fonctionnalité prête à l'emploi de STP. Ajustez le paramètre de coût de STP pour décider quels ports bloquent. Cet ajustement n'est généralement pas nécessaire si vous avez une conception hiérarchique et un pont racine à un bon emplacement.

Remarque importante : Pour chaque VLAN, sachez quels ports devraient bloquer dans le réseau stable. Ayez un diagramme de réseau qui montre clairement chaque boucle physique dans le réseau et quels ports bloqués cassent les boucles.

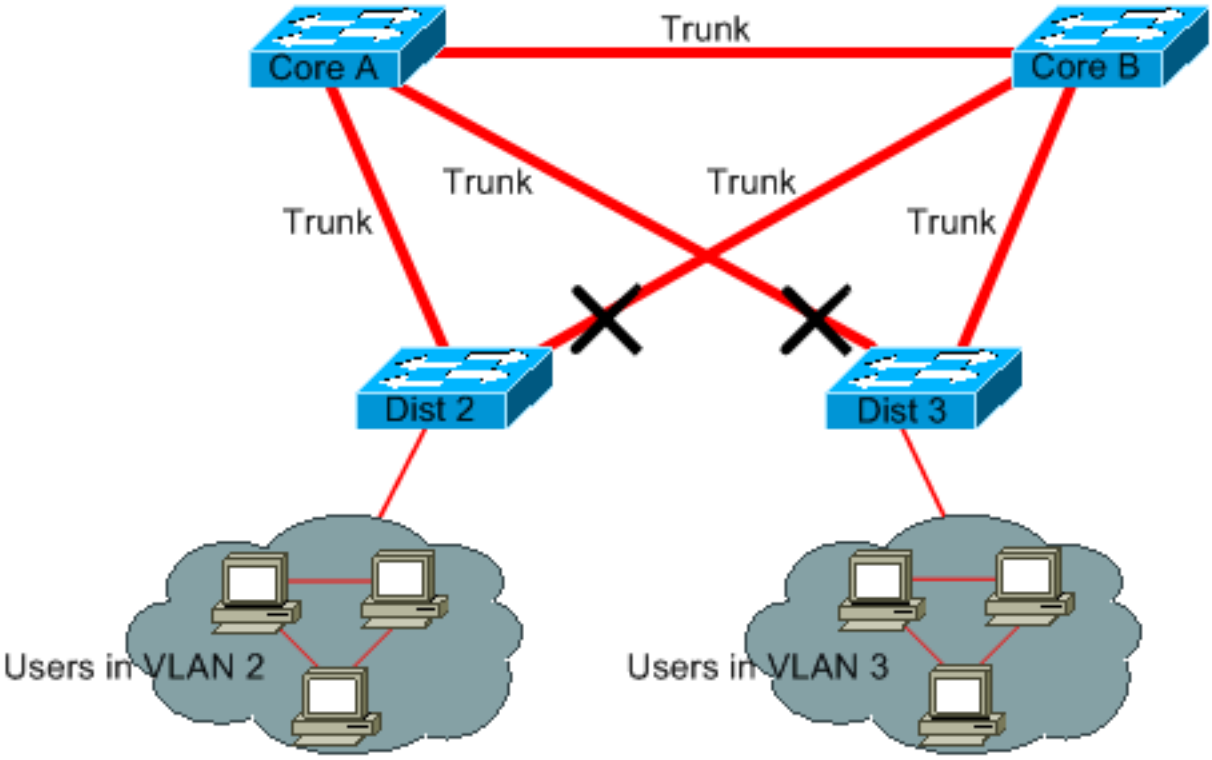
La connaissance de l'emplacement des liens redondants vous aide à identifier une boucle de pontage accidentelle et la cause. En outre, la connaissance de l'emplacement des ports bloqués vous permet de déterminer l'emplacement de l'erreur.

Réduire au minimum le nombre de ports bloqués

La seule action critique que prend le STP est le blocage des ports. Un simple port bloquant qui passe de manière erronée à la transmission peut faire s'écrouler une grande partie du réseau. Une bonne façon de limiter le risque inhérent à l'utilisation du STP est de réduire le nombre de ports bloqués autant que possible.

Élaguer les VLAN que vous n'utilisez pas

Vous n'avez pas besoin de plus de deux liens redondants entre deux nœuds dans a réseau ponté. Cependant, ce genre de configuration est commun :

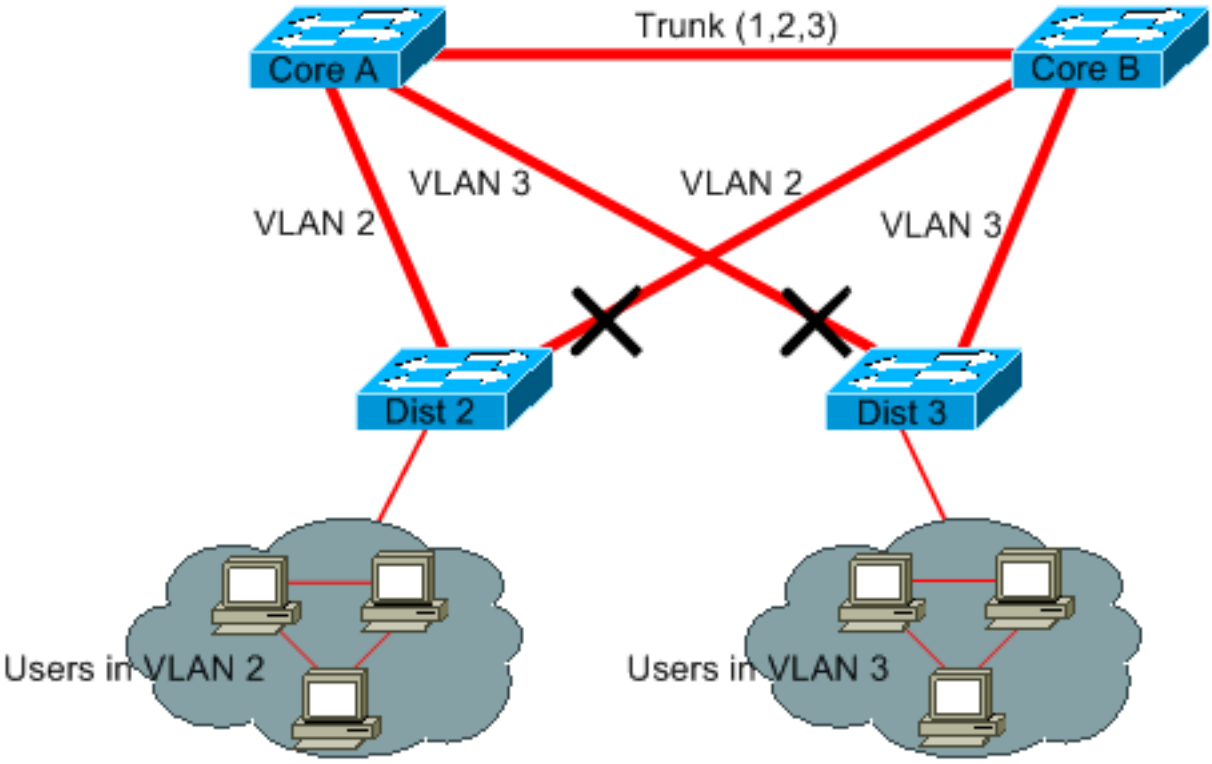


Les commutateurs de distribution ont une double connexion aux deux commutateurs principaux. Les utilisateurs qui se connectent sur des commutateurs de distribution sont seulement dans un sous-ensemble des VLAN disponibles dans le réseau. Dans cet exemple, les utilisateurs qui se connectent sur Dist 2 sont tous dans le VLAN 2 ; Dist 3 connecte seulement les utilisateurs dans le VLAN 3. Par défaut, les jonctions portent tous les VLAN définis dans le domaine du protocole de jonction VLAN (VTP). Seul Dist 2 reçoit un trafic de diffusion et de multidiffusion inutile pour le VLAN 3, mais il bloque également l'un de ses ports pour le VLAN 3. Le résultat est trois chemins redondants entre le noyau A et le noyau B. Cette redondance a comme conséquence plus de ports bloqués et une probabilité plus élevée d'avoir une boucle.

Remarque importante : Élaguez n'importe quel VLAN dont vous n'avez pas besoin sur vos jonctions.

L'élagage de VTP peut être une aide, mais ce genre de fonctionnalité prête à l'emploi n'est pas nécessaire dans le noyau du réseau.

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



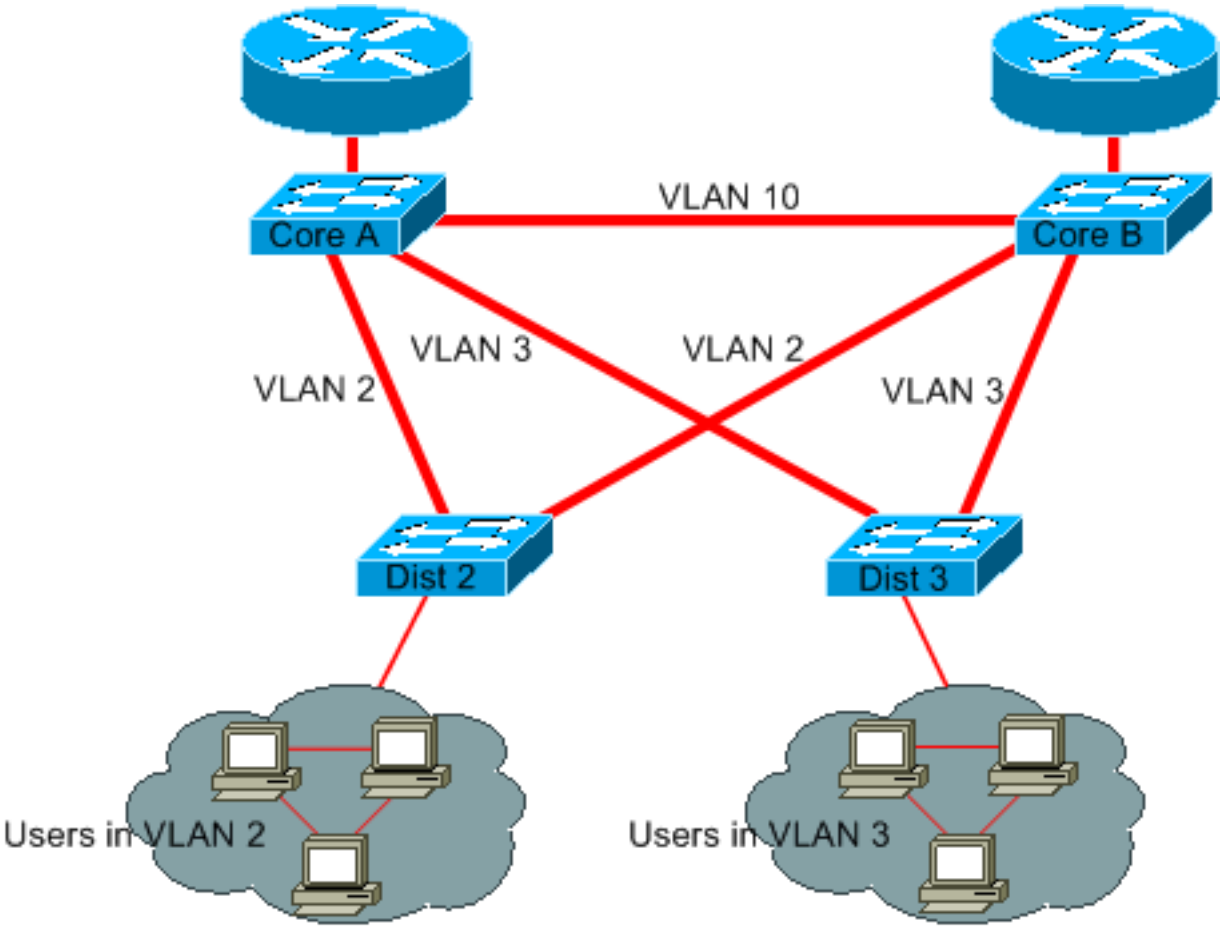
Dans cette conception, seul un port est bloqué par le VLAN. En outre, avec cette conception, vous pouvez éliminer tous les liens redondants en une seule étape si vous arrêtez le noyau A ou le noyau B.

Utiliser la commutation de couche 3

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

- Un routeur établit une table de transmission. Le routeur échange généralement des informations avec des homologues à l'aide de protocoles de routage.
- Un routeur reçoit des paquets et les transmet à la bonne interface en fonction de l'adresse de destination.

Les commutateurs de point Cisco de couche 3 peuvent maintenant exécuter cette seconde fonction à la même vitesse que la fonction de commutation de la couche 2. Si vous introduisez un saut de routage et que vous créez une segmentation supplémentaire du réseau, il n'y a aucune pénalité de vitesse. Ce diagramme utilise l'exemple de la section Élaguer les VLAN que vous n'utilisez pas comme base :



Le noyau A et le noyau B sont maintenant des commutateurs de couche 3. Les VLAN 2 et VLAN 3 ne sont plus pontés entre le noyau A et le noyau B, il n'y a donc aucune possibilité pour une boucle de STP.

- La redondance est encore présente, avec une dépendance sur des protocoles de routage de la couche 3. La conception assure un reconvergence qui est encore plus rapide que le reconvergence avec STP.
- Il n'y a plus un seul port que STP bloque. Par conséquent, il n'y a aucun risque de boucle de pontage.
- Il n'y a aucune pénalité de vitesse car quitter le VLAN par commutation de couche 3 est aussi rapide que ponter à l'intérieur du VLAN.

Il y a un seul inconvénient avec cette conception. La migration vers ce genre de conception implique généralement une refonte du système d'adressage.

Garder le STP même si c'est inutile

Même si vous avez réussi à éliminer tous les ports bloqués du votre réseau et que vous n'avez aucune redondance physique, ne désactivez pas STP. Le STP ne fait généralement pas un usage très intensif du processeur ; la commutation par paquets n'implique pas le CPU dans la plupart des commutateurs Cisco. En outre, le peu de BPDU qui sont envoyées sur chaque lien ne réduit pas de manière significative la bande passante disponible. Cependant, un réseau ponté sans STP peut s'écrouler en une fraction de seconde si un opérateur fait une erreur sur un panneau de connexions, par exemple. Généralement, désactiver le STP dans un réseau ponté est un risque inutile.

Garder le trafic hors du VLAN d'administration et ne pas avoir un seul VLAN pour

tout le réseau

Un commutateur Cisco a typiquement une seule adresse IP qui est liée à un VLAN, connu sous le nom de VLAN d'administration. Dans ce VLAN, le commutateur se comporte comme un hôte IP générique. En particulier, chaque paquet de diffusion ou de multidiffusion est transmis au CPU. Un débit élevé du trafic de diffusion ou de multidiffusion sur le VLAN d'administration peut défavorablement affecter le CPU et la capacité du CPU à traiter des BPDU essentielles. Par conséquent, gardez le trafic hors du VLAN d'administration.

Jusqu'à récemment, il n'y avait pas possibilité de supprimer le VLAN 1 d'une jonction dans l'implémentation Cisco. Le VLAN 1 sert généralement de VLAN d'administration dans lequel tous les commutateurs sont accessibles dans le même sous-réseau IP. Bien qu'utile, cette configuration peut être dangereuse, parce qu'une boucle de pontage sur le VLAN 1 affecte toutes les jonctions, ce qui peut mettre en panne tout le réseau. Naturellement, le même problème existe quel que soit le VLAN que vous utilisez. Essayez de segmenter les domaines de pontage en utilisant des commutateurs haut débit de couche 3.

En date de CatOS version 5.4 et du logiciel Cisco IOS Version 12.1(11b)E, vous pouvez supprimer le VLAN 1 des jonctions. Le VLAN 1 existe toujours, mais il bloque le trafic, ce qui empêche toute possibilité de boucle.

Informations connexes

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