Pratiques recommandées pour les commutateurs des gammes Catalyst 6500/6000 et Catalyst 4500/4000 exécutant le logiciel Cisco IOS

Contenu

Informations connexes

Introduction

Ce document décrit les meilleures pratiques applicables aux commutateurs Catalyst 6500/6000 et 4500/4000 du logiciel Cisco IOS sur Supervisor Engine.

Les commutateurs Catalyst 6500/6000 et Catalyst 4500/4000 prennent en charge l'un des deux systèmes d'exploitation suivants, exécutés sur Supervisor Engine :

- Catalyst OS (CatOS)
- Logiciel Cisco IOS

Avec CatOS, vous pouvez utiliser le logiciel Cisco IOS sur des cartes fille ou des modules de routeur telles que :

- La fonction MFSC (Multilayer Switch Feature Card) de Catalyst 6500/6000
- Le module 4232 de la couche 3 (L3) de Catalyst 4500/4000

Dans ce mode, il y a deux lignes de commande pour la configuration :

- La ligne de commande CatOS pour la commutation
- La ligne de commande du logiciel Cisco IOS pour le routage

CatOS représente le logiciel système, qui est exécuté sur Supervisor Engine. Le logiciel Cisco IOS, qui fonctionne sur le module de routage, est une option qui exige le logiciel système CatOS.

Pour le logiciel Cisco IOS, il existe une seule ligne de commande pour la configuration. Dans ce mode, la fonctionnalité de CatOS a été intégrée au logiciel Cisco IOS. L'intégration a comme conséquence une ligne de commande unique pour la configuration de la commutation et du routage. Dans ce mode, le logiciel Cisco IOS est le logiciel système. Il remplace CatOS.

Chacun de ces deux systèmes d'exploitation (CatOS et le logiciel Cisco IOS) sont déployés sur des réseaux critiques. CatOS, avec le logiciel Cisco IOS pour les cartes fille et les modules de routeur, est pris en charge dans les séries de commutateurs suivantes :

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

Le logiciel système Cisco IOS est pris en charge dans les séries de commutateurs suivantes :

- Catalyst 6500/6000
- Catalyst 4500/4000

Pour plus d'informations sur CatOS, référez-vous au document intitulé Meilleures pratiques applicables aux commutateurs Catalyst 4500/4000, 5500/5000 et 6500/6000 utilisant les fonctions CatOS de configuration et de gestion ; en effet, le présent document traite du logiciel système Cisco IOS.

Le logiciel système Cisco IOS offre notamment aux utilisateurs les avantages suivants :

- Une interface utilisateur unique
- Une plate-forme unifiée d'administration de réseau

- Des fonctions Qos améliorées
- Une prise en charge de la commutation distribuée

Ce document fournit des conseils de configuration modulaires. Par conséquent, vous pouvez lire chacune des sections indépendamment et apporter des modifications dans une approche par étapes. Ce document suppose une compréhension et une connaissance de base de l'interface utilisateur du logiciel Cisco IOS. Il ne couvre pas la conception globale de réseau campus.

Avant de commencer

Fond

Les solutions que ce document décrit représentent des années d'expérience terrain des ingénieurs Cisco, qui travaillent avec des réseaux complexes et des clients qui font partie des plus grands comptes du marché. Par conséquent, ce document souligne les configurations réelles qui assurent la réussite des réseaux. Ce document traite des solutions suivantes :

- Solutions qui bénéficient statistiquement de l'exposition la plus large sur le terrain et sont ainsi à faible risque.
- Solutions simples qui sacrifient une part de flexibilité pour des résultats déterministes.
- Solutions faciles à gérer et configurées par des équipes d'exploitation du réseau.
- Solutions qui favorisent une forte disponibilité et une forte stabilité.

Références

Il y a beaucoup de sites de référence pour les gammes de produits Catalyst 6500/6000 et Catalyst 4500/4000 sur le site Cisco.com. Les références que cette section mentionne fournissent des informations supplémentaires sur les sujets traités par ce document.

Référez-vous à la prise en charge de la technologie de commutation LAN pour plus d'informations sur les sujets abordés dans ce document. La page d'assistance fournit la documentation produit et les documents de dépannage et de configuration.

Ce document fournit des références à une documentation publique en ligne, que vous pourrez lire ultérieurement. Voici d'autres références intéressantes en matière de formation :

- Considérations de base ISP Cisco
- Comparaison des systèmes d'exploitation Cisco Catalyst et Cisco IOS pour les commutateurs Cisco Catalyst 6500
- Commutation LAN Cisco - Développement professionnel CCIE
- Mise en oeuvre de réseaux commutés multicouches Cisco
- Gestion des performances et des pannes
- SÉCURITAIRE: Un modèle de sécurité pour des réseaux d'entreprise
- Cisco Field Manual (Manuel Cisco): Configuration des commutateurs Catalyst

Configuration de base

Cette section décrit les fonctions déployées quand vous utilisez la plupart des réseaux Catalyst.

Protocoles de plan de contrôle Catalyst

Cette section présente les protocoles qui sont exécutés entre les commutateurs dans un mode de fonctionnement normal. Une compréhension de base des protocoles est utile quand vous abordez chacun section.

Trafic de Supervisor Engine

La plupart des fonctionnalités qui sont activées au sein d'un réseau Catalyst exigent deux commutateurs ou davantage. Par conséquent, il doit y avoir un échange contrôlé des messages keepalive, des paramètres de configuration et des modifications de gestion. Que ces protocoles soient la propriété de Cisco (comme par exemple le protocole CDP Cisco Discovery Protocol), ou qu'ils soient basés sur des normes (comme par exemple le protocole IEEE 802.1D STP Spanning-Tree Protocol), tous ont certains éléments en commun quand les protocoles sont mis en application sur la série Catalyst.

Dans la transmission de trame de base, les trames de données utilisateur proviennent des systèmes d'extrémité. L'adresse source (SA) et l'adresse de destination (DA) des trames de données ne sont pas changées dans les domaines commutés de la couche 2 (L2). Les tables de recherche associatives de mémoire (CAM) sur chacun des moteurs Supervisor Engine sont alimentées par un processus d'apprentissage SA. Les tableaux indiquent quel port de sortie transmet chaque trame reçue. Si la destination est inconnue ou si la trame est destinée à une adresse de diffusion ou à une adresse multicast, le processus d'apprentissage d'adresse est incomplet. Quand le processus est incomplet, les trames sont transmises à tous les ports de ce VLAN. Le commutateur doit également identifier les trames qui doivent être commutées par le système et celles qui doivent être dirigées vers le CPU du commutateur lui-même. Le CPU du commutateur est également appelé processeur NMP (Network Management Processor).

Des entrées spéciales de la table CAM sont utilisées pour créer le plan de contrôle Catalyst. Ces entrées spéciales s'appellent entrées système. Le plan de contrôle reçoit et dirige le trafic vers le processeur NMP sur un port de commutation interne. Ainsi, à l'aide des protocoles dotés d'adresses MAC de destination bien connues, le trafic du plan de contrôle peut être séparé du trafic de données.

Cisco possède une plage réservée d'adresses MAC Ethernet et d'adresses de protocole, comme l'indique le tableau de cette section. Ce document couvre en détail chacune de ces adresses réservées, mais un récapitulatif est présenté dans ce tableau pour un aperçu rapide :

Fonctionnalité	Type de protocole SNAP[1] HDLC[2]	Adresse MAC multipoint de destination
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+, RPVST+[4]	0x010b	01-00-0c-cc-cc-cd
Pont VLAN	0x010c	01-00-0c-cd-cd-ce
UDLD[5]	0x0111	01-00-0c-cc-cc-cc
CDP	0 x 2 000	01-00-0c-cc-cc-cc
DTP[6]	0x2004	01-00-0c-cc-cc-cc
UplinkFast STP	0 x 200 a	01-00-0c-cd-cd-cd

IEEE spanning tree 802.1D	S/O : DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00
ISL[9]	S/O	01-00-0c-00-00-00
VTP [10]	0x2003	01-00-0c-cc-cc-cc
IEEE Pause 802.3x	S/O — DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

[1] SNAP = Subnetwork Access Protocol.

[2] HDLC = High-Level Data Link Control.

[3] PAgP = Protocole d'agrégation de ports.

[4] PVST+ = Per VLAN Spanning Tree+ et RPVST+ = Rapid PVST+.

[5] UDLD = UniDirectional Link Detection.

[6] DTP = Dynamic Trunking Protocol.

[7] DSAP = point d'accès au service de destination.

[8] SSAP = point d'accès au service source.

[9] ISL = Inter-Switch Link.

[10] VTP = VLAN Trunk Protocol.

La majorité des protocoles de contrôle Cisco utilise une encapsulation SNAP IEEE 802,3, qui inclut le contrôle LLC (Logical Link Control) 0xAAAA03 et l'identifiant OUI (Organizational Unique Identifier) 0x00000C. Vous pouvez voir ceci sur une trace d'analyseur LAN.

Ces protocoles assument la connectivité point par point. Notez que l'utilisation délibérée des adresses de destination multicast permet à deux commutateurs Catalyst de communiquer d'une manière transparente sur des commutateurs non Cisco. Les périphériques, qui ne comprennent pas les trames et les interceptent, les propagent simplement. Cependant, les connexions point-à-multipoint établies par les environnements multi-constructeurs peuvent avoir comme conséquence un comportement incohérent. Évitez en général les connexions point-à-multipoint en environnements multi-constructeurs. Ces protocoles se terminent au niveau des routeurs de la couche 3 et fonctionnent uniquement au sein d'un domaine de commutation. Ces protocoles sont considérés comme prioritaires par rapport aux données utilisateur dans le cadre du traitement et de la programmation par circuit intégré d'entrée à application spécifique (ASIC).

Maintenant cette section va décrire les SA. Les protocoles de commutation utilisent une adresse MAC issue d'une banque d'adresses disponibles. Une EPROM sur le châssis fournit la banque d'adresses disponibles. Émettez la commande **show module afin d'afficher les plages d'adresses disponibles pour chaque module, pour l'élaboration de trafic (BPDU STP ou trames ISL).** Voici un exemple de sortie de commande :

```
>show module
…

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)      6.1(1d)
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
!--- These are the MACs for sourcing traffic.
```

VLAN 1

VLAN 1 a une importance spéciale dans les réseaux Catalyst.

Lors de la liaison de jonction, Catalyst Supervisor Engine utilise toujours le VLAN par défaut, VLAN 1, afin de baliser un certain nombre de protocoles de contrôle et de gestion. De tels protocoles incluent CDP, VTP, et PAgP. Tous les ports de commutation, qui incluent l'interface interne sc0, sont configurés par défaut pour être des membres du réseau VLAN 1. Toutes les jonctions portent VLAN 1 par défaut.

Ces définitions sont nécessaires afin de clarifier la signification de certains termes fréquemment utilisés sur les réseaux Catalyst :

- Le VLAN de gestion correspond à l'emplacement de sc0 pour les commutateurs CatOS et bas de gamme. Vous pouvez changer ce VLAN. Souvenez-vous lorsque vous mettez en réseau des commutateurs CatOS et Cisco IOS.
- Le VLAN natif est le VLAN vers lequel un port revient lorsqu'il n'est pas en liaison de jonction. En outre, le VLAN natif est le VLAN non balisé sur une jonction IEEE 802.1Q.

Voici plusieurs bonnes raisons de configurer un réseau et de modifier le comportement des ports dans le VLAN 1 :

- Quand le diamètre du VLAN 1, comme n'importe quel autre VLAN, devient assez grand pour être un risque à la stabilité (en particulier d'un point de vue STP), il doit être rétréci. Reportez-vous à la section Interface de gestion du commutateur et VLAN natif pour plus d'informations.
- Vous devez maintenir les données de plan de contrôle du réseau VLAN 1 séparées des données utilisateur afin de simplifier le dépannage et de maximiser les cycles CPU disponibles. Évitez les boucles de la couche 2 dans le VLAN 1 quand vous concevez des réseaux campus multicouches sans STP. Afin d'éviter les boucles de la couche 2, supprimez manuellement le VLAN1 des ports de jonction.

En résumé, notez ces informations sur les liaisons :

- Les mises à jour CDP, VTP et PAgP sont toujours transmises sur les liaisons dotées d'une balise VLAN 1. C'est le cas même si VLAN 1 a été effacé des liaisons réseau et n'est pas le VLAN natif. Si vous effacez le VLAN1 pour des données utilisateur, l'action n'a aucune incidence sur le trafic du plan de contrôle, qui est encore envoyé via l'utilisation du VLAN 1.
- Sur une liaison ISL, les paquets DTP sont envoyés sur VLAN1. C'est le cas même si VLAN 1 a été effacé de la liaison et n'est plus le VLAN natif. Sur une liaison 802.1Q, les paquets DTP sont envoyés sur le VLAN natif. C'est le cas même si le VLAN natif a été effacé de la jonction.
- Dans PVST+, les 802.1Q IEEE BPDU sont expédiées sans balise sur le Spanning Tree VLAN1 commun pour une interopérabilité avec d'autres constructeurs, à moins que VLAN 1 n'ait été effacé de la liaison. C'est le cas indépendamment de la configuration du VLAN natif. Les PVST+ BPDU Cisco sont transmis et balisés pour tous les autres VLAN. Pour plus

d'informations, reportez-vous à la section consacrée au protocole STP Spanning-Tree Protocol .
- Les BPDU 802.1s Multiple Spanning Tree (MST) sont toujours envoyés sur le VLAN 1 via des liaisons ISL et 802.1Q. Ceci s'applique même lorsque VLAN 1 a été effacé des jonctions.
- N'effacez pas et ne désactivez pas VLAN 1 sur les liaisons entre des ponts MST et des ponts PVST+. Mais si VLAN 1 est désactivé, le pont MST doit devenir racine pour éviter que celui-ci ne mette ses ports de borne dans l'état racine contradictoire. Référez-vous à la section Comprendre le protocole Multiple Spanning Tree (802.1s) pour plus de détails.

Fonctionnalités standard

Cette section du document se concentre sur les fonctionnalités de base de commutation qui sont communes à n'importe quel environnement. Configurez ces fonctionnalités sur tous les périphériques de commutation Catalyst du logiciel Cisco IOS du réseau client.

Protocole VTP

Objectif

Un domaine VTP, également appelé domaine de gestion de VLAN, se compose d'un ou de plusieurs commutateurs interconnectés par l'intermédiaire d'une jonction qui partage le même nom de domaine VTP. VTP est conçu pour permettre à des utilisateurs d'apporter des modifications de configuration VLAN centralement sur un ou plusieurs commutateurs. VTP communique automatiquement les changements à tous les autres commutateurs du domaine VTP (réseau). Vous pouvez configurer un commutateur pour qu'il se trouve uniquement dans un domaine VTP. Avant de créer des VLAN, déterminez le mode VTP à utiliser sur le réseau.

Aperçu opérationnel

VTP est un protocole de messagerie de la couche 2. Il contrôle l'ajout, la suppression de VLAN et l'affectation de nouveaux noms, au niveau du réseau entier, pour maintenir la cohérence de la configuration de réseau VLAN. VTP réduit au minimum les erreurs et les incohérences de configuration qui peuvent avoir comme conséquence un certain nombre de problèmes. Ces problèmes incluent des noms en double de VLAN, des caractéristiques incorrectes de type de VLAN et des violations de sécurité.

Par défaut, le commutateur est en mode de serveur VTP et dans l'état de domaine sans gestion. Ces configurations par défaut changent quand le commutateur reçoit une annonce pour un domaine sur une liaison de jonction ou quand un domaine de gestion est configuré.

Le protocole VTP communique entre les commutateurs avec l'utilisation d'une adresse Ethernet MAC multicast de destination bien connue (01-00-0c-cc-cc-cc) et un type de protocole SNAP HDLC 0x2003. Comme d'autres protocoles intrinsèques, VTP utilise également une encapsulation SNAP IEEE 802.3, qui inclut LLC 0xAAAA03 et OUI 0x00000C. Vous pouvez voir ceci sur une trace d'analyseur LAN. VTP ne fonctionne pas sur des ports sans agrégation. Par conséquent, les messages ne peuvent pas être envoyés avant que DTP ait établi la jonction. En d'autres termes, VTP est une charge utile d'ISL ou de 802.1Q.

Les types de messages incluent :

- Des annonces résumées toutes les 300 secondes (sec)
- Des annonces de sous-ensembles et des annonces de modifications
- Des messages d'arrivée lorsque l'élagage VTP est activé

Le numéro de révision de configuration VTP est incrémenté (de 1) à chaque modification sur un serveur, et des propagations de cette table ont lieu à travers le domaine.

Lors de la suppression d'un VLAN, les ports qui étaient membres du VLAN prennent l'`état inactif`. De même, si un commutateur en mode client ne peut pas recevoir la table VLAN VTP au démarrage (à partir d'un serveur VTP ou d'un autre client VTP), tous les ports dans les VLAN autres que le VLAN 1 par défaut sont mis hors fonction.

Vous pouvez configurer la plupart des commutateurs Catalyst pour qu'ils fonctionnent dans l'un des modes VTP suivants :

- Serveur — En mode serveur VTP, vous pouvez :Créer des VLANModifier des VLANSupprimer des VLANSpécifier d'autres paramètres de configuration, tels que la version VTP et l'élagage VTP, pour le domaine VTP entierLes serveurs VTP indiquent leur configuration VLAN aux autres commutateurs du même domaine VTP. Les serveurs VTP synchronisent également leur configuration VLAN avec celle des autres commutateurs, sur la base des annonces reçues via les liaisons de jonction. Le Serveur VTP est le mode par défaut.
- Client — Les clients VTP se comportent de la même façon que les serveurs VTP. Cependant, vous ne pouvez pas créer, modifier ou supprimer de VLAN sur un client VTP. De plus, le client ne se rappelle pas du VLAN après un redémarrage, car aucune information sur le VLAN n'est enregistrée dans NVRAM.
- Transparent — Les commutateurs VTP transparents ne participent pas à VTP. Un VTP transparent n'indique pas sa configuration VLAN et n'effectue pas de synchronisation sur la base des annonces reçues. Mais dans VTP version 2, les commutateurs transparents transmettent les annonces VTP que les commutateurs reçoivent via leurs interfaces de jonction.

Fonctionnalité	Serveur	Client	Transparence	Éteint [1]
Messages VTP sources	Oui	Oui	Non	—
Écouter les messages VTP	Oui	Oui	Non	—
Créer des VLAN	Oui	Non	Oui (significatif uniquement localement)	—
Rappeler les VLAN	Oui	Non	Oui (significatif uniquement localement)	—

[1] Le logiciel Cisco IOS n'a pas la possibilité de désactiver VTP avec l'utilisation du mode `off`.

Cette table constitue un récapitulatif de la configuration initiale :

Fonctionnalité	Valeur par défaut

Nom de domaine VTP	Null
Mode VTP	Serveur
Version VTP	La version 1 est activée
Élagage VTP	Désactivé

En mode VTP transparent, les mises à jour VTP sont simplement ignorées. L'adresse MAC multicast VTP connue est supprimée du CAM système normalement utilisé pour prendre des trames de contrôle et pour les diriger vers Supervisor Engine. Comme le protocole emploie une adresse multicast, le commutateur en mode transparent (ou un commutateur d'un constructeur différent) inonde simplement la trame vers les autres commutateurs Cisco du domaine.

VTP version 2 (VTPv2) inclut la flexibilité fonctionnelle que cette liste décrit. Mais VTPv2 n'est pas interopérable avec VTP version 1 (VTPv1) :

- Prise en charge de Token Ring
- Prise en charge des informations VTP non reconnues - Les commutateurs propagent maintenant des valeurs qu'ils ne peuvent pas analyser.
- Mode transparent dépendant de la version - Le mode transparent ne contrôle plus le nom de domaine. Ceci active la prise en charge de plusieurs domaines à travers un domaine transparent transparent.
- Propagation du numéro de version - Si VTPv2 est possible sur tous les commutateurs, tous les commutateurs peuvent être activés avec configuration d'un commutateur unique.

Pour plus d'informations, reportez-vous à Présentation du protocole VTP (VLAN Trunking Protocol).

Fonctionnement de VTP dans le logiciel Cisco IOS

Les changements de configuration dans CatOS sont écrits à NVRAM juste après qu'une modification soit faite. En revanche, le logiciel Cisco IOS n'enregistre pas les modifications de configuration dans NVRAM, sauf si vous émettez la commande **copy run start .** Le client VTP et les systèmes de serveur requièrent des mises à jour VTP d'autres serveurs VTP à enregistrer immédiatement dans NVRAM sans intervention de l'utilisateur. Les nécessités de mise à jour VTP sont satisfaites par l'opération CatOS par défaut, mais le modèle de mise à jour du logiciel Cisco IOS requiert une opération de mise à jour alternative.

Pour ce changement, une base de données VLAN a été introduite dans le logiciel Cisco IOS pour Catalyst 6500 comme une méthode pour sauvegarder immédiatement les mises à jour VTP pour des clients et des serveurs VTP. Dans certaines versions du logiciel, la base de données VLAN revêt la forme d'un fichier distinct dans NVRAM, appelé le fichier vlan.dat. Contrôlez votre version du logiciel afin de déterminer si une sauvegarde de la base de données VLAN est nécessaire. Vous pouvez afficher l'information VTP/VLAN qui est stockée dans le fichier vlan.dat pour le client VTP ou le serveur VTP si vous lancez la commande show vtp status.

La configuration totale du VTP/VLAN n'est pas sauvegardée dans le fichier de configuration de démarrage de NVRAM quand vous émettez la commande **copy run start sur ces systèmes.** Ceci ne s'applique pas aux systèmes exécutés comme transparent VTP. Les systèmes de VTP transparents sauvegardent l'ensemble de la configuration VTP/VLAN au fichier de configuration de démarrage dans NVRAM quand vous lancez la commande **copy run start.**

Dans des versions du logiciel Cisco IOS antérieures à la version 12.1(11b)E, vous pouvez seulement configurer VTP et des VLAN par l'intermédiaire du mode de base de données VLAN. Ce mode est un mode différent du mode de configuration globale. La raison de ces exigences de configuration est que, quand vous configurez le périphérique en mode de serveur VTP mode ou en mode de client VTP, VTP peut mettre à jour la base de données VLAN dynamiquement via les annonces VTP. Vous ne voulez pas que ces mises à jour soient automatiquement propagées dans la configuration. Par conséquent, les informations de la base de données VLAN et les informations VTP ne sont pas stockées dans la configuration principale, mais dans NVRAM (dans le fichier vlan.dat).

Cet exemple montre comment créer un VLAN Ethernet en mode de base de données VLAN :

```
Switch#vlan database
Switch(vlan)#vlan 3
VLAN 3 added:
Name: VLAN0003
Switch(vlan)#exit
APPLY completed.
Exiting....
```

Dans le Logiciel Cisco IOS Version 12.1(11b)E et versions ultérieures, vous pouvez configurer VTP et des VLAN par l'intermédiaire du mode de base de données VLAN ou via le mode de configuration globale. En mode serveur VTP ou en mode transparent VTP, la configuration des VLAN met à jour le fichier vlan.dat dans NVRAM. Cependant, ces commandes ne sont pas sauvegardées dans la configuration. Par conséquent, les commandes ne sont pas indiquées dans la configuration utilisée.

Référez-vous à la section Configuration de VLAN en mode de configuration globale du document Configuration des VLAN pour plus d'informations.

Cet exemple montre comment créer un VLAN Ethernet en mode de configuration globale et comment vérifier la configuration :

```
Switch#configure terminal
Switch(config#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config#vlan 3
Switch(config-vlan)#end
Switch#
OR
Switch#vlan database
Switch(vlan#vtp server
Switch device to VTP SERVER mode.
Switch(vlan#vlan 3
Switch(vlan#exit
APPLY completed.
Exiting....
Switch#
```

Remarque : La configuration VLAN est stockée dans le fichier vlan.dat, qui est stocké dans une mémoire non volatile. Pour effectuer une sauvegarde complète de votre configuration, le fichier vlan.dat doit être inclus dans la sauvegarde avec la configuration. Ensuite, si le commutateur ou le module Supervisor Engine doit être remplacé, l'administrateur réseau doit télécharger chacun des deux fichiers pour restaurer la configuration complète :

- Fichier vlan.dat

- Fichier de configuration

VTP et VLAN étendus

La fonction d'ID système étendu est utilisée pour activer l'identification de VLAN étendu. Une fois l'ID système étendu activée, elle désactive le pool d'adresses MAC utilisé pour Spanning-Tree et laisse une adresse MAC simple qui identifie le commutateur. Les versions 12.1(11b)EX et 12.1(13)E du logiciel Catalyst IOS introduisent la prise en charge des ID système étendus pour Catalyst 6000/6500 pour VLAN 4096, conformément à la norme IEEE 802.1Q. Cette fonction est introduite dans le logiciel Cisco IOS version 12.1(12c)EW pour commutateurs Catalyst 4000/4500. Ces VLAN sont organisés en plusieurs plages, qui peuvent être utilisées différemment. Certains de ces VLAN sont propagés à d'autres commutateurs du réseau quand vous utilisez VTP. Les VLAN étendus ne sont pas propagés, vous devez donc configurer les VLAN étendus manuellement, sur chaque périphérique réseau. Cette fonction d'ID système étendu est équivalente à la fonction de réduction d'adresses MAC de Catalyst OS.

Ce tableau décrit les plages de VLAN :

Réseaux locaux virtuels (VLAN)	Plage	Utilisation	Propagé par VTP ?
0, 4095	Réservé	Pour une utilisation système uniquement. Vous ne pouvez pas voir ou utiliser ces VLAN.	—
1	Normal	Valeur par défaut Cisco. Vous pouvez utiliser ce VLAN, mais vous ne pouvez pas le supprimer.	Oui
2–1001	Normal	Pour les VLAN Ethernet. Vous pouvez créer, utiliser et supprimer ces VLAN.	Oui
1002–1005	Normal	Valeurs par défaut Cisco pour FDDI et Token Ring. Vous ne pouvez pas supprimer les VLAN 1002-1005.	Oui
1006–4094	Réservé	Pour Les VLAN Ethernet seulement.	Non

Les protocoles de commutateurs utilisent une adresse MAC tirée d'une banque d'adresses disponibles qu'une EPROM sur le châssis fournit en tant qu'identifiants de ponts pour les VLAN qui exécutent PVST+ et RPVST+. Les commutateurs Catalyst 6000/6500 et Catalyst 4000/4500 supportent les adresses MAC 1024 ou 64, selon le type de châssis.

Les commutateurs Catalyst avec adresses MAC 1024 n'activent pas par défaut la fonction d'ID système étendu. Les adresses MAC sont allouées séquentiellement, avec la première adresse MAC dans la plage assignée au VLAN 1, la deuxième dans la plage assignée au VLAN 2, etc. Ceci permet aux commutateurs de prendre en charge les VLAN 1024, chaque VLAN utilisant un seul identifiant de pont.

Type de châssis	Adresse de châssis
WS-C4003-S1, WS-C4006-S2	1024
WS-C4503, WS-C4506	641
WS-C6509-E,WS-C6509, WS-C6509-NEB, WS-C6506-E, WS-C6506, WS-C6009, WS-C6006, OSR-7609-AC, OSR-7609-DC	1024
WS-C6513, WS-C6509-NEB-A, WS-C6504-E, WS-C6503-E, WS-C6503, CISCO7603, CISCO7606, CISCO7609, CISCO7613	641

[1] Le châssis doté de 64 adresses MAC active l'ID système étendu par défaut et ne peut pas être désactivé.

Référez-vous à la section Présentation de l'ID de pont de Configuration de MST STP et IEEE 802.1s pour plus d'informations.

Pour les commutateurs Catalyst avec adresses MAC 1024, l'activation de la fonction d'ID système étendu permet la prise en charge des VLAN exécutés sur des instances PVST+ ou 16 MISTP pour bénéficier d'identificateurs uniques sans augmentation du nombre d'adresses MAC requis sur le commutateur. La fonction d'ID système étendu permet de diminuer le nombre d'adresses MAC requis par STP (un par commutateur, et non un par VLAN ou par instance MISTP).

Cette figure montre l'identificateur de passerelle lorsque la fonction d'ID système étendu n'est pas activée. L'identifiant de passerelle se compose d'une priorité de pont à 2 octets et d'une adresse MAC à 6 octets.

La fonction d'ID système étendu modifie la partie d'identification STP (Spanning-Tree Protocol) des BPDU (Bridge Protocol Data Units). Le champ de priorité à 2 octets initial est coupé en 2 zones : Une zone de priorité de pont à 4 bits et une extension de l'ID système 12 bits qui tient compte de la numérotation VLAN 0-4095.

Une fois la fonction d'ID système étendu activée sur les commutateurs Catalyst pour les VLAN étendus, elle doit être activée sur tous les commutateurs du même domaine STP. Cela est nécessaire pour assurer la cohérence des calculs de racine STP sur tous les commutateurs. Une fois que cette fonction est activée, la priorité de pont racine devient un multiple de 4096 plus l'ID de VLAN. Les commutateurs sans ID système étendu peuvent éventuellement réclamer la racine par inadvertance, car ils ont une granularité plus fine dans la sélection d'ID de pont.

Il est recommandé de conserver une bonne cohérence de la configuration d'ID système étendu au sein d'un même domaine STP. Toutefois, il n'est pas pratique de mettre en oeuvre la fonction d'ID

système étendu sur tous les périphériques réseau lorsque vous introduisez un nouveau châssis avec adresses MAC 64 dans le domaine STP. Mais il est important de comprendre que quand deux systèmes sont configurés avec la même priorité Spanning-Tree, le système sans ID système étendu bénéficie d'une priorité Spanning Tree plus élevée. Émettez cette commande afin d'activer la configuration d'ID système étendu :

spanning-tree extend system-id

Les VLAN internes sont alloués par ordre croissant, en commençant par le VLAN 1006. Il est recommandé d'assigner les VLAN utilisateur aussi près de VLAN 4094 que possible afin d'éviter des conflits entre les VLAN utilisateur et les VLAN internes. Émettez la commande **show vlan internal usage sur un commutateur, afin d'afficher les VLAN assignés en interne.**

```
Switch#show vlan internal usage

VLAN Usage
---- --------------------
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
1010 online diag vlan4
1011 online diag vlan5
1012 PM vlan process (trunk tagging)
1013 Port-channel100
1014 Control Plane Protection
1015 L3 multicast partial shortcuts for VPN 0
1016 vrf_0_vlan0
1017 Egress internal vlan
1018 Multicast VPN 0 QOS vlan
1019 IPv6 Multicast Egress multicast
1020 GigabitEthernet5/1
1021 ATM7/0/0
1022 ATM7/0/0.1
1023 FastEthernet3/1
1024 FastEthernet3/2
------deleted------
```

Dans le logiciel IOS natif, **vlan internal allocation policy descending peut être configurée pour que les VLAN internes soient alloués par ordre décroissant.** La CLI équivalente pour CatOS n'est pas officiellement prise en charge.

vlan internal allocation policy descending

Recommandation de configuration Cisco

Des VLAN peuvent être créés quand un commutateur Catalyst 6500/6000 est en mode serveur VTP, même sans nom de domaine VTP. Configurez tout d'abord le nom de domaine VTP, avant que vous configuriez des VLAN sur des commutateurs Catalyst 6500/6000 exécutant le logiciel Cisco IOS. Une configuration dans cet ordre permet de maintenir une bonne cohérence avec les autres commutateurs Catalyst exécutant CatOS.

Il n'existe aucune recommandation spécifique dans le choix du mode client/serveur VTP ou VTP transparent. Certains clients préfèrent la facilité de la gestion du mode client/serveur VTP, en dépit de quelques considérations que cette section décrit. La recommandation est d'avoir deux commutateurs en server mode dans chaque domaine pour la redondance, généralement les deux

commutateurs de la couche distribution. Définissez le reste des commutateurs du domaine en mode client. Quand vous mettez en oeuvre client/server mode avec l'utilisation de VTPv2, souvenez-vous qu'un numéro de révision plus élevé est toujours accepté dans le même domaine VTP. Si un commutateur qui est configuré en mode client VTP ou server mode est introduit dans le domaine VTP et a un numéro de révision plus élevé que les serveurs existants de VTP, celui-ci remplace la base de données VLAN dans le domaine VTP. Si le changement de configuration est accidentel et que des VLAN sont supprimés, ce remplacement peut entraîner une panne importante du réseau. Afin de garantir que les commutateurs client ou serveur portent toujours un numéro de révision de configuration inférieur à celui du serveur, modifiez le nom de domaine VTP du client en utilisant un autre nom que le nom standard, puis rétablissez le nom standard. Cette action définit la révision de la configuration du client à 0.

Il y a le pour et le contre dans la capacité de VTP d'apporter des modifications facilement sur un réseau Beaucoup d'entreprises préfèrent une approche prudente et utilisent le VTP transparent pour les raisons suivantes et d'utilisation mode pour ces raisons :

- Cette pratique encourage le bon contrôle des modifications, parce que la condition de modification d'un VLAN sur un commutateur ou une jonction s'applique commutateur par commutateur.
- Le mode VTP transparent limite le risque d'erreurs de la part de l'administrateur (suppression accidentelle d'un VLAN, par exemple). De telles erreurs peuvent affecter le domaine entier.
- Des VLAN peuvent faire l'objet d'un élagage au niveau des commutateurs qui n'ont pas de ports au sein du VLAN. Cela optimise l'utilisation de la bande passante lors de l'inondation de trames. L'élagage manuel a également un diamètre Spanning-Tree réduit. Pour plus d'informations, reportez-vous à la section Dynamic Trunking Protocol . Une configuration de VLAN par commutateur encourage également cette pratique.
- Il n'y a aucun risque qu'un nouveau commutateur introduit dans le réseau avec un numéro de révision VTP plus élevé remplace la configuration VLAN du domaine tout entier.
- Le mode VTP transparent du logiciel Cisco IOS est pris en charge par Campus Manager 3.2, qui fait partie de CiscoWorks2000. La restriction antérieure exigeant de disposer d'un serveur minimum dans un domaine VTP a été supprimée.

Commandes VTP	**Commentaires**
Nom de domaine VTP	CDP contrôle le nom afin d'empêcher les erreurs de câblage entre les domaines. Les noms de domaine distinguent les majuscules et minuscules.
vtp mode {server | client | transparent}	VTP fonctionne dans l'un des trois modes.
vlan *vlan_number*	Cela crée un VLAN avec l'ID fourni.
switch	C'est une commande d'interface qui permet aux

port trunk allowed *vlan_range*	jonctions d'acheminer les VLAN vers la destination requise. La valeur par défaut est Tous les VLAN.
switchport trunk pruning *vlan_range*	C'est une commande d'interface qui limite le diamètre STP par élagage manuel, comme sur des jonctions entre la couche de distribution et la couche d'accès, où le VLAN n'existe pas. Par défaut, tous les VLAN peuvent être élagués.

Autres options

VTPv2 est une condition dans les environnements Token Ring, où le client/server mode est fortement recommandé.

La section Recommandation de configuration Cisco de ce document présente les avantages de l'élagage de VLAN pour réduire l'inondation inutile de trames. La commande **vtp pruning élague les VLAN automatiquement, ce qui arrête l'inondation inefficace des trames lorsqu'elles ne sont pas nécessaires.**

Remarque : Contrairement à l'élagage manuel des VLAN, l'élagage automatique ne limite pas le diamètre du Spanning Tree.

IEEE a produit une architecture fondée sur des standards afin d'obtenir des résultats semblables à ceux de VTP. En tant que membre du protocole GARP (Generic Attribute Registration Protocol) 802.1Q, le protocole GVRP (Generic VLAN Registration Protocol) permet l'interopérabilité de gestion VLAN entre les constructeurs. Cependant, GVRP est hors de portée de ce document.

Remarque : le logiciel Cisco IOS ne dispose pas de la fonctionnalité VTP off mode et prend uniquement en charge VTPv1 et VTPv2 avec élagage.

Autonégociation Fast Ethernet

Objectif

L'autonégociation est une fonction facultative de la norme IEEE 802.3u Fast Ethernet (FE). L'autonégociation permet aux périphériques d'échanger automatiquement des informations sur les capacités de vitesse et duplex d'une liaison. L'autonégociation fonctionne au niveau de la couche 1 (L1). La fonction est destinée à des ports qui sont alloués à des zones dans lesquelles des utilisateurs ou des périphériques temporaires se connectent à un réseau. Les exemples incluent des commutateurs et des concentrateurs de la couche d'accès.

Aperçu opérationnel

L'autonégociation utilise une version modifiée du test d'intégrité de liaison pour que les périphériques 10Base-T négocient et échangent d'autres paramètres d'autonégociation. Le test

d'intégrité de liaison 10Base-T initial est désigné sous le nom d'impulsion NLP (Normal Link Pulse). La version modifiée du test d'intégrité de liaison pour l'autonégociation 10/100-Mbps est désignée sous le nom d'impulsion FLP (Fast Link Pulse). Les périphériques 10Base-T s'attendent à une impulsion de rafale chaque 16 millisecondes (+/--8) en tant qu'élément du test d'intégrité de liaison. FLP pour l'autonégociation 10/100-Mbps envoie ces éclats chaque 16 millisecondes (+/--8) avec impulsions supplémentaires toutes les 62,5 microsecondes (+/--7). Les impulsions de la séquence de rafales produisent des mots de code qui sont utilisés pour les échanges de compatibilité entre les partenaires de liaison.

Dans 10BaseT, une impulsion de liaison est envoyée chaque fois qu'une station est activée. C'est une impulsion simple qui est envoyée toutes les 16 ms. Les périphériques 10Base-T envoient également une impulsion de liaison toutes les 16 millisecondes quand la liaison est inactive. Ces impulsions de liaison s'appellent également battement de coeur ou NLP.

Un périphérique 100BASE-T envoie une impulsion FLP. Cette impulsion est envoyée comme éclat au lieu d'une impulsion. La rafale est terminée en 2 ms et se répète toutes les 16 ms. Lors de l'initialisation, le périphérique transmet un message FLP 16 bits au partenaire de liaison pour la négociation de la vitesse, du mode duplex et du contrôle de flux. Ce message de 16 bits est envoyé de façon répétée, jusqu'à ce qu'un accusé de réception soit envoyé par le partenaire.

Remarque : Conformément à la spécification IEEE 802.3u, vous ne pouvez pas configurer manuellement un partenaire de liaison pour le mode bidirectionnel simultané à 100 Mbits/s et continuer à négocier automatiquement le mode bidirectionnel simultané avec l'autre partenaire de liaison. Une tentative de configuration d'un partenaire de liaison pour le full-duplex 100-Mbps et de l'autre partenaire de liaison pour l'autonégociation a comme conséquence une erreur de correspondance de duplex. L'erreur de correspondance de duplex résulte du fait qu'un partenaire autonégocie et ne voit aucun paramètre d'autonégociation en provenance de l'autre partenaire de liaison. Le premier partenaire de liaison est configuré par défaut en mode half-duplex.

Tous les modules de commutation Catalyst 6500 Ethernet prennent en charge 10/100 Mbps et half-duplex ou full-duplex. Émettez la commande **show interface capabilities afin de vérifier cette fonctionnalité sur d'autres commutateurs Catalyst.**

L'un des problèmes les plus communs en termes de performance sur les liaisons Ethernet 10/100 Mbps se produit quand un port sur la liaison fonctionne en mode half-duplex tandis que l'autre fonctionne en mode full duplex. Cette situation se produit de temps en temps quand vous réinitialisez un ou plusieurs ports sur une liaison et que le processus d'autonégociation n'entraîne pas la même configuration pour les deux partenaires de liaison. Cette situation se produit également quand vous reconfigurez un côté de liaison et que vous oubliez de reconfigurer l'autre côté. Vous pouvez éviter la nécessité de placer des appels d'assistance relatifs aux performances si vous :

- Créez une politique qui exige la configuration des ports pour le comportement requis, pour tous les périphériques non temporaires
- Mettez en oeuvre la politique avec les mesures de contrôle des modifications appropriées

Les symptômes classiques illustrant un problème de performances sont les suivants : augmentation de la séquence de contrôle de trame (FCS), contrôle de redondance cyclique (CRC), alignement, ou compteurs de trames trop petites sur le commutateur.

En mode half duplex, vous disposez d'une paire de fils de réception et d'une paire de fils de transmission. Les deux fils ne peuvent pas être utilisés en même temps. Le périphérique ne peut pas transmettre quand il y a un paquet du côté réception.

En mode full duplex, vous disposez de la même paire de fils de réception et de transmission. Cependant, chacun des deux peut être utilisé en même temps, parce que les fonctions de détection de porteuse et de détection de collisions ont été désactivées. Le périphérique peut transmettre et recevoir en même temps.

Par conséquent, une connexion half-duplex à full duplex fonctionne, mais il y a un grand nombre de collisions côté half duplex, entraînant des performances médiocres. Les collisions se produisent car le périphérique qui est configuré en full-duplex peut transmettre en même temps que le périphérique reçoit des données.

Les documents de cette liste détaillent l'autonégociation. Ces documents expliquent comment l'autonégociation fonctionne et décrivent diverses options de configuration :

- Configuration et dépannage de la négociation automatique de transmission semi-duplex/duplex intégral simultanée Ethernet 10/100/1000 MB
- Dépannage de problèmes de compatibilité des commutateurs Cisco Catalyst avec NIC

Une idée fausse commune au sujet de l'autonégociation est qu'il est possible de configurer manuellement un partenaire de liaison en mode full duplex 100 Mbps et d'autonégocier le même mode avec l'autre partenaire de liaison. En fait, une tentative de faire ceci a comme conséquence une erreur de correspondance de mode bidirectionnel. C'est lié au fait qu'un partenaire de liaison autonégocie, ne voit aucun paramètre d'autonégociation en provenance de l'autre partenaire de liaison, et est configuré par défaut en mode half-duplex.

La plupart des modules Ethernet Catalyst prennent en charge 10/100 Mbps et half/full-duplex. Toutefois, pour le vérifier, vous pouvez émettre la commande **show interface** ***mod/port capabilities*** .

FEFI

FEFI (Far End Fault Indication) protège les interfaces 100BASE-FX (fibre) et Gigabit, alors que l'autonégociation protège 100BASE-TX (cuivre) et empêche la couche physique de signaler les pannes associées.

Une panne d'extrémité lointaine est une erreur dans la liaison, qu'une station peut détecter alors que l'autre ne peut pas. Exemple : fil de transmission débranché. Dans cet exemple, la station émettrice continue de recevoir des données valides et détecte que la liaison est bonne par l'intermédiaire du contrôleur d'intégrité de liaison. Toutefois, la station émettrice ne peut pas détecter que l'autre station ne reçoit pas la transmission. Une station 100BASE-FX qui détecte une telle panne distante peut modifier son flux IDLE transmis et lui faire envoyer un schéma de bits spécial pour informer le voisin de la panne distante. Le schéma de bits spécial est appelé schéma `FEFI-IDLE`. Le schéma `FEFI-IDLE déclenche ensuite un arrêt du port distant (errDisable)`. Reportez-vous à la section UniDirectional Link Detection de ce document pour plus d'informations sur la protection contre les pannes.

Ces modules/matériels prennent en charge FEFI :

- Catalyst 6500/6000 et 4500/4000 :Tous les modules 100BASE-FX et modules GE

Recommandation de ports d'infrastructure Cisco

Le choix entre la configuration de l'autonégociation sur des liaisons 10/100-Mbps et l'encodage de

la vitesse et du mode bidirectionnel dépend du type de partenaire de liaison ou de périphérique d'extrémité que vous avez connecté à un port de commutation Catalyst. L'autonégociation entre les périphériques d'extrémité et les commutateurs Catalyst fonctionne bien généralement, et les commutateurs Catalyst sont conformes au cahier des charges IEEE 802.3u. Cependant, quand la carte réseau (NIC) ou les commutateurs du constructeur ne se conforment pas exactement, des problèmes peuvent en résulter. En outre, les fonctions avancées propres au constructeur qui ne sont pas décrites dans la spécification IEEE 802.3u pour l'autonégociation 10/100-Mbps peuvent entraîner une incompatibilité matérielle, ainsi que d'autres problèmes. Ces types de fonctionnalités avancées incluent la polarité automatique et l'intégrité du câblage. Ce document en fournit un exemple :

- Alerte sur site : Problème de performances avec des NIC Intel Pro/1000T se connectant à CAT4K/6K

Dans certaines situations, vous avez besoin de définir l'hôte, la vitesse de port et la configuration duplex. En règle générale, vous devez effectuer ces étapes de dépannage de base :

- Assurez-vous que l'autonégociation est configurée des deux côtés de la liaison ou que l'encodage est configuré des deux côtés.
- Lisez les avertissements communs mentionnés dans les notes de mise à jour.
- Vérifiez la version du pilote NIC ou du système d'exploitation que vous utilisez. Le pilote ou le correctif le plus récent est souvent exigé.

En général, essayez d'utiliser l'autonégociation d'abord pour n'importe quel type de partenaire de liaison. Il y a des avantages évidents à configurer l'autonégociation pour les périphériques temporaires tels que des ordinateurs portables. L'autonégociation fonctionne bien également avec d'autres périphériques, par exemple :

- Avec les périphériques non temporaires (tels que des serveurs et des postes de travail fixes)
- De commutateur à commutateur
- De commutateur à routeur

Mais, pour certaines raisons mentionnées dans cette section, des problèmes de négociations peuvent survenir. Référez-vous à Configuration et dépannage de l'autonégociation Ethernet 10/100/1000Mb Half/Full-duplex pour connaître les étapes de dépannage de base applicables à ces situations.

Désactivez l'autonégociation pour :

- Les ports qui prennent en charge les périphériques d'infrastructure réseau tels que des commutateurs et des routeurs
- D'autres systèmes d'extrémité non temporaires tels que des serveurs et des imprimantes

Veillez à toujours coder les paramètres de vitesse et de configuration duplex de ces ports.

Configurez manuellement ces configurations de liaisons 10/100-Mbps (vitesse et configuration duplex), qui sont habituellement des liaisons 100-Mbps Full Duplex :

- Commutateur à commutateur
- Commutateur à serveur
- Commutateur à routeur

Si la vitesse du port est définie sur auto sur un port Ethernet 10/100 Mbps, la vitesse et le mode bidirectionnel sont tous deux autonégociés. Émettez cette commande d'interface pour définir le port sur auto :

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
!--- This is the default.
```

Émettez ces commandes d'interface pour configurer la vitesse et le mode duplex :

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Recommandations de port d'accès Cisco

Les utilisateurs finaux, les travailleurs mobiles et les hôtes temporaires ont besoin de l'autonégociation pour minimiser la gestion de ces hôtes. Vous pouvez faire le travail d'autonégociation avec des commutateurs Catalyst également. Les pilotes NIC les plus récents sont souvent exigés.

Émettez ces commandes globales afin d'activer l'autonégociation de la vitesse pour le port :

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
```

Remarque : si vous définissez la vitesse du port sur auto sur un port Ethernet 10/100 Mbits/s, la vitesse et le duplex sont tous deux négociés automatiquement. Vous ne pouvez pas changer le mode duplex de ports d'autonégociation.

Lorsque des NIC ou des commutateurs du constructeur ne se conforment pas exactement à la spécification IEEE 802.3u, des problèmes peuvent survenir. En outre, les fonctions avancées propres au constructeur qui ne sont pas décrites dans la spécification IEEE 802.3u pour l'autonégociation 10/100-Mbps peuvent entraîner une incompatibilité matérielle, ainsi que d'autres problèmes. De telles fonctionnalités avancées incluent la polarité automatique et l'intégrité du câblage.

Autres options

Quand l'autonégociation est désactivée entre les commutateurs, l'indication de panne de la couche 1 peut également être perdue pour certains problèmes. Utilisez les protocoles de la couche 2 pour augmenter la détection de panne telle que le mode UDLD agressif.

L'autonégociation ne détecte pas ces situations, même lorsque l'autonégociation est activée :

- Les ports sont collés et ne reçoivent pas ou ne transmettent pas
- Sur l'un des côtés, la ligne est active, mais de l'autre, elle est inactive
- Des câbles fibre sont mal câblés

L'autonégociation ne détecte pas ces problèmes parce qu'ils ne sont pas au niveau de la couche physique. Les problèmes peuvent entraîner des boucles STP ou des trous noirs de trafic.

UDLD peut détecter tous ces cas et appliquer errdisable sur les deux ports de la liaison, s'il est configuré aux deux extrémités. De cette façon, UDLD empêche les boucles STP et les trous noirs.

Autonégociation Gigabit Ethernet

Objectif

La norme Gigabit Ethernet (GE) a une procédure de négociation automatique qui est plus extensive que celle utilisée pour l'Ethernet 10/100 Mbps (spécification IEEE 802.3z). Avec les ports GE, l'autonégociation est utilisée pour échanger :

- Les paramètres de régulation de débit
- Les informations sur une panne à distance
- Les informations duplex**Remarque :** les ports GE de la gamme Catalyst prennent uniquement en charge le mode bidirectionnel simultané.

La norme IEEE 802.3z a été remplacée par la spécification IEEE 802.3:2000. Référez-vous à l'Abonnement aux normes Local and Metropolitan Area Networks + Drafts (LAN/MAN 802s) pour plus d'informations.

Aperçu opérationnel

Àla différence de l'autonégociation avec 10/100-Mbps FE, l'autonégociation GE ne comporte pas la négociation de la vitesse du port. En outre, vous ne pouvez pas émettre la commande **set port speed afin de désactiver l'autonégociation.** La négociation de port GE est activée par défaut et les ports des deux extrémités d'une liaison GE doivent avoir la même configuration. La liaison n'est pas active si les ports de chaque extrémité de la liaison sont définis de façon incohérente, ce qui signifie que les paramètres échangés sont différents.

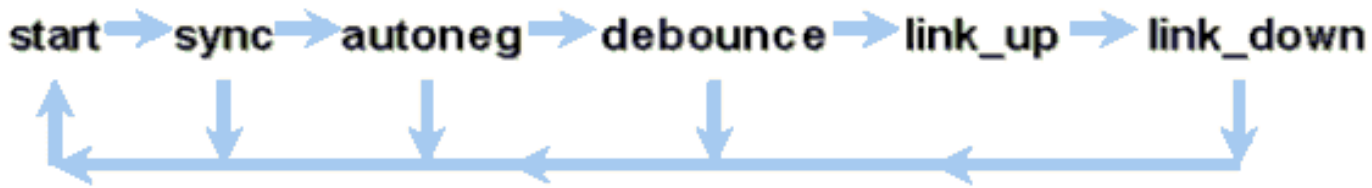
Par exemple, supposez qu'il y a deux périphériques, A et B. Chaque périphérique peut avoir l'autonégociation activée ou désactivée. C'est une table qui contient les configurations possibles, ainsi que l'état de leurs liaisons respectives :

Négociation	B activé	B désactivé
A désactivé	up des deux côtés	A down, B up
A désactivé	A up, B down	up des deux côtés

Dans une liaison GE, la synchronisation et l'autonégociation (si elles sont activées) sont exécutées au démarrage de la liaison par l'utilisation d'une séquence spéciale de noms de code pour liaison réservée.

Note : Il existe un dictionnaire de mots valides, et tous les mots possibles ne sont pas valides dans GE.

La vie d'une connexion GE peut être caractérisée de cette façon :



Une perte de synchronization signifie que MAC détecte une liaison hors service. La perte de

synchronisation s'applique, que l'autonégociation soit activée ou désactivée. La synchronisation est perdue dans certaines conditions d'échec telles que la réception de trois mots incorrects en succession. Si ce phénomène persiste pendant 10 ms, une condition « sync fail » est affirmée et la liaison passe en état `link_down` . Une fois la synchronisation perdue, trois délais d'inactivité valides consécutifs sont nécessaires afin de resynchroniser. D'autres événements catastrophiques, tels qu'une perte de signal de réception (Rx), entraînent la désactivation d'une liaison.

L'autonégociation est une partie du processus de liaison. Quand la liaison est active, l'autonégociation est terminée. Cependant, le commutateur continue à surveiller l'état de la liaison. Si l'autonégociation est désactivée sur un port, la phase d'« autoneg » n'est plus une option.

Le cahier des charges GE cuivre (1000BASE-T) supporte l'autonégociation par Next Page Exchange. Next Page Exchange permet l'autonégociation des vitesses 10/100/1000 Mbps/s sur des ports cuivre.

Remarque : Cependant, la spécification de la fibre GE ne prévoit que la négociation du mode bidirectionnel, du contrôle de flux et de la détection des pannes à distance. Les ports fibre GE ne négocient pas la vitesse du port. Référez-vous aux sections 28 et 37 de la spécification IEEE 802.3-2002 pour plus d'informations sur l'autonégociation.

Le délai de redémarrage de la synchronisation est une fonctionnalité logicielle qui contrôle la durée totale de l'autonégociation. Si l'autonégociation ne réussit pas dans ce délai, le firmware relance l'autonégociation au cas où il y aurait un blocage. La commande **sync-restart-delay a seulement un effet quand l'autonégociation est définie sur enable.**

Recommandation de ports d'infrastructure Cisco

La configuration de l'autonégociation est beaucoup plus critique dans un environnement GE que dans un environnement 10/100 Mbps. Désactivez l'autonégociation uniquement dans ces situations :

- Sur les ports de commutation reliés aux périphériques qui ne peuvent pas supporter la négociation
- Lorsque les problèmes de connectivité résultent de problèmes d'interopérabilité

Activez la négociation Gigabit sur toutes les liaisons commutateur à commutateur et, en règle générale, sur tous les périphériques GE. La valeur par défaut sur les interfaces Gigabit est l'autonégociation. Cependant, émettez cette commande afin de vérifier que l'autonégociation est activée :

```
switch(config)#interface type slot/port
switch(config-If)#no speed
!--- This command sets the port to autonegotiate Gigabit parameters.
```

Une exception connue se produit quand vous vous connectez à un routeur commutateur Gigabit (GSR) exécutant une version du logiciel Cisco IOS antérieure à la version 12.0(10)S (la version qui a ajouté le contrôle de flux et l'autonégociation). Dans ce cas, désactivez ces deux fonctions. Si vous ne le faites pas, le port de commutation est indiqué comme étant non connecté et le GSR indique la survenue d'erreurs. Voici un exemple de séquence de commandes d'interface :

```
flowcontrol receive off
```

```
flowcontrol send off
speed nonegotiate
```

Recommandations de port d'accès Cisco

Puisque les FLP peuvent peuvent varier selon les constructeurs, vous devez examiner les connexions commutateur à serveur au cas par cas. Les clients Cisco ont rencontré certains problèmes avec la négociation Gigabit sur des serveurs Sun, HP et IBM. Faites en sorte que tous les périphériques utilisent l'autonégociation, sauf indication contraire explicite du constructeur.

Autres options

Le contrôle de flux est une partie facultative de la spécification 802.3x. Le contrôle de flux doit être négocié si vous l'utilisez. Les périphériques peuvent ou ne peuvent pas envoyer et/ou répondre à une trame PAUSE (MAC 01-80-C2-00-00-00 0F). Et les périphériques peuvent ne pas être d'accord sur la demande de contrôle de flux du voisin distant. Un port avec un tampon d'entrée qui commence à se remplir envoie une trame PAUSE au partenaire de liaison. Le partenaire de liaison arrête la transmission et retient toutes les trames supplémentaires dans les mémoires tampon de sortie du partenaire de liaison. Cette fonction ne résout aucun problème de surabonnement. Mais la fonction rend effectivement le tampon d'entrée plus grand à hauteur d'une certaine fraction de la mémoire tampon de sortie du partenaire.

La fonction de PAUSE est conçue pour empêcher que les périphériques (commutateurs, routeurs ou stations) ne jettent inutilement les trames reçues, en raison des conditions de débordement de mémoire tampon qu'entraîne la surcharge à court terme du trafic temporaire. Un périphérique en surcharge empêche le débordement de tampon interne quand le périphérique envoie une trame PAUSE. La trame PAUSE contient un paramètre qui indique la durée d'attente du mode Full Duplex avant que le partenaire n'envoie d'autres trames de données. Le partenaire qui reçoit la trame PAUSE cesse d'envoyer des données pour la période spécifiée. Quand cette temporisation expire, la station commence à envoyer de nouveau des trames de données, à partir du point auquel la station s'est arrêtée.

Une station qui émet une trame PAUSE peut émettre une autre trame PAUSE qui contient un paramètre de durée zéro. Cette action annule le reste de la période de pause. Ainsi, une trame PAUSE qui vient d'être reçue remplace toute opération PAUSE en cours. En outre, la station qui émet la trame PAUSE peut prolonger la période de PAUSE. La station émet une autre trame PAUSE contenant un paramètre de durée non égale à zéro avant l'expiration de la première période de PAUSE.

Cette opération PAUSE n'est pas en contrôle de flux basé sur le débit. L'opération est un mécanisme simple de démarrage-arrêt qui permet au périphérique ayant envoyé la trame PAUSE de diminuer son encombrement de mémoire tampon.

Cette fonction est surtout utile sur les liaisons entre les ports d'accès et les hôtes d'extrémité, où la mémoire tampon de sortie de l'hôte est potentiellement aussi grande que la mémoire virtuelle. L'utilisation du commutateur à commutateur a des avantages limités.

Émettez ces commandes d'interface afin de contrôler cela sur les ports de commutation :

```
flowcontrol {receive | send} {off | on | desired}
```

```
>show port flowcontrol

 Port   Send FlowControl    Receive FlowControl   RxPause TxPause
        admin    oper       admin    oper
-----   -------- --------   -------- --------     ------- -------
 6/1    off      off        on       on           0       0
 6/2    off      off        on       on           0       0
 6/3    off      off        on       on           0       0
```

Remarque : Tous les modules Catalyst répondent à une trame `PAUSE` si elle est négociée. Certains modules (par exemple, WS-X5410 et WS-X4306) n'envoient jamais de trames PAUSE, même s'ils négocient pour cela, car ils sont non-bloquants.

Dynamic Trunking Protocol

Objectif

Afin d'étendre les VLAN entre les périphériques, les jonctions identifient temporairement et marquent les trames Ethernet initiales. Cette action active les trames à multiplexer sur une liaison unique. Elle garantit également que la diffusion VLAN séparée et les domaines de sécurité sont maintenus entre les commutateurs. Les tables CAM maintiennent la correspondance trame-à-VLAN à l'intérieur des commutateurs.

Aperçu opérationnel

DTP est la deuxième génération de DISL (Dynamic ISL). DISL ne prenait en charge qu'ISL. DTP prend en charge ISL et 802.1Q. Cette prise en charge garantit que les commutateurs situés à l'une ou l'autre des extrémités d'une jonction sont d'accord sur les différents paramètres des trames de liaison de jonction. Ces paramètres incluent :

- Le type d'encapsulation configuré
- VLAN natif
- La capacité matérielle

La prise en charge DTP protège également contre l'inondation des trames marquées par des ports sans agrégation, présentant un risque de sécurité potentiellement élevé. DTP protège contre cette inondation parce qu'il s'assure que les ports et leurs voisins portent des états cohérents.

Mode de jonction

DTP est un protocole de la couche qui négocie des paramètres de configuration entre un port de commutation et son voisin. Il utilise une autre adresse MAC multicast (01-00-0c-cc-cc-cc) et un type de protocole SNAP 0x2004. Ce tableau décrit la fonction pour chacun des modes de négociation DTP possible :

Mode	Fonction	Trames DTP transmises ?	État final (port local)
`Dynamic Auto`	Entraîne la tentative de conversion de la liaison en jonction. Le port	Oui, périodique	`Jonction`

(équivalent au mode Auto dans CatOS)	devient un port de jonction si le port voisin est défini sur le mode on ou desirable.		
Trunk (équivalent au mode ONdans CatOS)	Met le port en mode de jonction des liens permanent et négocie pour convertir la liaison en jonction. Le port devient un port de jonction même si le port voisin n'est pas d'accord sur la modification.	Oui, périodique	Liaison, sans réserve
Nonegotiate	Met le port dans le mode d'agrégation des liens permanent mais ne permet pas au port de produire des trames DTP. Vous devez configurer manuellement le port voisin comme port de jonction pour établir une liaison de jonction. C'est utile pour les périphériques qui ne prennent pas en charge le DTP.	Non	Liaison, sans réserve
Dynamic desirable (la commande CatOS comparable est desirable)	Force le port à essayer activement de convertir la liaison en liaison de jonction. Le port devient un port de liaison si le port voisin est défini sur le mode on, desirable ou auto .	Oui, périodique	Il finit dans l'état de jonction de liens seulement si le mode distant est on, auto ou desirable.
Accès	Met le port en mode non-jonction permanent non-trunking mode et négocie pour convertir la liaison en liaison sans agrégation. Le port devient un port sans agrégation, même si le port voisin n'est pas d'accord sur la	Non en état équilibré, mais transmet des informations pour accélérer la détection de l'extrémité	Non-jonction

	modification.	distante après la modification d' `on`.	

Remarque : Le type d'encapsulation ISL et 802.1Q peut être défini ou négocié.

Dans la configuration par défaut, DTP assume ces caractéristiques sur la liaison :

- Les connexions point-à-point et les équipements Cisco supportent les ports de jonction 802.1Q qui sont seulement point à point.
- Dans toute la négociation DTP, les ports ne participent pas à STP. Le port est ajouté à STP seulement une fois que le type de port devient de l'un de ces trois types :AccèsLien ISL802.1QPAgP est le processus suivant à être exécuté avant que le port STP ne participe à STP. PAgP est utilisé pour l'autonégociation d'EtherChannel.
- VLAN 1 est toujours présent sur le port de jonction. Si le port est avec agrégation en mode ISL, les paquets DTP sont envoyés sur le VLAN 1. Si le port est sans agrégation en mode ISL, les paquets DTP sont envoyés sur le VLAN natif (pour les ports avec ou sans agrégation 802.1Q).
- Les paquets DTP transfèrent le nom de domaine VTP, ainsi que la configuration de la jonction et le statut d'administration. Le nom de domaine VTP doit correspondre pour qu'une jonction négociée soit établie. Ces paquets sont envoyés chaque seconde pendant la négociation et toutes les 30 secondes après la négociation. Si un port en mode `auto ou desirable ne détecte pas un paquet DTP dans un délai de 5 minutes (min), il est défini comme étant sans agrégation.`

Attention : Vous devez comprendre que les modes `trunk`, `nonegotiate` et `access` spécifient explicitement dans quel état le port se termine. Une mauvaise configuration peut mener à un état dangereux/contradictoire dans lequel un côté est en agrégation et l'autre non.

Référez-vous à Configuration de la jonction ISL sur des commutateurs de la gamme Catalyst 5500/5000 et 6500/6000 pour plus de détails sur l'ISL. Référez-vous à Liaison entre commutateurs de la gamme Catalyst 4500/4000, 5500/5000 et 6500/6000 utilisant l'encapsulation 802.1Q avec le logiciel système Cisco CatOS pour plus de détails sur le 802.1Q.

Type d'encapsulation

Aperçu opérationnel de l'ISL

ISL est un protocole de jonction, propriété industrielle de Cisco (schéma de balisage VLAN). ISL est utilisé depuis de nombreuses années. En revanche, 802.1Q est beaucoup plus nouveau, mais il représente la norme IEEE.

ISL encapsule complètement la trame d'origine dans un schéma de balisage à deux niveaux. De cette façon, ISL est effectivement un protocole de tunnellisation et, comme avantage accessoire, porte des trames non-Ethernet. ISL ajoute un en-tête de 26 octets et un FCS 4 octets à la trame Ethernet standard. Les ports qui sont configurés pour être des jonctions traitent les trames Ethernet plus grandes. ISL prend en charge les VLAN 1024.

Format de trame - Balisage ISL Tag ombragé

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits
DA	Type	USER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve
01-00-0c-00-00					AAAA03	00000C				

Encapsulated Frame	FCS
Variable length	32 bits

Référez-vous à Liaison InterSwitch et format de trame IEEE 802.1Q pour plus d'informations.

Aperçu opérationnel du 802.1Q

Bien que la norme IEEE 802.1Q concerne seulement Ethernet, la norme spécifie bien davantage que les types d'encapsulation. 802.1Q inclut, entre autres, les protocoles GARP (Generic Attribute Registration Protocols), les améliorations spanning-tree et le balisage QoS 802.1p. Référez-vous aux Normes IEEE en ligne pour plus d'informations

Le format de trame de 802.1Q préserve les SA et DA Ethernet initiaux. Cependant, les commutateurs doivent maintenant compter recevoir les trames baby-giant, même sur des serveurs de ports d'accès sur lesquels les hôtes peuvent utiliser le balisage pour indiquer la priorité utilisateur 802.1p pour la signalisation QoS. La balise est de 4 octets. Les trames v2 Ethernet 802.1Q sont de 1522 octets, ce qui est une réalisation du groupe de travail IEEE 802.3ac. De plus, 802.1Q prend en charge l'espace de numérotation pour les VLAN 4096.

Toutes les trames de données qui sont transmises et reçues sont marquées 802.1Q, excepté les trames de données qui sont sur le VLAN natif. Dans ce cas, il y a une étiquette implicite qui est basée sur la configuration du port de commutateur d'entrée. Les trames sur le VLAN natif sont toujours transmises sans marqueur et normalement reçues sans marqueur. Cependant, ces trames peuvent également être reçues marquées.

Référez-vous à ces documents pour plus d'informations :

- Interopérabilité des VLAN
- Jonction entre les commutateurs Catalyst 4500/4000, 5500/5000 et 6500/6000 par encapsulation 802.1Q avec le logiciel système Cisco CatOS

Format de trame 802.1Q/802.1p

		Tag Header						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Variable length	32 bits
DA	SA	TPID	Priority	CFI	VLAN ID	Length/ Type	Data with PAD	FCS
		0x8100	0 – 7	0-1	0-4095			

Recommandation de configuration Cisco

L'un des objectifs de conception Cisco consiste à essayer d'obtenir la cohérence au sein du réseau dans la mesure du possible. Tous les nouveaux produits Catalyst prennent en charge 802.1Q et certains ne prennent en charge que 802.1Q (comme par exemple les premiers modules Catalyst 4500/4000 et 6500). Par conséquent, toutes les nouvelles réalisations doivent suivre cette norme IEEE 802.1Q et les réseaux plus anciens doivent être migrés graduellement à partir d'ISL.

Émettez ces commandes d'interface afin d'activer l'agrégation 802.1Q sur un port particulier :

```
Switch(config)#interface type slot#/port#
Switch(config-if)#switchport
!--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation
dot1q
```

Le standard IEEE permet l'interopérabilité constructeur. L'interopérabilité constructeur est avantageuse dans tous les environnements Cisco lorsque de nouveaux NIC et périphériques hôtes compatibles avec 802.1p deviennent disponibles. Bien que les réalisations ISL et 802.1Q soient solides, la norme IEEE a finalement une plus grande exposition et un plus grand support tiers, qui inclut le soutien des analyseurs de réseau. En outre, une considération mineure est que la norme 802.1Q a également un temps système d'encapsulation inférieur à celui d'ISL.

Pour l'exhaustivité, le balisage implicite sur les VLAN natifs crée une considération liée à la sécurité. La transmission des trames d'un VLAN, VLAN X, à un autre VLAN, VLAN Y, sans routeur est possible. La transmission peut se produire sans routeur si le port source (VLAN X) est dans le même VLAN que le VLAN natif d'une jonction 802.1Q sur le même commutateur. La solution consiste à utiliser un VLAN factice pour le VLAN natif de la jonction.

Émettez ces commandes d'interface afin d'établir un VLAN en tant que VLAN natif (valeur par défaut) pour l'agrégation 802.1Q sur un port particulier :

```
Switch(config)#interface type slot#/port#
Switch(config-If)#switchport trunk native vlan 999
```

Puisque tout nouveau matériel prend en charge 802.1Q, toutes les nouvelles implémentations doivent se conformer à la norme IEEE 802.1Q et les réseaux antérieurs doivent être migrés graduellement à partir d'ISL. Jusqu'à récemment, de nombreux modules Catalyst 4500/4000 ne prenaient pas en charge ISL. Par conséquent, 802.1Q est la seule option pour l'agrégation Ethernet. Référez-vous à la sortie de la commande **show interface capabilities** ou à la commande show port capabilities pour CatOS. Puisque le support de liaison de jonction exige un matériel approprié, un module qui ne supporte pas 802.1Q peut ne jamais supporter 802.1Q. Une mise à niveau logicielle ne confère pas de support de 802.1Q. La plupart des nouveaux matériels pour commutateurs Catalyst 6500/6000 et 4500/4000 prend en charge ISL et 802.1Q.

Si VLAN 1 est effacé d'une jonction, ce qui est décrit dans la section Interface de gestion de la commutation VLAN natifs , bien qu'aucune donnée utilisateur ne soit transmise ou reçue, NMP continue à utiliser des protocoles de contrôle sur VLAN 1. Les exemples des protocoles de contrôle incluent CDP et VTP.

En outre, comme l'indique la section VLAN 1 , les paquets CDP, VTP, et PAgP sont toujours envoyés sur le VLAN 1 lors de l'agrégation. En utilisant l'encapsulation dot1q (802.1Q), ces trames de contrôle sont marquées avec le VLAN 1 si le VLAN natif du commutateur est changé. Si la liaison dot1q à un routeur est activée et le VLAN natif est changé sur le commutateur, une sous-interface dans le VLAN 1 est nécessaire pour recevoir les trames CDP balisées et pour fournir une visibilité du voisin CDP sur le routeur.

Remarque : Il existe un risque potentiel de sécurité avec dot1q que le balisage implicite du VLAN natif provoque. La transmission des trames d'un VLAN à l'autre sans routeur peut être possible. Référez-vous à FAQ sur la détection d'intrusion pour plus d'informations. La solution de contournement consiste à utiliser un ID de VLAN pour le VLAN natif de l'agrégation qui n'est pas utilisé pour l'accès de l'utilisateur final. Pour cela, la majorité des clients Cisco laissent simplement VLAN 1 comme VLAN natif sur une liaison et assignent des ports d'accès aux VLAN autres que le VLAN 1 afin de réaliser ceci simplement.

Cisco recommande une configuration de jonction explicite en mode `dynamic desirable aux deux extrémités.` C'est le mode par défaut. Dans ce mode, les opérateurs réseau peuvent faire confiance à des messages d'état de Syslog et de ligne de commande indiquant qu'un port est `actif et avec agrégation.` Ce mode est différent du mode `on , qui peut faire apparaître un port comme étant actif, bien que le voisin soit mal configuré.` En outre, les jonctions en mode `desirable fournissent la stabilité dans les situations dans lesquelles un côté de la liaison ne peut pas devenir une jonction ou supprime l'état de jonction.`

Si le type d'encapsulation est négocié entre les commutateurs avec l'utilisation de DTP et si ISL est choisi comme gagnant par défaut si les deux extrémités le prennent en charge, vous devez émettre cette commande d'interface afin de spécifier dot1q[1] :

```
switchport trunk encapsulation dot1q
```

[1] Certains modules comprenant WS-X6548-GE-TX et WS-X6148-GE-TX ne prennent pas en charge l'agrégation ISL. Ces modules n'acceptent pas la commande **switchport trunk encapsulation *dot1q***.

Remarque : Émettez la commande **switchport mode access** afin de désactiver les trunks sur un port. Cette désactivation aide à éliminer les temps de négociation gaspillés lorsque des ports hôte sont introduits.

```
Switch(config-if)#switchport host
```

Autres options

Une autre configuration client commune utilise le mode `dynamic desirable seulement au niveau de la couche de distribution et la configuration par défaut la plus simple (mode dynamic auto) au niveau de la couche d'accès.` Quelques commutateurs, tels que Catalyst 2900XL, les routeurs Cisco IOS ou les périphériques d'autres constructeurs, ne supportent pas actuellement la négociation de jonction via DTP. Vous pouvez utiliser le `mode nonegotiate pour définir l'agrégation sur un port avec ces périphériques.` Ce mode peut faciliter la standardisation sur une configuration commune à travers le campus.

Cisco recommande l'utilisation du mode `nonegotiate quand vous vous connectez à un routeur Cisco IOS.` Lors du pontage, certaines trames DTP reçues d'un port qui est configuré avec **switchport mode trunk peuvent retourner au port de jonction.** À la réception de la trame DTP, le port de commutation essaye de renégocier inutilement. Afin de renégocier, le port de commutation rend la jonction `inactive puis active`. Si `nonegotiate est activé, le commutateur n'envoie pas de trames DTP.`

```
switch(config)#interface type slot#/port#
switch(config-if)#switchport mode dynamic desirable
!--- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with
multiple VLANs. !--- And... switch(config-if)#switchport mode trunk
!--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or...
switch(config-if)#switchport nonegotiate
!--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers.
switch(config-if)#switchport access vlan vlan_number
!--- Configure a fallback VLAN for the interface. switch(config-if)#switchport trunk native vlan
999
!--- Set the native VLAN. switch(config-if)#switchport trunk allowed vlan vlan_number_or_range
!--- Configure the VLANs that are allowed on the trunk.
```

protocole STP

Objectif

Spanning-tree met à jour un environnement sans boucles de la couche 2 sur les réseaux commutés redondants. Sans STP, les trames font une boucle et/ou se multiplient indéfiniment. Cette occurrence entraîne un ralentissement des données sur le réseau parce que le trafic élevé interrompt tous les périphériques du domaine de diffusion.

Àcertains égards, STP est un protocole qui a été au commencement développé pour des spécifications articulées autour d'un pont à logiciel lent (IEEE 802.1D). Cependant, STP peut être compliqué afin de le mettre en application avec succès sur les grands réseaux commutés qui ont :

- Beaucoup de réseaux VLAN
- Beaucoup de commutateurs dans un domaine
- Un support multi-constructeurs

- De nouvelles améliorations IEEE

Le logiciel Cisco IOS tire profit des nouveaux développements STP. Les nouveaux standards IEEE qui incluent 802.1w Rapid STP et 802.1s Multiple spanning-tree offrent une convergence rapide, un partage de charge et une évolutivité du plan de contrôle. Par ailleurs, les améliorations STP telles que RootGuard, le filtrage BPDU, la protection PortFast BPDU et le Loopguard assurent une protection supplémentaire contre des boucles de réacheminement de la couche 2.

Aperçu opérationnel PVST+

La sélection du pont racine par VLAN est remportée par le commutateur avec le plus bas identifiant de pont racine (BID). Le BID est la priorité de pont combinée avec l'adresse MAC du commutateur.

Initialement, les BPDU sont envoyés à partir de tous les commutateurs, et contiennent le BID de chaque commutateur et le coût de chemin pour atteindre ce commutateur. Ceci active la détermination du pont racine et le chemin le moins coûteux à la racine à déterminer. Les paramètres de configuration supplémentaires transportés dans les BPDU de la racine ont priorité sur ceux qui sont localement configurés de sorte que le réseau utilise des timers cohérents. Pour chaque BPDU envoyé au commutateur par la racine, le NMP Catalyst central traite un nouveau BPDU et l'envoie avec les informations racine.

La topologie converge alors par ces étapes :

1. Un pont racine unique est élu pour le domaine du spanning tree tout entier.
2. Un port racine (ce fait face au pont racine) est élu sur chaque pont non racine.
3. Un port donné est sélectionné pour expédier les BPDU sur chaque segment.
4. Les ports non désignés deviennent bloquants.

Référez-vous à ces documents pour plus d'informations :

- Configuration de STP et d'IEEE 802.1s MST
- Présentation du protocole Rapid Spanning Tree (STP) (802.1w)

Valeurs par défaut des temporisateurs de base	Name (nom)	Fonction
2 sec	hello	Contrôle le départ des BPDU.
15 sec	Délai de transmission (Fwddelay)	Contrôle la durée qu'un port passe dans l'état d'écoute et l' état d'apprentissage et influence le processus de modification de topologie.
20 sec	maxage	Contrôle la durée de maintien de la topologie actuelle par le commutateur avant la recherche d'un chemin alternatif. Après le délai maxage (vieillissement maximum), un BPDU est

		considéré comme obsolète et le commutateur recherche un nouveau port racine parmi le pool de ports bloquants. Si aucun port bloqué n'est disponible, le commutateur prétend être la racine elle-même sur les ports indiqués.

Cisco recommande que vous ne changiez pas les temporisateurs, parce que ceci peut compromettre la stabilité. La majorité des réseaux déployés ne sont pas accordés. Les temporisateurs STP simples qui sont accessibles par l'intermédiaire de la ligne de commande (comme les intervalles Hello, maxage, etc.) sont eux-mêmes composés d'un ensemble complexe d'autres temporisateurs intrinsèques. Par conséquent, il est difficile d'accorder les temporisateurs et de considérer toutes les ramifications. De plus, cela risque de nuire à la protection UDLD. Reportez-vous à la section Unidirectional Link Detection pour plus d'informations.

Remarque sur les temporisateurs STP :

Les valeurs par défaut des temporisateurs STP sont basées sur un calcul qui considère un diamètre réseau de sept commutateurs (de la racine au bord du réseau), et la durée nécessaire d'acheminement de BPDU du pont racine aux commutateurs périphériques du réseau, qui se trouvent sept sauts plus loin. Cette supposition calcule des valeurs de temporisation acceptables pour la plupart des réseaux. Mais vous pouvez adopter des valeurs plus optimales afin d'accélérer les temps de convergence dans toutes les modifications de la topologie réseau.

Vous pouvez configurer le pont racine avec le diamètre du réseau pour un VLAN spécifique, et les valeurs de temporisation sont calculées en conséquence. Cisco recommande, en cas d'apport de modifications, de ne configurer que le diamètre et les paramètres Hello du pont racine pour le VLAN.

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-time]]
!--- This command needs to be on one line.
```

Cette macro fait du commutateur la racine pour le VLAN spécifique, calcule de nouvelles valeurs de temporisation sur la base du diamètre et du délai Hello spécifiés, et propage cette information dans les BPDU de configuration à tous autres commutateurs de la topologie.

La section Nouveaux états de port et rôles de port décrit 802.1D STP et compare 802.1D STP à Rapid STP (RSTP). Référez-vous à Présentation du protocole Rapid Spanning Tree (802.1w) pour plus d'informations sur RSTP.

Nouveaux états de port et rôles de port

802.1D est défini dans quatre états de port différents :

- Écouter
- Apprendre
- Bloquer
- Transmettre

Reportez-vous au tableau de la section États de port pour plus d'informations. L'état du port est

mixte, qu'il bloque le trafic ou le transmette, car c'est son rôle dans la topologie active (port racine, port désigné, etc.). Par exemple, du point de vue opérationnel, il n'y a aucune différence entre un port à l'état blocking et un port à l'état listening. Les deux ports écartent les trames et n'apprennent pas les adresses MAC. La différence réelle réside dans le rôle que le spanning-tree affecte au port. Il peut être supposé sans risque qu'un port à l'état listening est désigné ou racine et va passer à l'état forwarding. Malheureusement, une fois le port à l'état forwarding, il n'y a aucun moyen de savoir avec l'état du port si le port est racine ou désigné. Ceci explique l'échec de cette terminologie basée sur l'état. RSTP remédie à cette défaillance, parce que RSTP découple le rôle et l'état d'un port.

États du port

États de port dans STP 802.1D

Etats de port	Moyens	Temporisation par défaut jusqu'au prochain état
Désactivé	Administrativement inactif.	
Bloquer	Reçoit les BPDU et arrête les données utilisateur.	Surveille la réception des BPDU. Attente de 20 secondes avant l'expiration de maxage ou la modification immédiate si une défaillance de liaison directe/locale est détectée.
Écouter	Envoie ou reçoit les BPDU afin de contrôler si le retour au blocage est nécessaire.	Attente de 15 secondes Fwddelay.
Apprendre	Construit la table topologie/CAM.	Attente de 15 secondes Fwddelay.
Transmettre	Envoie/reçoit les données.	

La modification totale de la topologie de base est :

- 20 + 2 (15) = 50 sec, si attente d'expiration de maxage
- 30 secondes pour la défaillance de liaison directe

Il y a seulement trois états de port dans RSTP qui correspondent aux trois états opérationnels possibles. Les états 802.1D désactivé, bloquant, et écoute ont été fusionnés dans un seul état 802.1w (Mis à l'écart).

État de port STP (802.1D)	État de port RSTP (802.1w)	Le port est-il inclus dans la topologie active ?	Le port apprend-il les adresses MAC ?
Désactivé	Rejeter	Non	Non
Bloquer	Rejeter	Non	Non

Écouter	Rejeter	Oui	Non
Apprendre	Apprendre	Oui	Oui
Transmettre	Transmettre	Oui	Oui

Rôles de port

Le rôle est une nouvelle variable affectée à un port donné. Les rôles de port racine et de port désigné demeurent, mais le rôle de port blocking est désormais réparti en rôles de port de secours et alternatifs. L'algorithme Spanning Tree (STA) détermine le rôle d'un port sur la base des BPDU. Rappelez-vous ceci au sujet des BPDU afin de simplifier les choses : Il y a toujours moyen de comparer deux BPDU et de décider si l'un est plus utile que l'autre. La base de la décision est la valeur qui est enregistrée dans BPDU et, de temps en temps, le port sur lequel est reçue le BPDU. Le reste de cette section explique des approches très pratiques en matière de rôles de port.

Rôle de port racine

Le port qui reçoit le meilleur BPDU sur un pont est le port racine. C'est le port qui est le plus proche du pont racine en termes de coût de chemin. Le STA élit un seul pont racine dans le réseau ponté total (par VLAN). Le pont racine envoie les BPDU qui sont plus utiles que ceux que peut envoyer tout autre pont. Le pont racine est le seul pont du réseau qui n'a pas de port racine. Tous les autres ponts reçoivent les BPDU sur au moins un port.

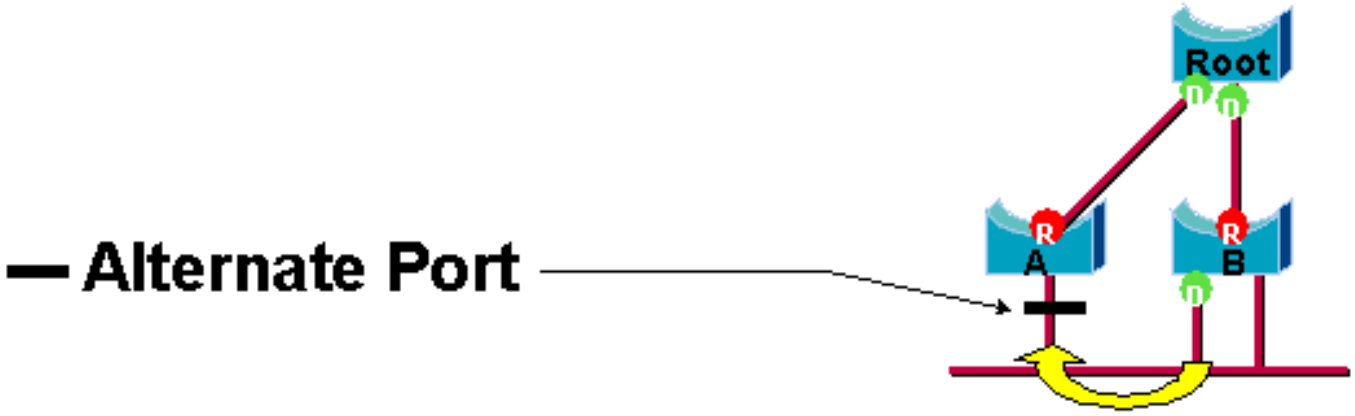
Rôle du port désigné

Un port est dit désigné s'il peut envoyer le meilleur BPDU sur le segment auquel ce port est connecté. 802.1D relie différents segments (segments Ethernet, par exemple) pour créer un domaine partagé. Sur un segment donné, il peut seulement y avoir un chemin vers le pont racine. S'il y en a deux, il y a une boucle de pontage sur le réseau. Tous les ponts connectés à un segment donné écoutent les BPDU des autres et conviennent du pont qui envoie le meilleur BPDU en tant que pont désigné pour le segment. Le port correspondant sur ce pont est indiqué.

Rôles des ports alternatifs et de secours

Ces deux rôles de port correspondent à l'état blocking de la norme 802.1D. La définition d'un port bloqué est un port qui n'est pas le port désigné ou le port racine. Un port bloqué reçoit un BPDU plus utile que celui qu'il envoie sur son segment. Rappelez-vous qu'un port a absolument besoin de recevoir des BPDU pour rester bloqué. RSTP introduit ces deux rôles à cet effet.

Un port alternatif est un port qui est bloqué en recevant des BPDU plus utiles en provenance des autres ponts. Ce diagramme illustre :



Un port de secours est un port qui est bloqué en recevant des BPDU plus utiles en provenance du même pont que celui sur lequel le port se trouve. Ce diagramme illustre :

Cette distinction a déjà été faite en interne dans la norme 802.1D. C'est essentiellement comme cela que fonctionne Cisco UplinkFast. Le raisonnement derrière ceci est qu'un port alternatif fournit un autre chemin au pont racine. Par conséquent, ce port peut remplacer le port racine si celui-ci échoue. Naturellement, un port de secours fournit une connectivité redondante au même

segment et ne peut pas garantir une connectivité alternative au pont racine. Par conséquent, le port de secours a été exclu du groupe de liaisons ascendantes.

Par conséquent, RSTP calcule la topologie finale pour spanning-tree avec l'utilisation des mêmes critères que 802.1D. Il n'y a absolument aucun changement dans la façon dont les différentes priorités de pont et de port sont utilisées. L'adjectif blocking est utilisé pour l'état discarding dans l'implémentation Cisco. CatOS version 7.1 et versions ultérieures affiche toujours les états d'écoute et d'apprentissage, qui fournissent bien plus d'informations sur un port que ne l'exige la norme IEEE. Mais la nouveauté réside dans le fait que désormais, une différence existe entre le rôle déterminé par le protocole pour un port et son état actuel. Par exemple, il est maintenant parfaitement valable pour un port d'être désigné et blocking en même temps. Comme ceci se produit généralement pendant des périodes très courtes, cela signifie simplement que ce port est dans un état transitoire avant de passer à l'état forwarding.

Interactions STP avec des VLAN

Il y a trois manières différentes de corréler des VLAN avec Spanning Tree :

- Un spanning tree unique pour tous les VLAN, ou le protocole CST (common spanning tree) tel qu'IEEE 802.1D
- Un spanning tree par VLAN, ou un spanning tree partagé, comme Cisco PVST
- Un spanning-tree par ensemble de VLAN, ou le protocole MST (multiple spanning-tree), comme IEEE 802.1s

D'un point de vue configuration, ces trois types de modes spanning-tree (puisqu'ils sont associés à l'interaction avec des VLAN) peuvent être configurés dans l'un des trois types de modes suivants :

- **pvst - Par spanning-tree de VLAN.** Ceci met en application réellement PVST+, mais figure simplement dans le logiciel Cisco IOS sous la forme PVST.
- **rapid-pvst — L'évolution de la norme 802.1D améliore les temps de convergence et intègre les propriétés basées sur la norme 802.1w d'UplinkFast et de BackboneFast.**
- **mst - C'est la norme 802.1s pour un spanning-tree par ensemble de VLAN ou de MST.** Cela inclut également le composant 802.1w de la norme.

Un spanning tree mono pour tous les VLAN permet seulement une topologie active et donc aucun équilibrage de charge. Un port STP bloqué bloque pour tous les VLAN et ne transporte aucune donnée.

Un spanning tree par VLAN ou PVST+ permet l'équilibrage de charge mais exige plus de traitement BPDU à mesure que le nombre de VLAN augmente.

La nouvelle norme 802.1s (MST) permet la définition de 16 instances/topologies actives STP maximum, et le mappage de tous les VLAN sur ces instances. Dans un environnement typique de campus, seulement deux instances doivent être définies. Cette technique permet à STP de mesurer des milliers de VLAN tandis que l'équilibrage de charge est activé.

La prise en charge de Rapid-PVST et de MST est introduit dans le logiciel Cisco IOS versions 12.1(11b)EX et 12.1(13)E pour Catalyst 6500. Catalyst 4500 avec la version 12.1(12c)EW du logiciel Cisco IOS et les versions ultérieures prennent en charge MST pré-standard. Rapid PVST est ajouté au logiciel Cisco IOS version 12.1(19)EW pour la plate-forme Catalyst 4500. Le MST conforme à la norme est pris en charge dans le logiciel Cisco IOS Version 12.2(18)SXF pour commutateurs Catalyst 6500 et dans le logiciel Cisco IOS Version 12.2(25)SG pour commutateurs

Catalyst 4500.

Référez-vous à Présentation du protocole Rapid spanning-tree (802.1w) et à Présentation du protocole Multiple spanning-tree (802.1s) pour plus d'informations.

Ports logiques Spanning-tree

Les notes de publication de Catalyst 4500 et 6500 fournissent des conseils sur le nombre de ports logiques recommandé dans le spanning-tree par commutateur. La somme de tous les ports logiques est égale au nombre de jonctions sur le commutateur par le nombre de VLAN actifs sur les jonctions, plus le nombre d'interfaces de non-liaison sur le commutateur. Le logiciel IOS de Cisco produit un message du journal système si le nombre maximal d'interfaces logiques dépasse la limitation. Il est recommandé de ne pas dépasser les valeurs figurant dans les instructions.

Ce tableau compare le nombre de ports logiques pris en charge pour les différents modes STP et types de supervision :

Superviseur	PVST+	RPVST+	MST
Catalyst 6500 Superviso r 1	6 000 [1] au total 1 200 par module de commutation	6 000 au total 1 200 par module de commutation	25 000 au total 3 000 [2] par module de commutation
Catalyst 6500 Superviso r 2	13 000 [1] total 1 800 [2] par module de commutation	10 000 au total 1 800 [2] par module de commutation	50 000 au total 6 000 [2] par module de commutation
Catalyst 6500 Superviso r 720	13 000 au total 1 800 [2] par module de commutation	10 000 au total 1 800 [2] par module de commutation	50 003 au total 6 000 [2] par module de commutation
Catalyst 4500 supervisor II plus	1 500 au total	1 500 au total	25 000 au total
Catalyst 4500 Superviso r II plus-10GE	1 500 au total	1 500 au total	25 000 au total
Catalyst 4500 supervisor IV	3 000 au total	3 000 au total	50 000 au total
Catalyst 4500 Superviso	3 000 au total	3 000 au total	50 000 au total

r V			
Catalyst 4500 Superviso r V 10GE	3 000 au total	3 000 au total	80 000 au total

[1] Le nombre maximal de ports logiques pris en charge dans PVST+ avant la version 12.1(13)E du logiciel Cisco IOS est de 4 500.

[2] modules de commutation 10 Mbits/s, 10/100 Mbits/s et 100 Mbits/s prennent en charge un maximum de 1 200 interfaces logiques par module.

[3] Le nombre maximal de ports logiques pris en charge dans MST avant la version 12.2(17b)SXA du logiciel Cisco IOS est de 30 000.

Recommandation

Il est difficile de fournir une recommandation de spanning-tree mode sans informations détaillées telles que le matériel, le logiciel, le numéro de périphériques et le nombre de VLAN. Généralement si le nombre de ports logiques ne dépasse pas la directive recommandée, Rapid PVST est recommandé pour le déploiement de nouveaux réseaux. Rapid PVST offre une convergence réseau rapide sans configuration supplémentaire (Backbone Fast et Uplink Fast, par exemple). Émettez la commande suivante pour définir le protocole Spanning-Tree en mode Rapid-PVST :

```
spanning-tree mode rapid-pvst
```

Autres options

Dans un réseau contenant un mélange de matériels existants et de logiciels plus anciens, le mode PVST+ est recommandé. Émettez cette commande pour définir spanning-tree en mode PVST+ :

```
spanning-tree mode pvst
----This is default and it shows in the configuration.
```

Le mode MST est recommandé pour les VLAN lorsque la conception réseau fait apparaître un grand nombre de VLAN. Pour ce réseau, la somme des ports logiques peut dépasser la directive pour PVST et Rapid-PVST. Émettez cette commande pour définir spanning-tree en mode MST :

```
spanning-tree mode mst
```

Formats de BPDU

Afin de supporter la norme IEEE 802.1Q, Cisco a étendu le protocole PVST, protocole existant afin d'offrir le protocole PVST+. PVST+ ajoute la prise en charge des liaisons dans la région mono Spanning Tree IEEE 802.1Q. PVST+ est compatible avec chacun des deux protocoles Cisco existants (IEEE spanning-tree mono 802.1Q et PVST). En outre, PVST+ ajoute des mécanismes de vérification afin de s'assurer qu'il n'y a aucune incohérence dans la configuration de la liaison de port et des ID de VLAN à travers les commutateurs. PVST+ est compatible avec PVST et prêt

à l'emploi, sans nécessité d'une nouvelle interface de commande en ligne (CLI) ou d'une nouvelle configuration.

Voici quelques points clés de la théorie opérationnelle du protocole PVST+ :

- PVST+ interopère avec le protocole 802.1Q mono spanning-tree. PVST+ interopère avec les commutateurs 802.1Q sur STP par agrégation 802.1Q. Common Spanning-Tree se trouve par défaut sur le VLAN 1, le VLAN natif. Un BBDU spanning-tree est transmis ou reçu avec l'adresse MAC du groupe de pontage selon la norme IEEE (01-80-c2-00-00-00, type de protocole 0x010c) sur des liaisons 802.1Q. Common Spanning Tree peut être enraciné dans le PVST ou dans la région mono spanning-tree.
- PVST+ perce un tunnel dans les BPDU PVST à travers la région VLAN 802.1Q VLAN en tant que données multicast. Pour chaque VLAN d'une jonction, les BPDU avec adresse MAC STP Cisco (SSTP) partagée (01-00-0c-cc-cd) sont transmis ou reçus. Pour les VLAN qui sont égaux à l'identificateur de port VLAN (PVID), les BPDU ne sont pas balisés. Pour tous les autres VLAN, les BPDU sont balisés.
- PVST+ est compatible avec le commutateur Cisco existant sur PVST par la liaison de jonction ISL. Les BPDU avec encapsulation ISL sont transmis ou reçus par des jonctions ISL, de la même façon qu'avec le PVST Cisco précédent.
- PVST+ vérifie les incohérences au niveau des ports et des VLAN. PVST+ bloque ces ports qui reçoivent des BPDU incohérents, afin d'empêcher l'occurrence des boucles de réacheminement. PVST+ informe également les utilisateurs des incohérences détectées par l'intermédiaire de messages Syslog.

Remarque : dans les réseaux ISL, toutes les BPDU sont envoyées avec l'utilisation de l'adresse MAC IEEE.

Recommandations de configuration Cisco

Tous les commutateurs Catalyst ont STP activé par défaut. Même si vous choisissez une conception qui n'inclut pas des boucles de la couche 2 et que le protocole STP n'est pas activé pour la mise à jour active d'un port bloqué, laissez cette fonction activée pour les raisons suivantes :

- S'il y a une boucle, STP empêche la survenue de problèmes qui peuvent être aggravés par la présence de données multicast et de diffusion. Souvent, un mauvais câblage, un câble défectueux ou une autre cause peut entraîner la présence d'une boucle.
- STP assure une bonne protection contre les pannes EtherChannel.
- La plupart des réseaux sont configurés avec STP, et bénéficient donc d'une exposition maximale. Plus d'exposition signifie généralement un code plus stable.
- STP assure la protection contre les défaillances des NIC à double connexion (ou pontage activé sur les serveurs).
- Beaucoup de protocoles sont étroitement liés à STP en code. Exemples :PAgPSnooping IGMP (Internet Group Message Protocol)JonctionSi vous n'utilisez pas STP, vous pouvez obtenir des résultats indésirables.
- Pendant une interruption de réseau signalée, les ingénieurs Cisco suggèrent habituellement que la non utilisation de STP peut être au centre de la défaillance, le cas échéant.

Afin d'activer spanning-tree sur tous les VLAN, émettez ces commandes globales :

```
Switch(config)#spanning-tree vlan vlan_id
!--- Specify the VLAN that you want to modify. Switch(config)#default spanning-tree vlan vlan_id
!--- Set spanning-tree parameters to default values.
```

Ne changez pas les timers, car ceci peut compromettre la stabilité. La majorité des réseaux déployés ne sont pas accordés. Les timers STP simples qui sont accessibles via la ligne de commande (intervalles Hello et maxage, par exemple) comportent un ensemble complexe d'autres timers intrinsèques. Par conséquent, vous pouvez rencontrer des difficultés si vous essayez d'accorder des timers et de tenir compte de toutes les ramifications. De plus, cela risque de nuire à la protection UDLD.

Dans le meilleur des cas, gardez le trafic utilisateur du VLAN de gestion. Ceci ne s'applique pas aux commutateurs Catalyst 6500/6000 du logiciel Cisco IOS. Vous devez respecter cette recommandation concernant les commutateurs Cisco IOS et CatOS qui peuvent avoir une interface de gestion distincte et devoir être intégrés à des commutateurs de Cisco IOS. Particulièrement avec les processeurs de commutation Catalyst plus anciens, il vaut mieux éviter des problèmes avec VLAN en gardant le STP de gestion séparé des données utilisateur. Une station d'extrémité qui se conduit mal pourrait potentiellement maintenir le processeur du Supervisor Engine si occupé avec des paquets de diffusion que le processeur pourrait manquer un ou plusieurs BPDU. Cependant, des commutateurs plus récents avec des CPU plus puissants et des systèmes de contrôle d'étranglement soulagent cette considération. Reportez-vous à la section Interface de gestion de la commutation et VLAN natifs de ce document pour plus d'informations.

Ne forcez pas trop sur la redondance. Ceci peut mener à trop de ports de blocage et peut compromettre la stabilité à long terme. Maintenez le diamètre STP total inférieur à sept sauts. Essayez d'appliquer la conception Cisco multicouches partout où cette conception est possible. Les fonctionnalités du modèle sont les suivantes :

- De plus petits domaines commutés
- Triangles STP
- Ports bloqués déterministes

Sachez où résident les fonctionnalités de base et les ports bloqués. Documentez cette information sur le diagramme de topologie. Connaissez votre topologie Spanning Tree, qui est essentielle pour le dépannage. Les ports bloqués constituent le point de départ du dépannage STP. La cause de la modification de blocage à transmission est souvent la partie principale d'analyse de la cause d'origine. Choisissez la distribution et les couches de base comme emplacement de racine/racine secondaire, puisque ces couches sont considérées comme les parties les plus stables du réseau. Vérifiez la couche 3 et le protocole HSRP (Hot Standby Router Protocol) pour détecter le recouvrement avec des chemins de données de la couche 2.

Cette commande est une macro qui configure la priorité de pont. La racine fixe la priorité à une valeur très inférieure à la valeur par défaut (32 768), et le secondaire fixe la priorité à une valeur raisonnablement inférieure à la valeur par défaut :

```
Switch(config)#interface type slot/port
Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

Remarque : Cette macro définit la priorité racine comme suit :

- 8192 valeur par défaut
- Priorité racine actuelle moins 1, si un autre pont racine est connu

- Priorité racine actuelle, si son adresse MAC est inférieure à la racine actuelle

Élaguez les VLAN inutiles des ports de liaison (exercice bidirectionnel). Cette action limite le diamètre du temps de traitement STP et NMP sur les portions du réseau où certains VLAN ne sont pas requis. L'élagage VTP automatique ne supprime pas STP d'une jonction. Vous pouvez également retirer le VLAN 1 par défaut des jonctions.

Référez-vous aux Problèmes et considérations de conception du protocole spanning tree pour plus d'informations.

Autres options

Cisco possède un autre protocole STP, appelé **VLAN-bridge**, qui fonctionne avec l'utilisation d'une adresse MAC de destination bien connue **01-00-0c-cd-cd-ce et du type de protocole 0x010c.**

Ce protocole est très utile en cas de besoin de pont non routable ou de présence de protocoles existants entre des VLAN sans interférence avec les instances IEEE Spanning Tree exécutées sur ces réseaux VLAN. Si les interfaces VLAN de trafic non ponté sont bloquées pour le trafic de couche 2, le trafic de la couche 3 en recouvrement est élagué par inadvertance, ce qui est un effet secondaire non désiré. Ce blocage de la couche 2 peut facilement se produire si les interfaces VLAN pour trafic de non-pontage utilisent le même STP que les VLAN IP. Le protocole VLAN-bridge est une instance STP séparée pour les protocoles pontés. Ce protocole fournit une topologie distincte qui peut être manipulée sans effet sur le trafic IP.

Exécutez le protocole VLAN-bridge si un pontage est requis entre les VLAN sur des routeurs Cisco tels que le MSFC.

Fonction STP PortFast

Vous pouvez utiliser PortFast afin d'ignorer le fonctionnement Spanning Tree normal sur des ports d'accès. PortFast accélère la connectivité entre les stations d'extrémité et les services auxquels les stations d'extrémité doivent se connecter après l'initialisation de la liaison. La mise en oeuvre de Microsoft DHCP doit inclure la définition du port d'accès en `mode forwarding une fois que l'état de la liaison passe à up , pour que la demande et la réception d'adresses IP soient possibles.` Certains protocoles, tels que les protocoles IPX (Internetwork Packet Exchange)/SPX (Sequenced Packet Exchange) supposent la définition du port d'accès en mode forwarding une fois que l'état de la liaison passe à up , afin d'éviter les problèmes GNS (Get Nearest Server).

Pour plus d'informations, reportez-vous à Utilisation de PortFast et d'autres commandes pour corriger les retards de connectivité au démarrage du poste de travail.

Aperçu opérationnel PortFast

PortFast ignore les états STP normaux (`listening`, `learning` et `forwarding`). La fonction déplace un port directement du mode `blocking vers le mode forwarding une fois que la liaison est active`. Si cette fonctionnalité n'est pas activée, STP ignore toutes les données utilisateur jusqu'à ce qu'il décide que le port est prêt à passer en `mode d'acheminement`. Ce processus peut prendre du temps (2 x ForwardDelay), fixé par défaut à 30 secondes.

`Le mode PortFast empêche la génération d'un avis de changement de topologie STP (TCN) chaque fois qu'un port passe de l'état learning à l'état forwarding`. Les TCN sont normaux. Mais une vague de TCN qui frappe le pont racine peut allonger inutilement la durée de convergence. Une vague de TCN se produit souvent le matin, au moment du démarrage des ordinateurs.

Recommandation Cisco en matière de configuration des ports d'accès

Définissez STP PortFast sur `on pour tous les ports d'hôte activés.` En outre, définissez explicitement STP PortFast sur `off pour les liens et les ports de commutateur à commutateur non utilisés.`

Émettez la commande macro **switchport host** dans le mode de configuration de l'interface afin de mettre en application la configuration recommandée pour les ports d'accès. La configuration facilite également les performances d'autonégociation et de connexion de manière significative :

```
switch(config)#interface type slot#/port#

switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
!--- This macro command modifies these functions.
```

Remarque : PortFast ne signifie pas que le Spanning Tree n'est pas exécuté du tout sur les ports. Les BPDU sont encore envoyés, reçus et traités. Spanning-Tree est essentiel pour bénéficier d'un LAN entièrement fonctionnel. Sans détection de boucle et sans blocage, une boucle peut involontairement mettre hors service le LAN entier rapidement.

En outre, désactivez la liaison de jonction et l'acheminement pour tous les ports hôte. Chaque port d'accès est activé par défaut pour l'agrégation de liens et l'acheminement, pourtant les voisins de commutation ne sont pas prévus à la base sur les ports hôtes. Si vous laissez ces protocoles négocier, le retard qui s'ensuit dans l'activation du port peut conduire à des situations indésirables. Des paquets initiaux de postes de travail, tels que des demandes DHCP et IPX, ne sont pas expédiés.

Une meilleure option consiste à configurer PortFast par défaut en mode de configuration globale avec l'utilisation de cette commande :

```
Switch(config)#spanning-tree portfast enable
```

Puis, sur n'importe quel port d'accès qui a un concentrateur ou un commutateur dans un seul VLAN, désactivez la fonctionnalité PortFast sur chaque interface à l'aide de la commande **interface :**

```
Switch(config)#interface type slot_num/port_num
Switch(config-if)#spanning-tree portfast disable
```

Autres options

La protection du protocole BPDU PortFast fournit une méthode permettant d'empêcher les boucles. La protection BPDU place un port sans agrégation à l'état `errDisable à la réception d'un BPDU sur ce port.`

Dans des conditions normales, ne recevez jamais aucun paquet BPDU sur un port d'accès qui est configuré pour PortFast. Un BPDU entrant indique une configuration incorrecte. La meilleure action est d'arrêter le port d'accès.

Le logiciel système Cisco IOS offre une commande globale utile qui active automatiquement `BPDU-ROOT-GUARD sur n'importe quel port activé pour UplinkFast.` *Utilisez toujours cette commande.* La commande fonctionne par commutateur et non par port.

Émettez cette commande globale afin d'activer `BPDU-ROOT-GUARD`:

```
Switch(config)#spanning-tree portfast bpduguard default
```

Une alerte SNMP (Simple Network Management Protocol) ou un message Syslog informe l'administrateur réseau si le port devient inactif. Vous pouvez également configurer une reprise automatique pour les ports `errDisabled`. Reportez-vous à la section Unidirectional Link Detection de ce document pour plus d'informations.

Référez-vous à Amélioration de Spanning Tree PortFast BPDU Guard pour plus d'informations.

Remarque : PortFast pour les ports agrégés a été introduit dans le logiciel Cisco IOS Version 12.1(11b)E. PortFast pour les ports de jonction est conçu pour augmenter les temps de convergence pour les réseaux de la couche 3. Quand vous utilisez cette fonction, veillez à désactiver BPDU Guard et le filtre BPDU sur une interface de base.

UplinkFast

Objectif

Uplinkfast fournit une convergence STP rapide après une défaillance de liaison directe dans la couche d'accès au réseau. UplinkFast fonctionne sans modification de STP. Le but est d'accélérer le temps de convergence dans une circonstance spécifique en le faisant passer à moins de trois secondes, plutôt que le délai par défaut de 30 secondes. Reportez-vous à Compréhension et configuration de la fonctionnalité Cisco UplinkFast

Aperçu opérationnel

Avec le modèle Cisco multicouche au niveau de la couche d'accès, la liaison montante bloquante passe immédiatement à un `état forwarding si la liaison montante d'expédition est perdue.` La fonction n'attend pas les `états d'écoute et d'apprentissage.`

Un groupe de liaisons ascendantes est un ensemble de ports par VLAN qui peut être considéré comme un port racine et un port racine de secours. Dans des conditions normales, les ports racine assurent la connectivité de l'accès vers la racine. Si cette connexion racine primaire échoue pour n'importe quelle raison, la liaison racine de secours intervient immédiatement sans devoir passer par les 30 secondes typiques du retard de convergence.

Puisqu'UplinkFast ignore le processus de modification-manipulation de topologie STP normal (`listening et learning`), un autre mécanisme de correction de topologie est nécessaire. Ce mécanisme a besoin de mettre à jour les commutateurs du domaine à l'aide des informations accessibles pour les stations d'extrémité locale, via un autre chemin. Ainsi, le commutateur de la couche d'accès qui utilise Uplinkfast produit également des trames pour chaque adresse MAC de sa table CAM envoyées à une adresse MAC multicast bien connue (01-00-0c-cd-cd-cd HDLC protocole 0x200a). Ce processus met à jour la table CAM de tous les commutateurs du domaine, à l'aide de la nouvelle topologie.

Recommandation Cisco

Cisco recommande d'activer UplinkFast pour les commutateurs d'accès avec ports bloqués si vous utilisez 802.1D spanning-tree. Ne l'utilisez pas sur les commutateurs sans connaissance implicite de la topologie d'une liaison racine de secours - typiquement la distribution et les commutateurs de base dans la conception Cisco multicouche. D'une façon générale, n'activez pas UplinkFast sur un commutateur avec plus de deux voies hors d'un réseau. Si le commutateur se trouve dans un environnement d'accès complexe et que plusieurs liaisons sont à l'état blocking (plus une liaison à l'état forwarding), évitez l'utilisation de cette fonction sur le commutateur, ou consultez votre ingénieur de services avancés.

Émettez cette commande globale afin d'activer UplinkFast :

```
Switch(config)#spanning-tree uplinkfast
```

Cette commande du logiciel Cisco IOS n'ajuste pas automatiquement toutes les valeurs de priorité de pont en spécifiant une valeur élevée. En revanche, elle ne modifie que les VLAN avec une priorité de pont qui n'a pas été changée manuellement. Par ailleurs, contrairement à CatOS, quand vous restaurez un commutateur sur lequel UplinkFast était activé, la forme de cette commande (**no spanning-tree UplinkFast**) rétablit toutes les valeurs par défaut qui ont été modifiées. Par conséquent, quand vous utilisez cette commande, vous *devez contrôler l'état actuel des priorités de pont avant et après, afin de vérifier que le résultat désiré est atteint.*

Remarque : Vous avez besoin du mot clé **all protocols** pour la commande UplinkFast lorsque la fonction de filtrage de protocole est activée. Comme le CAM enregistre le type de protocole aussi bien que les informations MAC et VLAN lorsque le filtrage de protocole est activé, une trame UplinkFast doit être générée pour chaque protocole sur chaque adresse MAC. Le mot clé **rate** indique le nombre de paquets par seconde des trames de mise à jour de la topologie UplinkFast. La valeur par défaut est recommandée. Vous n'avez pas besoin de configurer UplinkFast avec RSTP parce que le mécanisme est inclus et automatiquement activé dans RSTP.

BackboneFast

Objectif

BackboneFast fournit une convergence rapide des défaillances de liaison indirecte. BackboneFast ramène les temps de convergence de 50 secondes (valeur par défaut) à 30 secondes généralement et, de cette façon, ajoute la fonctionnalité à STP. De nouveau, cette fonction s'applique seulement quand vous exécutez 802.1D. Ne configurez pas la fonction quand vous utilisez Rapid PVST ou MST (qui incluent le composant rapide).

Aperçu opérationnel

BackboneFast est lancé quand un port racine ou un port bloqué sur un commutateur reçoit des BPDU inférieures du pont désigné. Le port reçoit généralement des BPDU inférieurs quand un commutateur en aval détruit la connexion à la racine et commence à envoyer des BPDU afin d'élire une nouvelle racine. Une BPDU inférieure identifie un commutateur comme pont racine et pont désigné.

Selon des règles normales de spanning-tree, le commutateur récepteur ignore les BPDU inférieurs pour le temps maxage time configuré. Par défaut, la durée de maxage est égale à 20

secondes. Mais, avec BackboneFast, le commutateur perçoit la BPDU inférieure comme un signal de modification possible de la topologie. Le commutateur utilise les BPDU RLQ (Root Link Query) pour déterminer s'il dispose d'un autre chemin pour l'accès au pont racine. Cet ajout de protocole RLQ permet à un commutateur de vérifier si la racine est encore disponible. RLQ passe un port bloqué à l'état `forwarding et informe le commutateur isolé qui a envoyé la BPDU inférieure que la racine est toujours là.`

Voici quelques points opérationnels importants sur le fonctionnement du protocole :

- Un commutateur transmet le paquet RLQ sur le port racine seulement (ce qui signifie que le paquet va vers la racine).
- Un commutateur qui reçoit un RLQ peut répondre si c'est le commutateur racine, ou si ce commutateur sait qu'il a perdu la connexion à la racine. Si le commutateur ne connaît pas ces faits, il doit expédier la requête à son port racine.
- Si un commutateur a perdu sa connexion à la racine, celle-ci doit répondre de manière négative à cette requête.
- La réponse doit être envoyée seulement via le port dont la requête est venue.
- Le commutateur racine doit toujours répondre à cette requête avec une réponse positive.
- Si la réponse est reçue sur un port non racine, ignorez la réponse.

L'opération peut diminuer les temps de convergence STP jusqu'à 20 secondes, parce que la durée maxage n'a pas besoin d'expirer. Référez-vous à Comprendre et configurer Backbone Fast sur des commutateurs Catalyst pour plus d'informations.

Recommandation Cisco

Activez BackboneFast sur tous les commutateurs qui exécutent STP seulement si le domaine spanning-tree entier peut supporter cette fonction. Vous pouvez ajouter la fonction sans interruption à un réseau de production.

Émettez cette commande globale afin d'activer BackboneFast :

```
Switch(config)#spanning-tree backbonefast
```

Remarque : Vous devez configurer cette commande de niveau global sur tous les commutateurs d'un domaine. Cette commande ajoute la fonction à STP ; tous les commutateurs doivent la comprendre.

Autres options

BackboneFast n'est pas pris en charge sur les commutateurs Catalyst 2900XL et 3500XL. Généralement vous devez activer BackboneFast si le domaine des commutateurs contient ces commutateurs en plus des commutateurs Catalyst 4500/4000, 5500/5000 et 6500/6000. Quand vous mettez en application BackboneFast dans des environnements comportant des commutateurs XL et des topologies strictes, vous pouvez activer la fonction à un emplacement au sein duquel le commutateur XL est le dernier commutateur de la ligne et n'est connecté qu'au noyau, à deux endroits. Ne mettez pas en application cette fonction si l'architecture des commutateurs XL est de mode guirlande.

Vous n'avez pas besoin de configurer BackboneFast avec RSTP ou 802.1w parce que le mécanisme est inclus de manière native et automatiquement activé dans RSTP.

Fonctionnalité de protection de Spanning Tree contre les boucles

La fonctionnalité de protection contre les boucles est une optimisation propriétaire Cisco pour STP. Le dispositif protecteur de boucle protège les réseaux de la couche 2 des boucles qui se produisent en raison d'un défaut de fonctionnement d'interface réseau, de CPU occupé, ou de tout ce qui empêche l'expédition normale de BPDU. Une boucle STP est créée lorsqu'un port de blocage de STP dans une topologie redondante passe par erreur dans l'état de transfert. Cela se produit habituellement parce qu'un des ports d'une topologie physiquement redondante (pas nécessairement le port bloquant) a cessé de recevoir des BPDU.

Le dispositif protecteur de boucle est seulement utile sur les réseaux commutés sur lesquels des commutateurs sont connectés via des liaisons point à point, comme c'est le cas dans la plupart des réseaux campus modernes et dans les centres de données. L'idée est que, sur une llaison point à point, un pont désigné ne peut pas disparaître sans envoyer une BPDU inférieure ou sans rendre la liaison inactive. La fonction STP de dispositif protecteur de boucle a été introduite dans le logiciel Cisco IOS Version 12.1(13)E pour commutateurs Catalyst 6500 et Cisco IOS Version 12.1(9)EA1 pour commutateurs Catalyst 4500.

Référez-vous à Amélioration du protocole Spanning Tree à l'aide des fonctionnalités de protection contre les boucles et de détection des différences de temps de propagation des BPDU pour plus d'informations sur la protection contre les boucles.

Aperçu opérationnel

Le dispositif protecteur de boucle contrôle si un port racine ou un autre port de sauvegarde reçoit des BPDU. Si le port ne reçoit pas de BPDU, le dispositif de protection contre les boucles met le port dans un état contradictoire (blocage) jusqu'à ce que le port recommence à recevoir des BPDU. Un port en état contradictoire ne transmet pas de BPDU. Si un tel port reçoit des BPDU de nouveau, le port (et la liaison) est considéré viable de nouveau. La condition contradictoire est retirée du port et STP détermine l'état du port. De cette façon, la reprise est automatique.

La fonctionnalité de protection contre les boucles isole la panne et laisse spanning tree converger vers une topologie stable sans la liaison ou le pont en échec. Le dispositif de protection contre les boucles évite les boucles STP avec la vitesse de la version STP en service. Il n'y a aucune dépendance au niveau de STP lui-même (802.1D ou 802.1w) ou du réglage des temporisateurs STP. Pour ces raisons, Cisco recommande de mettre en oeuvre le dispositif de protection contre les boucles en même temps que l'UDLD dans les topologies qui s'appuient sur le STP et où le logiciel prend en charge ces fonctions.

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

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

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

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

Interaction avec les autres fonctions STP

Protection de la racine

La protection de la racine force un port à être constamment désigné. Le dispositif protecteur de boucle est pertinent seulement si le port est un port racine ou un autre port, ce qui signifie que leurs fonctionnements sont mutuellement exclusifs. Par conséquent, le dispositif de protection contre les boucles et la protection de la racine ne peuvent pas être activés sur un port en même temps.

UplinkFast

La fonctionnalité de protection contre les boucles est compatible avec UplinkFast. Si le dispositif de protection contre les boucles met un port racine dans un état de blocage, UplinkFast place un nouveau port racine dans l'état de transmission. En outre, UplinkFast ne sélectionne pas un *port en état de boucle incohérente comme porte racine.*

BackboneFast

La fonctionnalité de protection contre les boucles est compatible avec BackboneFast. BackboneFast est déclenché par la réception d'un BPDU inférieur qui vient d'un pont désigné. Puisque les BPDU proviennent de cette liaison, le dispositif de protection contre les boucles n'intervient pas. Par conséquent, BackboneFast et dispositif protecteur de boucle sont compatibles.

PortFast

Portfast fait passer un port en mode désigné de transmission à l'activation de la liaison. Puisqu'un port en PortFast n'est pas un port racine ou un autre port, le dispositif de protection contre les boucles et PortFast s'excluent mutuellement.

PAgP

Le dispositif de protection contre les boucles utilise les ports qui sont connus à STP. Par conséquent, le dispositif de protection contre les boucles peut tirer profit de l'abstraction des ports logiques que PAgP fournit. Mais, afin de former un canal, tous les ports physiques groupés dans le canal doivent avoir des configurations compatibles. PAgP impose la configuration uniforme du dispositif de protection contre les boucles sur tous les ports physiques pour former un canal. Notez que ce sont des obstacles quand vous configurez le dispositif de protection contre les boucles sur un EtherChannel :

- STP sélectionne toujours le premier port opérationnel du canal pour envoyer les BPDU. Si cette liaison devient unidirectionnelle, la fonctionnalité de protection contre les boucles bloque le canal, même si d'autres liaisons dans le canal fonctionnent correctement.
- Si un ensemble de ports qui sont déjà bloqués par le dispositif protecteur de boucle est regroupé afin de former un canal, STP perd toutes les informations d'état pour ces ports, et le nouveau port de canal peut prendre l'état de transmission avec un rôle désigné.
- Si un canal est bloqué par la fonctionnalité de protection contre les boucles et si le canal est détruit, STP perd toutes les informations d'état. Les différents ports physiques peuvent atteindre l'état de transmission avec un rôle indiqué, même si une ou plusieurs des liaisons qui ont formé le canal sont unidirectionnelles.

Dans ces deux derniers cas, il est possible qu'une boucle se forme jusqu'à ce qu'UDLD détecte la panne. Mais le dispositif protecteur de boucle ne peut pas la détecter.

Comparaison des fonctionnalités de protection contre les boucles et UDLD

Le dispositif protecteur contre les boucles et la fonction UDLD de fonctionnalité se superposent partiellement, en partie dans un but de protection contre les pannes STP entraînées par les liaisons unidirectionnelles. Ces deux fonctions sont différentes dans l'approche du problème et également dans la fonctionnalité. Spécifiquement, il existe des défaillances continues spécifiques que l'UDLD ne peut pas détecter, comme les pannes qui sont provoquées par une CPU qui n'envoie pas de BPDU. En outre, l'utilisation de timers STP agressifs et du mode RSTP peut avoir comme conséquence la formation de boucles avant qu'UDLD puisse détecter les pannes.

Le dispositif de protection contre les boucles ne fonctionne pas sur les liaisons partagées ou dans les situations dans lesquelles la liaison a été unidirectionnelle depuis son activation. Dans le cas où une liaison a été unidirectionnelle depuis son activation, le port ne reçoit jamais de BPDU et devient indiqué. Ce comportement peut être normal, ainsi le dispositif de protection contre les boucles ne couvre pas ce cas particulier. UDLD fournit une protection contre un tel scénario.

L'activation d'UDLD et du dispositif protecteur de boucle fournit le plus haut niveau de protection possible. Pour plus d'informations sur la comparaison entre le dispositif protecteur de boucle et UDLD, référez-vous à :

- *Protection contre les boucles et détection de liaison unidirectionnelle* de la section Améliorations du protocole Spanning Tree à l'aide de la protection contre les boucles et des fonctions de détection de décalage BPDU
- la section UDLD de ce document

Recommandation Cisco

Cisco recommande d'activer le dispositif de protection contre les boucles globalement sur un réseau de commutation avec des boucles physiques. Vous pouvez activer le dispositif protecteur de boucle globalement sur tous les ports. En fait, la fonctionnalité est activée sur toutes les liaisons point à point. La liaison point à point est détectée par l'état duplex de la liaison. Si le mode duplex est bidirectionnel simultané, la liaison est considérée point à point.

```
Switch(config)#spanning-tree loopguard default
```

Autres options

Pour les commutateurs qui ne supportent pas une configuration globale de protection contre les boucles, la recommandation est d'activer la fonction sur tous les ports individuels, ce qui inclut les ports de canaux. Bien qu'il n'y ait aucun avantage à activer le dispositif protecteur de boucle sur un port désigné, ne considérez pas cette activation comme un problème. En outre, une reconvergence valide de spanning tree peut réellement transformer un port désigné en port racine, ce qui rend la fonction utile sur ce port.

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard loop
```

Les réseaux avec des topologies sans boucles peuvent encore tirer bénéfice de la fonctionnalité de protection contre les boucles dans le cas où des boucles sont introduites accidentellement. Mais l'activation du dispositif de protection contre les boucles dans ce type de topologie peut mener à des problèmes d'isolement du réseau. Si vous établissez une topologie sans boucles et que vous souhaitez éviter les problèmes d'isolement réseau, vous pouvez désactiver le dispositif protecteur de boucle globalement ou individuellement. N'activez pas la fonctionnalité de protection

contre les boucles sur des liaisons partagées.

```
Switch(config)#no spanning-tree loopguard default
!--- This is the global configuration.
```

ou

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no spanning-tree guard loop
!--- This is the interface configuration.
```

Protection de la racine Spanning tree

La fonctionnalité de protection de la racine fournit un moyen d'imposer le placement du pont racine dans le réseau. Le dispositif de protection de la racine garantit que le port sur lequel cette fonctionnalité est activée est le port désigné. Normalement, les ports du pont racine sont tous des ports désignés, à moins que deux ou plusieurs des ports du pont racine soient connectés ensemble. Si le pont reçoit des BDPU STP supérieurs sur un port où la protection de la racine est activée, cette protection place ce port à l'état de racine STP contradictoire. Cet état contradictoire est effectivement égal à un état d'écoute. Aucun trafic n'est acheminé sur ce port. De cette façon, le dispositif de protection de la racine impose la position du pont racine. Le dispositif de protection contre les boucles est disponible dans les premières versions du logiciel Cisco IOS 12.1E et dans les versions ultérieures.

Aperçu opérationnel

La protection de la racine est un mécanisme STP intégré. La protection de la racine n'a pas de timer propre et elle se fonde sur la réception de BPDU seulement. Quand ce dispositif est appliqué à un port, il refuse à ce port la possibilité de devenir un port racine. Si la réception d'une BPDU déclenche une convergence de spanning tree qui fait qu'un port désigné devient un port racine, le port est mis dans un état de racine contradictoire. Ce message Syslog illustre cette situation :

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

Une fois que le port a cessé d'envoyer des BPDU supérieures, il est de nouveau débloqué. Par l'intermédiaire de STP, le port va de l'état d'écoute à l'état d'apprentissage, et par la suite à l'état d'acheminement. Ce message Syslog illustre la transition :

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

La reprise est automatique. Aucune intervention humaine n'est nécessaire.

Puisque le dispositif de protection de la racine force la désignation d'un port et que le dispositif de protection contre les boucles n'est efficace que si le port est un port racine ou un autre port, ces fonctions s'excluent mutuellement. Par conséquent, le dispositif de protection contre les boucles et la protection de la racine ne peuvent pas être activés sur un port en même temps.

Référez-vous à Perfectionnement de la protection de la racine du protocole Spanning Tree pour plus d'informations.

Recommandation Cisco

Cisco recommande d'activer la fonction de protection de la racine sur les ports qui se connectent aux périphériques réseau qui ne sont pas sous contrôle administratif direct. Afin de configurer la protection de la racine, utilisez ces commandes quand vous êtes en mode de configuration de l'interface :

```
Switch(config)#interface type slot#/port#
Switch(config-if)#spanning-tree guard root
```

EtherChannel

Objectif

EtherChannel comprend un algorithme de distribution de trames qui multiplexe efficacement des trames à travers le composant 10/100 Mbps ou des liaisons Gigabit. L'algorithme de la distribution de trames permet le multiplexage inverse des plusieurs canaux en une liaison logique simple. Bien que chaque plate-forme diffère de la plate-forme suivante, vous devez comprendre ces propriétés communes :

- Il doit y avoir un algorithme pour multiplexer statistiquement les trames sur plusieurs canaux. Dans les commutateurs Catalyst, c'est lié au matériel. Voici quelques exemples :Catalyst 5500/5000s - La présence ou l'absence d'une puce EBC (Ethernet Bundling Chip) sur le moduleCatalyst 6500/6000s - Un algorithme qui peut lire plus loin dans les messages de trame et multiplexer par adresse IP
- Il y a création d'un canal logique de sorte qu'une instance simple STP puisse être exécutée ou qu'un appariement de routage puisse être utilisé, selon qu'il s'agit d'un EtherChannel de la couche 2 ou 3.
- Il y a un protocole de gestion à vérifier (cohérence des paramètres aux extrémités de la liaison et gestion de la reprise après la défaillance d'une liaison ou d'un ajout de liaison). Ce protocole peut être PAgP ou LACP (Link Aggregation Control Protocol).

Aperçu opérationnel

EtherChannel comprend un algorithme de distribution de trames qui multiplexe efficacement des trames à travers le composant 10/100 Mbps ou des liaisons Gigabit ou 10-Gigabit. Les différences dans les algorithmes par plate-forme résultent de la capacité de chaque type de matériel à extraire les informations d'en-tête de trame afin de prendre une décision de distribution.

L'algorithme de répartition des charges est une option globale pour les deux protocoles de contrôle de canal. PAgP et LACP utilisent l'algorithme de distribution de trames parce que le standard IEEE n'exige aucun algorithme particulier de distribution. Cependant, n'importe quel algorithme de distribution s'assure que, quand les trames sont reçues, l'algorithme n'entraîne pas de désordre dans les trames qui font partie de n'importe quelle conversation ou duplication de trames.

Ce tableau illustre l'algorithme de distribution de trames en détail pour chaque plate-forme énumérée :

Plate form	Algorithme d'équilibrage de charge du canal

e	
Gamme Catalyst 3750	Catalyst 3750 qui exécute le logiciel Cisco IOS équilibre en charge l'algorithme qui utilise les adresses MAC ou IP et la source ou la destination des messages (ou les deux).
Gamme Catalyst 4500	Catalyst 4500 qui exécute le logiciel Cisco IOS équilibre en charge l'algorithme qui utilise les adresses MAC ou IP (ou encore des numéros de ports de la couche 4) et la source ou la destination des messages (ou les deux).
Gamme Catalyst 6500/6000	Il y a deux algorithmes de hachage qui peuvent être utilisés, en fonction du Supervisor Engine. Le hachage est un polynôme de dix-septième-degré qui est mis en application dans le matériel. Dans tous les cas, les informations de hachage utilisent les adresses MAC ou IP (ou encore le numéro de port IP TCP/UDP) et appliquent l'algorithme afin de générer une valeur 3 bits. Ce processus se produit séparément pour les SA et les DA. Le fonctionnement XOR est ensuite utilisé avec les résultats afin de produire une autre valeur 3-bits. La valeur détermine le port du canal utilisé pour expédier le paquet. Des canaux sur Catalyst 6500/6000 peuvent être formés entre les ports de tout module et peuvent atteindre 8 ports.

Ce tableau indique les méthodes de distribution qui sont supportées sur les différents modèles Catalyst 6500/6000 du Supervisor Engine. Ce tableau montre également le comportement par défaut :

Matériel	Description	Méthodes de distribution
WS-F6020A (moteur de couche 2) WS-F6K-PFC (moteur de couche 3)	Supervisor Engine Ultérieur et Supervisor Engine IA Supervisor Engine IA/Policy Feature Card 1 (PFC1)	MAC de couche 2 : SA ; DA ; IP de couche 3 SA et DA : SA ; DA ; SA et DA (valeur par défaut)
WS-F6K-PFC 2	Supervisor engine II/PFC2	MAC de couche 2 : SA ; DA ; IP de couche 3 SA et DA : SA ; DA ; Session de couche 4 SA et DA (par défaut) : Port S ; port D ; Ports S et D
WS-F6K-PFC3A WS-F6K-	Supervisor Engine 720/PFC3A Supervisor Engine	MAC de couche 2 : SA ; DA ; IP de couche 3 SA et DA : SA ; DA ;

PFC3B WS-F6K-PFC3BXL	720/Supervisor Engine 32/PFC3B Supervisor Engine 720/PFC3BXL	Session de couche 4 SA et DA (par défaut) : Port S ; port D ; Ports S et D

Remarque : avec la distribution de couche 4, le premier paquet fragmenté utilise la distribution de couche 4. Tous les paquets suivants utilisent la distribution de la couche 3.

Remarque : reportez-vous à ces documents afin de trouver plus de détails sur la prise en charge d'EtherChannel sur d'autres plates-formes et sur la façon de configurer et de dépanner EtherChannel :

- Présentation de l'équilibrage de charge et de la redondance EtherChannel sur les commutateurs Catalyst
- Configuration d'EtherChannel couches 3 et 2 (guide de configuration du logiciel Cisco IOS pour Catalyst 6500, 12.2SX)
- Configuration d'EtherChannel couches 3 et 2 (guide de configuration du logiciel Cisco IOS pour Catalyst 6500, 12.1E)
- Configuration d'EtherChannel (guide de configuration du logiciel Cisco IOS pour commutateurs Catalyst 4500, 12.2(31)SG)
- Configuration des EtherChannel (guide de configuration de logiciel de commutateurs Catalyst 3750, 12.2(25)SEE)
- Configuration d'EtherChannel entre des commutateurs Catalyst 4500/4000, 5500/5000 et des commutateurs 6500/6000 qui exécutent le logiciel système CatOS

Recommandation Cisco

Les commutateurs Catalyst 3750, Catalyst 4500 et Catalyst 6500/6000 exécutent l'équilibrage de charge via le hachage par défaut des adresses IP source et de destination. Cela est recommandé, avec la supposition que l'IP est le protocole dominant. Émettez cette commande pour définir l'équilibrage de charge :

```
port-channel load-balance src-dst-ip
!--- This is the default.
```

Autres options

Selon les flux de trafic, vous pouvez utiliser la distribution de la couche 4 afin d'améliorer l'équilibrage de charge si la majorité du trafic est située entre la même adresse IP source et de destination. Vous devez comprendre que, quand la distribution de la couche 4 est configurée, le hachage inclut seulement les ports source et de destination de la couche 4. Il ne combine pas les adresses IP de la couche 3 dans l'algorithme de hachage. Émettez cette commande pour définir l'équilibrage de charge :

```
port-channel load-balance src-dst-port
```

Remarque : la distribution de couche 4 n'est pas configurable sur les commutateurs de la gamme Catalyst 3750.

Exécutez la commande **show etherchannel load-balance pour vérifier la politique de distribution**

des trames.

Selon les plates-formes matérielles, vous pouvez utiliser les commandes CLI afin de déterminer quelle interface d'EtherChannel achemine le flux de trafic spécifique, avec la politique de distribution de trames comme base.

Pour les commutateurs Catalyst 6500, émettez la commande **remote login switch pour vous connecter à distance à la console SP (Switch Processor).** Ensuite, exécutez la commande **test etherchannel load-balance interface port-channel number {ip | l4port | mac} [*source_ip_add* | *source_mac_add* | *port_source*] [***dest_ip_add* | *dest_mac_add* | *dest_l4_port*]**.

Pour les commutateurs Catalyst 3750, émettez la commande **test etherchannel load-balance interface port-channel number {ip | mac} [*source_ip_add* | *source_mac_add*] [***dest_ip_add* | *dest_mac_add*]**.

Pour Catalyst 4500, la commande équivalente n'est pas encore disponible.

Directives de configuration et restrictions d'EtherChannel

EtherChannel vérifie les propriétés de port sur tous les ports physiques avant qu'il agrège les ports compatibles dans un port logique simple. Les directives de configuration et les restrictions varient pour différentes plates-formes de commutation. Respectez ces directives et restrictions afin d'éviter les problèmes de groupement. Par exemple, si QoS est activé, les EtherChannels ne se forment pas si vous groupez des modules de commutation de la gamme Catalyst 6500/6000 avec différentes capacités QoS. Pour les commutateurs Catalyst 6500 qui exécutent le logiciel Cisco IOS, vous pouvez désactiver le contrôle d'attribut de port QoS sur le groupement EtherChannel à l'aide de la commande d'interface port-canal **no mls qos channel-consistency .** La commande **show interface capability *mod/port*** affiche la capacité de port QoS et détermine si des ports sont compatibles.

Reportez-vous à ces directives pour différentes plates-formes afin d'éviter des problèmes de configuration :

- Configuration d'EtherChannel couches 3 et 2 (guide de configuration du logiciel Cisco IOS pour Catalyst 6500, 12.2SX)
- Configuration d'EtherChannel couches 3 et 2 (guide de configuration du logiciel Cisco IOS pour Catalyst 6500, 12.1E)
- Configuration d'EtherChannel (guide de configuration du logiciel Cisco IOS pour commutateurs Catalyst 4500, 12.2(31)SG)
- Configuration des EtherChannel (guide de configuration de logiciel de commutateurs Catalyst 3750, 12.2(25)SEE)

Le nombre maximal d'EtherChannels pris en charge dépend également de la plate-forme matérielle et des versions de logiciel. Les commutateurs Catalyst 6500 qui exécutent le logiciel Cisco IOS Version 12.2(18)SXE et versions ultérieures prennent en charge un nombre maximal de 128 interfaces port-canal. Les versions de ce logiciel antérieures à la version 12.2(18)SXE prennent en charge un nombre maximal de 64 interfaces port-canal. Le nombre de groupes configurables peut être compris entre 1 et 256, quelle que soit la version du logiciel. Les commutateurs Catalyst 4500 prennent en charge un nombre maximal de 64 EtherChannels. Pour les commutateurs Catalyst 3750, la recommandation est de ne pas configurer plus de 48 EtherChannels sur la pile de commutateurs.

Calcul de coût de port Spanning Tree

Vous devez comprendre le calcul de coût de port Spanning Tree pour les EtherChannels. Vous pouvez calculer le coût du port Spanning Tree pour EtherChannel selon la méthode courte ou longue. Par défaut, le coût du port est calculé en mode court.

Ce tableau illustre le coût du port Spanning Tree pour un EtherChannel de couche 2 en fonction de la bande passante :

Bande passante	Ancienne valeur STP	Nouvelle valeur STP longue
10 Mbits/s	100	2,000,000
100 Mbits/s	19	200,000
1 Gbit/s	4	20,000
N X 1 Gbit/s	3	6660
10 Gbits/s	2	2,000
100 Gbit/s	S/O	200
1 Tbit/s	S/O	20
10 Tbit/s	S/O	2

Remarque : dans CatOS, le coût du port Spanning Tree pour un EtherChannel reste le même après la défaillance de la liaison de membre du canal de port. Dans le logiciel Cisco IOS, le coût du port pour l'EtherChannel est mis à jour immédiatement afin de refléter la nouvelle bande passante disponible. Si le comportement désiré est d'éviter les modifications inutiles de topologie Spanning Tree, vous pouvez statiquement configurer le coût de port Spanning Tree via l'utilisation de la commande **spanning-tree cost** ***coût*** .

Protocole d'agrégation de ports (PAgP)

Objectif

PAgP est un protocole de gestion qui examine la cohérence des paramètres aux deux extrémités de la liaison. PAgP aide également le canal à s'adapter à la défaillance ou à l'ajout de liaison. Voici les caractéristiques de PAgP :

- PAgP nécessite que tous les ports du canal appartiennent au même réseau VLAN ou soient configurés comme ports de liaison agrégée. (Puisque les VLAN dynamiques peuvent forcer le passage d'un port dans un VLAN différent, ils ne sont pas inclus dans la participation d'EtherChannel.)
- Quand il existe déjà un lot et que la configuration d'un port est modifiée, tous les ports du lot sont modifiés afin de correspondre à cette configuration. Un exemple d'une telle modification est une modification de VLAN ou une modification de `mode de jonction.`
- Le PAgP ne regroupe pas les ports qui fonctionnent à des vitesses ou à un mode bidirectionnel différents. Si la vitesse et le mode bidirectionnel sont modifiés alors qu'un groupement existe, le PAgP modifie la vitesse et le mode bidirectionnel de tous les ports du groupement.

Aperçu opérationnel

Le port PAgP contrôle chacun des ports physiques (ou logiques) à grouper. Les mêmes adresses MAC multicast que celles utilisées pour les paquets CDP servent à envoyer les paquets PAgP. L'adresse MAC est 01-00-0c-cc-cc-cc. Mais la valeur du protocole est 0x0104. Voici un résumé du

fonctionnement du protocole :

- Tant que le port physique est actif, les paquets PAgP sont transmis toutes les secondes pendant la détection et toutes les 30 secondes en état équilibré.
- Si les paquets de données sont reçus mais aucun paquet PAgP, on suppose que le port est connecté à un périphérique non-compatible PAgP.
- L'écoute des paquets PAgP prouve que le port physique a une connexion bidirectionnelle à un autre périphérique compatible PAgP.
- Dès que deux paquets sont reçus sur un groupe de ports physiques essayez de former un port agrégé.
- Si les paquets PAgP s'arrêtent pendant une période, l'état PAgP passe à `down`.

Traitement normal

Ces concepts expliquent le comportement du protocole :

- Agport - un port logique composé de tous les ports physiques dans la même agrégation, il peut être identifié par son propre SNMP ifIndex. Un agport ne contient pas de ports non-opérationnels.
- Canal - Une agrégation qui répond aux critères de formation. Un canal peut contenir des ports non-opérationnels et est une version élaborée d'agport. Les protocoles, qui incluent STP et VTP mais excluent CDP et DTP, sont exécutés au-dessus de PAgP sur les agports. Aucun de ces protocoles ne peut envoyer ou recevoir de paquets jusqu'à ce que PAgP attache les agports à un ou plusieurs ports physiques.
- Capacité de groupe — chaque port physique et chaque agport possède un paramètre de configuration appelé la capacité de groupe. Un port physique peut être agrégé avec n'importe quel autre port physique qui a la même `capacité de groupe`, et seulement avec un tel port physique.
- Procédure d'agrégation — Lorsqu'un port physique atteint l'état UpData ou UpPAgP , le port est associé à un agport approprié. Quand le port quitte l'un ou l'autre de ces états pour un autre état, il est isolé de l'agport.

Ce tableau fournit davantage d'informations sur les états :

Province	Signification
`DonnéesHaut`	Aucun paquet PAgP n'a été reçu. Des paquets PAgP sont envoyés. Le port physique est le seul connecté à l'agport. Les paquets non-PAgP sont échangés entre le port physique et l'agport.
`BiDir`	Exactement un paquet PAgP a été reçu, ce qui prouve qu'une connexion bidirectionnelle existe à exactement un voisin. Le port physique n'est connecté à aucun agport. Les paquets PAgP sont envoyés et peuvent être reçus.
`PAgPsHaut`	Ce port physique, peut-être en association avec d'autres ports physiques, est connecté à un agport. Les paquets PAgP sont envoyés et reçus sur le port physique. Les paquets non-PAgP sont échangés entre le port physique et l'agport.

Les deux extrémités des deux connexions doivent convenir sur le groupement. Le groupement est défini comme le plus grand groupe de ports de l'agport que les deux extrémités de la connexion permettent d'obtenir.

Quand un port physique atteint l'état d'UpPAgP, il est assigné à l'agport qui a des ports physiques membres qui correspondent à la capacité de groupe du nouveau port physique et qui sont dans les états de BiDir ou d' UpPAgP . (De tels ports `BiDir sont passés à l'état UpPAgP en même temps.)` S'il n'y a aucun agport dont les paramètres constitutifs de port physique sont compatibles avec le port physique nouvellement prêt, celui-ci est assigné à un agport avec des paramètres appropriés qui n'a aucun port physique associé.

PAgP peut expirer sur le dernier voisin connu sur le port physique. Le port qui arrive à expiration est retiré de l'agport. En même temps, tous les ports physiques sur le même agport dont les timers ont également expiré sont enlevés. Ceci permet à un agport dont l'autre extrémité est morte d'être désactivé tout d'un coup, au lieu d'un port physique à la fois.

Comportement en cas de panne

Si une liaison de canal existant échoue, l'agport est mis à jour et le trafic est haché au niveau des liens qui restent sans perte. Les exemples d'une telle défaillance incluent :

- Le port est débranché
- Le GBIC (convertisseur d'interface Gigabit) (GBIC) est retiré
- Une fibre est cassée

Remarque : lorsque vous échouez à une liaison dans un canal avec une mise hors tension ou la suppression d'un module, le comportement peut être différent. Par définition, un canal exige deux ports physiques. Si un port est perdu par le système dans un canal à deux ports, l'agport logique est désactivé et le port physique initial est réinitialisé par rapport au spanning tree. Le trafic peut être ignoré jusqu'à ce que STP permette au port de devenir à nouveau disponible aux données.

Cette différence dans les deux modes de défaillance est importante quand vous prévoyez la maintenance d'un réseau. Il peut y avoir un changement de topologie STP dont vous devez tenir compte quand vous exécutez un retrait ou une mise en place en ligne d'un module. Vous devez gérer chaque liaison physique du canal avec le système de gestion de réseaux (NMS) puisque l'agport n'est pas perturbé par une panne.

Complétez une de ces recommandations afin d'atténuer des changements de topologie non désirés sur Catalyst 6500/6000 :

- Si un port est utilisé par module afin de former un canal, utilisez trois modules ou davantage (trois totaux).
- Si le canal enjambe deux modules, utilisez deux ports sur chaque module (quatre totaux).
- Si un canal à deux ports est nécessaire sur deux cartes, utilisez seulement les ports de Supervisor Engine.

Options de configuration

Vous pouvez configurer des EtherChannels dans différents modes, comme récapitulé dans le tableau suivant :

Mode	Options configurables
`On (activé`	PAgP n'est pas en fonctionnement. Les canaux

)	du port, indépendamment de la façon dont le port voisin est configuré. Si le mode du port voisin est on, un canal est formé.
« Auto »	L'agrégation est sous le contrôle du protocole PAgP. Un port est placé dans un état de négociation passive. Aucun paquet PAgP n'est envoyé sur l'interface jusqu'à ce qu'au moins un paquet PAgP soit reçu qui indique que l'expéditeur fonctionne en mode desirable.
« Desirable »	L'agrégation est sous le contrôle du protocole PAgP. Un port est placé dans un état de négociation actif, dans lequel le port entame des négociations avec d'autres ports par l'intermédiaire de la transmission de paquets PAgP. Un canal est formé avec un autre groupe de ports en mode desirable ou auto .
Non-Silencieux Il s'agit de la valeur par défaut sur les ports FE et GE fibre optique du Catalyst 5500/5000.	Un mot clé en mode auto ou desirable. Si aucun paquet de données n'est reçu sur l'interface, l'interface n'est jamais attachée à un agport et ne peut pas être utilisée pour des données. Ce contrôle de bidirectionalité a été donné pour des équipements Catalyst 5500/5000 spécifiques, car certaines défaillances de liaison ont comme conséquence une coupure du canal. Lorsque vous activez le mode non-silent, un port voisin en récupération ne peut jamais se réactiver et disloquer le canal inutilement. Des contrôles plus flexibles et efficaces du groupement et de la bidirectionnalité sont présents par défaut sur le matériel de la gamme Catalyst 4500/4000 et 6500/6000.
Silent : valeur par défaut sur tous les ports Catalyst 6500/6000 et 4500/4000, ainsi que sur les	Un mot clé en mode auto ou desirable. Si aucun paquet de données n'est reçu sur l'interface, après une période de temporisation de 15 secondes, l'interface seule est attachée à un agport. Ainsi, l'interface peut être utilisée pour la transmission de données. Le mode Silent permet également au canal de fonctionner quand le partenaire est un analyseur ou un serveur qui n'envoie jamais de PAgP.

ports cuivre 5500/5000.	

Le paramètre `silent/non-silent affecte la façon dont les ports réagissent aux situations entraînant un trafic unidirectionnel.` Quand un port ne peut pas transmettre en raison d'une interface physique échouée ou d'une fibre ou d'un câble cassé(e), le port voisin peut être laissé à l'état opérationnel. Le partenaire continue à transmettre des données. Mais ces données sont perdues parce que le trafic de retour ne peut pas être reçu. Des boucles de Spanning Tree peuvent également se former en raison de la nature unidirectionnelle de la liaison.

Certains ports fibre ont la capacité désirée de faire passer le port en état non-opérationnel quand il perd son signal de réception (FEFI). Cette action force le port associé à passer en mode non-opérationnel et les deux ports d'extrémité de la liaison à devenir inactifs.

Quand vous utilisez des périphériques qui transmettent des données (BPDU), si vous ne pouvez pas détecter des conditions unidirectionnelles, utilisez le `mode non silent afin de permettre aux ports de rester non-opérationnels jusqu'à ce que les données soient présentes et que la vérification de la liaison permette d'affirmer qu'elle est bidirectionnelle.` Le temps passé par PAgP pour détecter une liaison unidirectionnelle est d'environ 3,5 * 30 secondes = 105 sec. Trente secondes est la durée entre deux messages PAgP successif ayant abouti. Utilisez UDLD, qui est un détecteur plus rapide de liens unidirectionnels.

Quand vous utilisez des périphériques qui ne transmettent aucune donnée, utilisez le mode `silent.` L'utilisation du mode `silent force le port à devenir connecté et opérationnel, indépendamment du fait que les données reçues soient présentes ou non.` Par ailleurs, pour les ports qui peuvent détecter la présence d'une condition unidirectionnelle, le mode `silent est utilisé par défaut.` Des exemples de ces ports sont les nouvelles plates-formes qui utilisent la couche 1 FEFI et UDLD.

Afin de mettre hors fonction l'acheminement sur interface, émettez la commande **no-channel-group number** :

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no channel-group 1
```

Vérification

Le tableau de cette section présente un résumé de tous les possibles scénarios de mode de canalisation LACP-à-PAgP entre deux commutateurs directement connectés (commutateur A et commutateur B) Certaines de ces combinaisons peuvent mener STP à mettre les ports du côté canalisation en état `errDisable (ce qui signifie que certaines des combinaisons arrêtent les ports du côté canalisation).` La fonction de dispositif protecteur de configuration d'EtherChannel est activée par défaut.

Mode canal du commutateur A	Mode canal du commutateur B	État du canal du commutateur A	État du canal du commutateur B
On (activé)	On (activé)	Channel (non-PAgP)	Channel (non-PAgP)

On (activé)	Non configuré	Not Channel (errdisable)	Not Channel
On (activé)	« Auto »	Not Channel (errdisable)	Not Channel
On (activé)	« Desirable »	Not Channel (errdisable)	Not Channel
Non configuré	On (activé)	Not Channel	Not Channel (errdisable)
Non configuré	Non configuré	Not Channel	Not Channel
Non configuré	« Auto »	Not Channel	Not Channel
Non configuré	« Desirable »	Not Channel	Not Channel
« Auto »	On (activé)	Not Channel	Not Channel (errdisable)
« Auto »	Non configuré	Not Channel	Not Channel
« Auto »	« Auto »	Not Channel	Not Channel
« Auto »	« Desirable »	Canal PAgP	Canal PAgP
« Desirable »	On (activé)	Not Channel	Not Channel
« Desirable »	Non configuré	Not Channel	Not Channel
« Desirable »	« Auto »	Canal PAgP	Canal PAgP
« Desirable »	« Desirable »	Canal PAgP	Canal PAgP

Recommandation de configuration Cisco pour les canaux L2

Activez PAgP et utilisez une configuration desirable-desirable sur toutes les liaisons Etherchannel. Pour plus d'informations, voir la sortie suivante :

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no ip address
!--- This ensures that there is no IP !--- address that is assigned to the LAN port.
Switch(config-if)#channel-group number mode desirable
!--- Specify the channel number and the PAgP mode.
```

Vérifiez la configuration de cette façon :

```
Switch#show run interface port-channel number
Switch#show running-config interface type slot#/port#
Switch#show interfaces type slot#/port# etherchannel
Switch#show etherchannel number port-channel
```

Prévention des erreurs de configuration EtherChannel

Vous pouvez mal configurer un EtherChannel et créer une boucle Spanning Tree. Cette configuration incorrecte peut affecter le processus de commutation. Le logiciel Cisco IOS inclut la fonction **spanning-tree etherchannel guard misconfig qui permet d'éviter ce problème.**

Émettez cette commande de configuration sur tous les commutateurs Catalyst qui exécutent le logiciel Cisco IOS en tant que logiciel système :

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

Autres options

En acheminant deux périphériques qui ne supportent pas PAgP mais supportent LACP, la recommandation est d'activer LACP avec configuration de LACP actif sur les deux extrémités des périphériques. Reportez-vous à la section Protocole de contrôle d'agrégation de lien (LACP) de ce document pour plus d'informations.

En effectuant une transmission vers des périphériques qui ne supportent pas PAgP ou LACP, vous devez coder en dur le canal sur `on`. Cette exigence s'applique à ces exemples de périphériques :

- Serveurs
- Local Director
- Commutateurs de contenu
- Routeurs
- Commutateurs avec le logiciel antérieur
- Commutateurs Catalyst 2900XL/3500XL
- Catalyst 8540s

Émettez les commandes suivantes :

```
Switch(config)#interface type slot#/port#
Switch(config-if)#channel-group number mode on
```

Protocole de contrôle d'agrégation de lien (LACP)

Le LACP est un protocole qui permet à des ports aux caractéristiques semblables de former un canal par la négociation dynamique avec les commutateurs contigus. PAgP est un protocole propriétaire de Cisco que vous pouvez exécuter uniquement sur les commutateurs Cisco et sur les commutateurs qui sont fabriqués par les constructeurs autorisés. Mais LACP, qui est défini dans IEEE 802.3ad, permet aux commutateurs Cisco de gérer la canalisation Ethernet avec des périphériques qui se conforment à la spécification 802.3ad.

Le LACP est supporté avec ces plates-formes et versions :

- Gammes Catalyst 6500/6000 avec versions du logiciel Cisco IOS 12.1(11b)EX et ultérieures
- Gammes Catalyst 4500 avec versions du logiciel Cisco IOS 12.1(13)EW et ultérieures
- Gammes Catalyst 3750 avec versions du logiciel Cisco IOS 12.1(14)EA1 et ultérieures

Il y a très peu de différence entre le LACP et le PAgP d'un point de vue fonctionnel. Les deux protocoles supportent un maximum de huit ports dans chaque canal, et les mêmes propriétés de

port sont contrôlées avant la formation du groupement. Ces propriétés comprennent :

- Vitesse
- Duplex
- VLAN natif et type de jonction

Les différences notables entre le LACP et le PAgP sont :

- Le LACP peut s'exécuter seulement sur des ports en mode bidirectionnel simultané , et ne supporte pas les ports bidirectionnels en alternat.
- Le protocole LACP prend en charge les ports de secours immédiat. Le LACP essaye toujours de configurer le nombre maximal de ports compatibles dans un canal, jusqu'au nombre maximal que le matériel autorise (huit ports). Si le LACP ne peut pas agréger tous les ports qui sont compatibles (par exemple, si le système distant a des limitations matérielles plus restrictives), tous les ports qui ne peuvent pas être activement inclus dans le canal sont placés dans l'état de secours immédiat et utilisés seulement si un des ports utilisés échoue.

Remarque : pour les commutateurs de la gamme Catalyst 4500, le nombre maximal de ports pour lesquels vous pouvez attribuer la même clé administrative est de huit. Pour les commutateurs Catalyst 6500 et 3750 qui exécutent le logiciel Cisco IOS, LACP essaye de configurer le nombre maximal de ports compatibles dans un EtherChannel, jusqu'au nombre maximum que le matériel permet (huit ports). Huit ports supplémentaires peuvent être configurés en tant que ports de veille.

Aperçu opérationnel

LACP contrôle chaque port physique individuel (ou logique) à grouper. Les paquets LACP sont envoyés à l'aide de l'adresse MAC de groupe multipoint **01-80-c2-00-00-02**. Le type/valeur du champ est 0x8809 avec un sous-type de 0x01. Voici un résumé du fonctionnement du protocole :

- Le protocole s'appuie sur les périphériques pour annoncer leurs capacités d'agrégation et leurs informations d'état. Les transmissions sont envoyées sur une base régulière et périodique sur chaque liaison « agrégable ».
- Tant que le port physique est up, les paquets LACP sont transmis toutes les secondes pendant la détection et toutes les 30 secondes en état équilibré.
- Les partenaires d'une liaison « agrégable » écoutent l'information qui est envoyée au sein du protocole et décident quelles actions prendre.
- Des ports compatibles sont configurés dans un canal, jusqu'au nombre maximal que le matériel autorise (huit ports).
- Les agrégations sont maintenues par l'échange régulier et opportun d'informations d'état à jour entre les partenaires de liaison. Si la configuration change (en raison d'une défaillance de liaison, par exemple), les partenaires de protocole expirent et prennent les mesures appropriées sur la base du nouvel état de système.
- En plus des transmissions périodiques de l'unité de données LACP (LACPDU), s'il y a une modification des informations d'état, le protocole transmet un LACPDU sur événement aux partenaires. Les partenaires de protocole prennent les mesures appropriées sur la base du nouvel état de système.

Paramètres LACP

Afin de permettre à LACP de déterminer si un ensemble de liaisons se connecte au même système et si ces liaisons sont compatibles du point de vue de l'agrégation, il est nécessaire de pouvoir établir les points suivants :

- Un identifiant global unique pour chaque système participant à l'agrégation de liaisons.Chaque système qui exécute LACP doit porter une priorité qui peut être choisie ou automatique (avec la priorité par défaut de 32768) ou définie par l'administrateur. La priorité système est principalement utilisée en conjonction avec l'adresse MAC du système afin de former l'identifiant système.
- Un moyen d'identifier les capacités associées à chaque port et chaque agrégateur, car un système donné les comprend.Chaque port du système doit porter une priorité qui peut être affectée ou automatique (avec la priorité par défaut de 128) ou définie par l'administrateur. La priorité est utilisée en conjonction avec le numéro de port afin de former l'identifiant de port.
- Un moyen d'identifier link un groupe d'agrégation de liaisons et son agrégateur associé.La capacité d'un port à s'agréger avec un autre est récapitulée par un paramètre de 16 bits simple de nombre entier qui est plus grand que zéro, appelé clé. Chaque clé est déterminée sur la base de différents facteurs, tels que :Les caractéristiques physiques de port, qui incluent le débit, la bidirectionnalité et le point à point ou médium partagéContraintes de configuration établies par l'administrateur réseauDeux clés sont associées à chaque port :Une clé administrativeUne clé opérationnelleLa clé administrative permet la manipulation des valeurs de la clé par la gestion, et par conséquent, l'utilisateur peut choisir cette clé. La clé opérationnelle est utilisée par le système afin de former des agrégations. L'utilisateur ne peut pas choisir ou directement changer cette clé. L'ensemble de ports d'un système donné qui partagent la même valeur de clé opérationnelle sont considérés comme des membres du même groupe de clés.

Ainsi, si deux systèmes et un ensemble de ports portent la même clé administrative, chaque système tente d'agréger les ports, à partir du port affichant la plus haute priorité au sein du système le plus prioritaire. Ce comportement est possible parce que chaque système connaît ces priorités :

- Sa propre priorité, que l'utilisateur ou le logiciel a assignée
- La priorité de son partenaire, qui a été indiquée par les paquets LACP

Comportement en cas de panne

Le comportement en cas de panne pour LACP est identique au comportement en cas de panne pour PAgP. Si une liaison dans un canal existant a échoué (par exemple, si un port est débranché, un GBIC est retiré, ou une fibre est cassée), l'agport est mis à jour et le trafic est haché au niveau des autres liaisons en l'espace d'1 seconde. Tout trafic qui n'a pas besoin d'être réhaché après la panne (trafic qui continue à transmettre sur la même liaison) n'enregistre aucune perte. La restauration de la liaison qui a échoué déclenche une autre mise à jour sur l'agport, et le trafic est haché de nouveau.

Options de configuration

Vous pouvez configurer des EtherChannels LACP dans différents modes, comme récapitulé dans le tableau suivant :

Mode	Options configurables
On (activé)	La formation de l'agrégation de lien est forcée sans aucune négociation LACP. Le commutateur ni n'envoie le paquet LACP ni ne traite n'importe quel paquet LACP entrant. Si le mode du port voisin est on, un canal est formé.

Off (ou) non configuré	Le port ne canalise pas, indépendamment de la façon dont le port voisin est configuré.
Passive (valeur par défaut)	Ce mode est semblable au mode **auto dans PAgP.** Le commutateur ne lance pas le canal, mais comprend les paquets LACP entrants. L'homologue (dans l'état actif) lance une négociation (en envoyant un paquet LACP) que le commutateur reçoit et à laquelle il répond, formant par la suite le canal d'agrégation avec l'homologue.
Actif	Ce mode est semblable au mode **desirable dans PAgP.** Le commutateur entame la négociation pour former une liaison agrégée. L'agrégat de liaisons est formé si l'autre extrémité s'exécute en mode LACP active ou passive .

LACP utilise un compteur d'intervalle de 30 secondes (Slow_Periodic_Time) après que les EtherChannels LACP sont établis. Le nombre de secondes avant l'invalidation d'informations LACPDU reçues en utilisant de longs délais d'attente (3 fois le Slow_Periodic_Time) est 90. UDLD est recommandé comme détecteur plus rapide des liaisons unidirectionnelles. Vous ne pouvez pas ajuster les temporisateurs LACP et à ce stade, vous ne pouvez pas configurer les commutateurs en vue de l'utilisation de la transmission PDU (chaque seconde) pour mettre à jour le canal une fois formé.

Vérification

Le tableau de cette section présente un résumé de tous les possibles scénarios de mode de canalisation LACP entre deux commutateurs directement connectés (commutateur A et commutateur B). Certaines de ces combinaisons peuvent amener le dispositif protecteur d'EtherChannel à placer les ports du côté canalisation dans l'état errdisable. La fonction de dispositif protecteur de configuration d'EtherChannel est activée par défaut.

Mode canal du commutateur A	Mode canal du commutateur B	État du canal du commutateur A	État du canal du commutateur B
On (activé)	On (activé)	Canal (non LACP)	Canal (non LACP)
On (activé)	Off (désactivé)	Not Channel (errdisable)	Not Channel
On (activé)	Passif	Not Channel (errdisable)	Not Channel
On (activé)	Actif	Not Channel (errdisable)	Not Channel
Off (désactivé)	Off (désactivé)	Not Channel	Not Channel
Off (désactivé)	Passif	Not Channel	Not Channel

Off (désactivé)	Actif	Not Channel	Not Channel
Passif	Passif	Not Channel	Not Channel
Passif	Actif	Canal LACP	Canal LACP
Actif	Actif	Canal LACP	Canal LACP

Recommandations Cisco

Cisco recommande d'activer PAgP sur des connexions de canal entre les commutateurs Cisco. En acheminant deux périphériques qui ne supportent pas PAgP mais supportent LACP, la recommandation est d'activer LACP avec configuration de LACP actif sur les deux extrémités des périphériques.

Sur les commutateurs qui exécutent CatOS, tous les ports sur Catalyst 4500/4000 et Catalyst 6500/6000 utilisent par défaut le protocole PAgP. Afin de configurer des ports pour utiliser LACP, vous devez définir le protocole de canal des modules sur LACP. LACP et PAgP ne peuvent pas s'exécuter sur le même module sur les commutateurs qui exécutent CatOS. Cette limitation ne s'applique pas aux commutateurs qui exécutent le logiciel Cisco IOS. Les commutateurs qui exécutent le logiciel Cisco IOS peuvent prendre en charge PAgP et LACP sur le même module. Emettez ces commandes pour définir le mode de canal LACP (mode actif) et pour affecter un numéro de clé administrative :

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode active
```

La commande **show etherchannel summary un affiche un récapitulatif sur une ligne par groupe de canaux qui inclut cette information :**

- Numéros de groupe
- Numéros de canal de port
- État des ports
- Les ports qui font partie du canal

La commande **show etherchannel port-channel affiche des informations détaillées de canal de port pour tous les groupes de canaux.** La sortie inclut ces informations :

- Statut du canal
- Protocole utilisé
- Durée écoulée depuis que les ports ont été regroupés

Afin d'afficher les informations détaillées pour un groupe de canaux spécifique, avec le détail de chaque port montré séparément, utilisez la commande *channel_number de show etherchannel detail* . La sortie de commande inclut les détails sur le partenaire et les détails sur le canal de port. Référez-vous à Configuration de LACP (802.3ad) entre Catalyst 6500/6000 et Catalyst 4500/4000 pour plus d'informations.

Autres options

Avec les périphériques de canal qui ne supportent pas PAgP ou LACP, vous devez coder en dur le canal sur `on`. Cette condition s'applique à ces périphériques :

- Serveurs
- Local Director
- Commutateurs de contenu
- Routeurs
- Commutateurs avec logiciel plus ancien
- Commutateurs Catalyst 2900XL/3500XL
- Catalyst 8540s

Émettez les commandes suivantes :

```
Switch(config)#interface range type slot#/port#
Switch(config-if)#channel-group admin_key mode on
```

Unidirectional Link Detection

Objectif

L'UDLD est un protocole propriétaire Cisco et léger qui a été développé pour détecter des instances de transmissions unidirectionnelles entre les périphériques. Il existe d'autres méthodes permettant de détecter l'état bidirectionnel des supports de transmission, telles que FEFI. Mais dans certains cas, les mécanismes de détection de la couche 1 ne sont pas suffisants. Ces scénarios peuvent avoir comme conséquence :

- Le fonctionnement imprévisible de STP
- La diffusion incorrecte ou excessive de paquets
- La formation de trous noirs dans le trafic

La fonction UDLD est destinée à faire face à ces conditions de panne sur des interfaces Ethernet fibre et cuivre :

- Elle permet de surveiller les configurations de câblage physiques et d'arrêter les ports mal câblés en tant que errDisabled .
- Protège contre les liaisons unidirectionnelles—Quand une liaison unidirectionnelle est détectée, en raison d'une défaillance de média ou de ports/interfaces, le port affecté est arrêté en tant que errDisabled. Un message Syslog correspondant est produit.
- En outre, le mode UDLD agressif vérifie qu'une llaison bidirectionnelle précédente ne perd pas la connectivité au cas où elle deviendrait inutilisable en raison de l'encombrement. Le mode UDLD agressif effectue en continu des tests de connectivité au niveau de la liaison. L'objectif principal du mode UDLD agressif consiste à éviter les trous noirs dans le trafic dans certaines conditions d'échec qui ne sont pas prises en charge par le mode UDLD normal.

Référez-vous à Comprendre et configurer le protocole Unidirectional Link Detection (UDLD) pour plus de détails.

Spanning-tree a un flux BPDU continu équilibré et peut rencontrer les pannes que cette section mentionne. Un port peut soudainement échouer dans la transmission de BPDU, ce qui entraîne une modification d'état STP (de `blocage à transfert sur le voisin.` Cependant, il reste une boucle, car le port est toujours capable de réception.

Aperçu opérationnel

UDLD est un protocole de couche 2 qui fonctionne au-dessus de la couche LLC (MAC de destination 01-00-0c-cc-cc-cc, protocole SNAP HDLC 0x0111). Quand vous exécutez UDLD en combination avec des mécanismes FEFI et d'autonégociation de la couche 1, vous pouvez valider l'intégrité physique (L1) et logique (L2) d'une liaison.

UDLD prend des dispositions au niveau des fonctions et de la protection que FEFI et l'autonégociation ne peuvent pas exécuter. Ces fonctions incluent :

- La détection et la mise en cache des informations sur les voisins
- L'arrêt de tous les ports mal connectés
- La détection des mauvais fonctionnements ou des pannes de l'interface/des ports logiques qui ne sont pas point à pointRemarque : lorsque les liaisons ne sont pas point à point, elles traversent des convertisseurs de supports ou des concentrateurs.

UDLD utilise ces deux mécanismes de base.

1. UDLD se renseigne sur les voisins et actualise les informations correspondantes dans un cache local.
2. UDLD envoie un train des sondes/écho UDLD (messages Hello) pour la détection d'un nouveau voisin, ou chaque fois qu'un voisin demande une resynchronisation du cache.

UDLD envoie constamment des messages sonde/écho à tous les ports. A la réception d'un message UDLD correspondant sur un port, une phase de détection et de validation est déclenchée. Le port est activé si toutes les conditions valides sont remplies. Ces conditions sont remplies si le port est bidirectionnel et est correctement câblé. Si les conditions ne sont pas remplies, le port est `errDisabled`, ce qui déclenche le message Syslog suivant :

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

Pour obtenir la liste complète des messages système par installation (ce qui inclut les événements UDLD), référez-vous à Messages UDLD (Cisco IOS System Messages, volume 2/2).

Après l'établissement d'une liaison et sa classification comme bidirectionnelle, UDLD continue d'envoyer des messages sonde/écho à un intervalle par défaut de 15 secondes.

Ce tableau fournit des informations sur les états du port :

État du port	commentaire
Indéterminé	La Détection en cours ou une entité UDLD voisine a été désactivée.
Sans objet	UDLD a été désactivé.
Arrêt	Une liaison unidirectionnelle a été détectée et le port a été désactivé.
Enjeux bidirectionnels	Une liaison bidirectionnelle a été détectée.

Maintenance du cache du voisin

UDLD envoie périodiquement des paquets de sonde/écho sur chaque interface active afin de maintenir l'intégrité du cache UDLD voisin. Toutes les fois qu'un message Hello est reçu, il est mis en cache et maintenu dans la mémoire pendant une période maximale appelée temps de maintien. Quand le temps de maintien expire, l'entrée cache correspondante est vieillie. Si un nouveau message sonde est reçu au cours de la période de maintien, la nouvelle entrée remplace l'ancienne et le temporisateur time-to-live correspondant est réinitialisé.

Toutes les fois qu'une interface UDLD est désactivée ou qu'un périphérique est réinitialisé, toutes les entrées existantes de cache pour les interfaces affectées par les modifications de configuration sont effacées. Cela met à jour l'intégrité du cache UDLD. UDLD transmet au moins un message pour informer les voisins respectifs de la nécessité de vider les entrées de cache correspondantes.

Mécanisme de détection d'écho

Le mécanisme de détection d'écho forme la base de l'algorithme de détection. Toutes les fois qu'un périphérique UDLD se renseigne sur un nouveau voisin ou reçoit une demande de resynchronisation d'un voisin hors synchronisation, il ouvre/relance la fenêtre de détection de son côté de la connexion et envoie des rafales de messages d'écho en réponse. Puisque ce comportement doit être identique à travers tous les voisins, l'expéditeur d'écho compte recevoir des échos en réponse. Si la fenêtre de détection ne reçoit pas de messages de réponse valides, la liaison est considérée comme étant unidirectionnelle. A partir de ce moment, un rétablissement de liaison ou un processus d'arrêt de port peut être déclenché. Les autres conditions anormales rares contrôlées par le périphérique sont les suivantes :

- Transmissions retournées en boucle (Tx) au connecteur de Rx du même port
- Erreurs de câblage dans le cas d'une interconnexion de supports partagés (par exemple, un concentrateur ou un périphérique semblable)

Temps de convergence

Afin d'empêcher les boucles STP, dans le Logiciel Cisco IOS Version 12.1 et versions ultérieures, l'intervalle de messages par défaut UDLD a été ramené de 60 secondes à 15 secondes. Cet intervalle a été changé afin d'arrêter une llaison unidirectionnelle avant qu'un port autrefois bloqué dans Spanning-tree 802.1D puisse effectuer une transition vers un état de transmission. La valeur d'intervalle des messages détermine le débit auquel un voisin envoie des sondes UDLD après la phase de liaison ou de détection. L'intervalle des messages n'a pas besoin d'être le même aux deux extrémités de la liaison, bien que la configuration constante soit désirable si possible. Quand des voisins UDLD sont établis, l'intervalle des messages configurés est envoyé au voisin et le délai de temporisation pour cet homologue est calculé :

```
3 * (message interval)
```

Un rapport de partenariat expire après trois sondes ou Hellos consécutifs manqués. Puisque les intervalles des messages sont différents de chaque côté, cette valeur de temporisation est simplement différente de chaque côté, et un côté identifie une panne plus rapidement.

La durée approximative qui est nécessaire pour qu'UDLD détecte une défaillance unidirectionnelle d'une liaison auparavant stable est approximativement :

```
2.5 * (message interval) + 4 seconds
```

41 secondes environ avec l'intervalle des messages par défaut de 15 secondes. Ce temps est beaucoup plus court que les 50 secondes qui sont habituellement nécessaires pour que STP reconverge. Si le CPU NMP a quelques cycles disponibles et que l'utilisateur surveille soigneusement son niveau d'utilisation (bonne pratique), une réduction de l'intervalle des messages à la valeur minimale de 7 secondes est acceptable. En outre, cette réduction d'intervalle accélère la détection selon un facteur important.

Remarque : le minimum est de 1 seconde dans le logiciel Cisco IOS Version 12.2(25)SEC.

Par conséquent, UDLD une dépendance assumée aux timers de spanning tree par défaut. Si STP est réglé pour converger plus rapidement qu'UDLD, envisagez un mécanisme alternatif, tel que la fonction de protection contre les boucles STP. Envisagez dans ce cas un mécanisme alternatif, quand vous mettez en application RSTP (802.1w) également, parce que RSTP a des caractéristiques de convergence en ms, selon la topologie. Pour ces instances, utilisez la fonction de protection contre les boucles en conjonction avec UDLD, ce qui assure une protection maximale. Le dispositif de protection contre les boucles évite les boucles STP avec la vitesse de la version STP en service. Et UDLD effectue une détection des connexions unidirectionnelles sur différentes liaisons Etherchannel ou lorsque les BPDU n'empruntent pas la direction interrompue.

Remarque : UDLD est indépendant de STP. UDLD ne détecte pas chaque situation de panne STP, telle que les pannes qui sont provoquées par un CPU qui n'envoie pas de BPDU pendant une durée supérieure à (2 * FwddDelay + maxage). Pour cette raison, Cisco recommande que vous mettiez en application UDLD en même temps que le dispositif de protection contre les boucles dans les topologies basées sur STP.

Attention : Méfiez-vous des versions antérieures d'UDLD dans les commutateurs 2900XL/3500XL qui utilisent un intervalle de messages par défaut de 60 secondes non configurable. Il est possible que des états de boucle Spanning-tree aient lieu.

Mode UDLD agressif

La détection UDLD agressive a été créée spécifiquement pour faire face aux (rares) cas dans lesquels un test de la connectivité bidirectionnelle est nécessaire. En soi, le mode agressif assure une protection améliorée contre des états dangereux de liaison unidirectionnelle dans ces situations :

- Quand la perte des PDU UDLD est symétrique et que les deux extrémités dépassent le temps d'attente. Dans ce cas, aucun des deux ports n'entre en état errdisabled.
- Un côté d'une liaison a un port collé (Tx et Rx).
- Un côté d'une liaison demeure actif tandis que l'autre côté est devenu inactif.
- L'autonégociation, ou un mécanisme différent de détection des pannes de la couche 1, est désactivé.
- Une réduction de la fiabilité dans les mécanismes FEFI de la couche 1 est souhaitable.
- Une protection maximale contre les défaillances de liaisons unidirectionnelles sur des liaisons point à point FE/GE est nécessaire. Spécifiquement, lorsqu'aucune panne entre deux voisins n'est admissible, les sondes UDLD en mode agressif peuvent être considérées comme un « battement de coeur » dont la présence garantit la santé de la liaison.

Les circonstances les plus communes pour la mise en place d'UDLD agressif est l'exécution d'un contrôle de connectivité sur un membre d'un groupement quand l'autonégociation ou un

mécanisme différent de détection des pannes de la couche 1 est désactivé ou inutilisable. C'est particulièrement utile avec les connexions EtherChannel parce que PAgP et LACP, même si activés, n'utilisent pas de timers de sonde faibles en état équilibré. Dans ce cas, le mode UDLD agressif a l'avantage supplémentaire d'éviter de potentielles boucles de spanning tree.

Il est important de comprendre qu'UDLD en mode normal vérifie une liaison unidirectionnelle, même après qu'elle ait atteint l'état bidirectionnel. UDLD a pour objectif de détecter les problèmes de la couche 2 qui entraînent des boucles STP, et ces problèmes sont habituellement unidirectionnels parce que les BPDU s'écoulent seulement dans une direction en état équilibré. Par conséquent, l'utilisation de l'UDLD en mode normal en même temps que l'autonégociation et la protection contre les boucles (pour les réseaux qui s'appuient sur STP) est presque toujours suffisante. UDLD en mode agressif étant activé, une fois que tous les voisins d'un port ont vieilli, dans la phase d'annonce ou de détection, UDLD redémarre la séquence d'établissement de liaison, afin d'obtenir une resynchronisation avec des voisins potentiellement hors synchronisation. Si après une série rapide de messages (huit relances échouées), la liaison est encore considérée comme « indéterminée », le port est alors placé en état errdisable.

Remarque : certains commutateurs ne sont pas compatibles UDLD agressifs. Actuellement, les commutateurs Catalyst 2900XL et Catalyst 3500XL ont des intervalles de messages encodés de 60 secondes. Ceci n'est pas considéré comme suffisamment rapide pour assurer la protection contre les boucles STP potentielles (avec les paramètres STP par défaut).

Reprise automatique des liaisons UDLD

La récupération sur errdisable est globalement désactivée par défaut. Une fois activé globalement, si un port entre en état errdisable, il est réactivé automatiquement après un délai sélectionné. Ce délai est de 300 secondes par défaut, qui est un timer global maintenu pour tous les ports dans un commutateur. Selon la version du logiciel, vous pouvez manuellement empêcher une réactivation de port si vous définissez la temporisation errdisable pour que ce port soit désactivé avec l'utilisation du mécanisme de reprise errdisable pour UDLD :

```
Switch(config)#errdisable recovery cause udld
```

Considérez l'utilisation de la fonction d'expiration errdisable quand vous mettez en application le mode UDLD agressif sans capacités d'administration de réseau hors bande, en particulier dans la couche d'accès ou sur n'importe quel périphérique qui peut devenir isolé du réseau en cas de situation errdisable.

Référez-vous à errdisable recovery (Guide de référence des commandes Cisco IOS de la gamme Catalyst 6500, 12.1 E) pour plus de détails sur la façon de configurer un délai d'attente pour les ports dans l'état errdisable.

La récupération errdisable peut être particulièrement importante pour UDLD dans la couche d'accès, quand les commutateurs d'accès sont distribués à travers un environnement de campus et que la visite manuelle de chacun d'entre eux visant à réactiver les deux liaisons ascendantes prend un temps considérable.

Cisco ne recommande pas la récupération errdisable au niveau du noyau du réseau, parce qu'il y a typiquement de multiples points d'entrée dans un noyau, et la reprise automatique dans le noyau peut entraîner des problèmes périodiques. Par conséquent, vous devez manuellement réactiver un port au niveau du noyau si UDLD désactive le port.

UDLD sur des liaisons routées

Pour les besoins de cette discussion, une liaison routée répond à l'un de ces deux types de connexion :

- Point à point entre deux noeuds de routeurs (configurés avec un masque de sous-réseau de 30 bits)
- UN VLAN avec plusieurs ports mais prenant en charge seulement les connexions routées, comme dans une topologie de noyau de la couche 2 de fractionnement

Chaque protocole IGRP (Interior Gateway Routing Protocol) a des caractéristiques uniques en ce qui concerne la façon dont il gère les relations de voisinage et la convergence d'itinéraires. Cette section décrit les caractéristiques qui sont pertinentes quand vous mettez en contraste deux des protocoles de routage les plus répandus qui sont utilisés aujourd'hui, Open Shortest Path First (OSPF) et Enhanced IGRP (EIGRP).

Remarque : Une défaillance de couche 1 ou de couche 2 sur un réseau point à point entraîne l'arrêt quasi immédiat de la connexion de couche 3. Puisque le seul port de commutation dans des transitions VLAN est à un état non connecté sur la panne de la couche 1/2, la fonction d'état automatique d'interface synchronise les états du port de la couche 2 et de la couche 3 en approximativement deux secondes et place l'interface VLAN de la couche 3 dans un état actif/inactif (le protocole de ligne étant inactif).

Si vous utilisez les valeurs de temporisateur par défaut, OSPF envoie des messages Hello toutes les 10 secondes et a un intervalle d'inactivité de 40 secondes (4 * Hello). Ces timers sont cohérents pour les réseaux de diffusion et OSPF point-à-point. Puisqu'OSPF nécessite une communication bidirectionnelle afin de former une juxtaposition, le temps de basculement peut être maximum de 40 secondes. C'est vrai même si la panne de la couche 1/2 n'est pas sur une connexion point-à-point et laisse un scénario à demi opérationnel que le protocole de la couche 3 doit traiter. Puisque le temps de détection d'UDLD est très semblable à la durée d'expiration d'un timer OSPF (environ 40 secondes), les avantages de configuration du mode normal d'UDLD sur une liaison OSPF de couche 3 point-à-point sont limités.

Dans de nombreux cas, EIGRP converge plus rapidement qu'OSPF. Mais il est important de noter que la transmission bi-directionnelle n'est pas une condition requise pour que les voisins puissent échanger des informations de routage. Dans les scénarios de fonctionnement à demi opérationnel très spécifiques, EIGRP est vulnérable face aux trous noirs dans le trafic qui durent jusqu'à ce qu'un autre événement « active » les routes menant à ce voisin. UDLD en mode normal peut alléger cette situation, parce qu'il détecte la défaillance de liaison unidirectionnelle et désactive le port.

Pour les connexions routées de la couche 3 qui utilisent n'importe quel protocole de routage, UDLD en mode normal assure toujours la protection contre les problèmes d'activation de liaison initiale, tels que les erreurs de câblage ou un matériel défectueux. En outre, le mode UDLD agressif fournit ces avantages sur les connexions routées de couche 3 :

- Empêche les trous noirs inutiles de trafic (avec temporisation minimale dans certains cas)
- Place une liaison oscillante en état errdisable
- Protège contre les boucles qui résultent des configurations de l'EtherChannel de la couche 3

Comportement par défaut d'UDLD

UDLD est désactivé globalement et activé dans la promptitude sur des ports fibre par défaut. Puisqu'UDLD est un protocole d'infrastructure qui est nécessaire entre les commutateurs

seulement, il est désactivé par défaut sur les ports cuivre, qui tendent à être utilisés pour l'accès aux hôtes. Notez qu'UDLD doit être activé globalement et au niveau de l'interface avant que les voisins ne puissent atteindre l'état bidirectionnel. L'intervalle des messages par défaut est de 15 secondes. Mais l'intervalle des messages par défaut peut être de sept secondes dans certains cas. Référez-vous à l'ID de bogue Cisco CSCea70679 (clients inscrits uniquement) pour plus d'informations. L'intervalle des messages par défaut est configurable entre sept et 90 secondes, et UDLD en mode agressif est désactivé. Le Logiciel Cisco IOS Version 12.2(25)SEC ramène cette durée minimale à une seconde.

Recommandation de configuration Cisco

Dans la grande majorité des cas, Cisco recommande d'activer le mode normal d'UDLD sur toutes les liaisons FE/GE point à point entre les commutateurs Cisco, et de définir l'intervalle des messages UDLD à 15 secondes lorsque vous utilisez les temporisateurs Spanning-tree 802.1D par défaut. Par ailleurs, lorsque les réseaux sont basés sur STP pour la redondance et la convergence (ce qui signifie qu'il y a un ou plusieurs ports en état de blocage STP dans la topologie), il est recommandé d'utiliser UDLD avec les fonctions et protocoles appropriés. Ces fonctions incluent FEFI, l'auto-négociation, la protection contre les boucles, entre autres. Typiquement, si l'autonégociation est activée, le mode agressif n'est pas nécessaire parce que l'autonégociation compense la détection de panne sur la couche 1.

Émettez l'une de ces deux commandes afin d'activer UDLD :

Note : La syntaxe a changé sur différentes plates-formes/versions.

- ```
  udld enable
  !--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.
  udld port
  ```

  ou

- ```
  udld enable
  !--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled
  by individual port command.
  ```

Vous devez manuellement activer les ports qui sont arrêtés en raison des symptômes de liaisons unidirectionnelles. Utilisez l'une de ces méthodes :

```
udld reset
!--- Globally reset all interfaces that UDLD shut down. no udld port
udld port [aggressive]
!--- Per interface, reset and reenable interfaces that UDLD shut down.
```

Les commandes de configuration **errdisable recovery cause udld** et ***errdisable recovery interval interval*** peuvent être utilisées pour la récupération automatique à partir de l'état UDLD error-disabled.

Cisco recommande que vous utilisiez seulement le mécanisme errdisable recovery dans la couche d'accès du réseau, avec des temporisateurs de 20 minutes ou plus, si l'accès physique au commutateur est difficile. La meilleure solution consiste à allouer un certain temps à la stabilisation et au dépannage réseau, avant que le port ne soit rétabli, ce qui risquerait d'entraîner

une instabilité réseau.

Cisco recommande de ne *pas utiliser les mécanismes de reprise dans le noyau du réseau, parce que cela risque d'entraîner une instabilité liée aux événements de convergence chaque fois qu'une liaison défectueuse est rétablie.* La conception redondante d'un réseau de base fournit un chemin de secours pour un échec de liaison et tient compte de la durée d'investigation sur les raisons de la défaillance UDLD.

Utilisation d'UDLD sans dispositif STP de protection contre les boucles

Pour les liaisons de la couche 3 point à point, ou de la couche 2 avec topologie STP sans boucles (aucun port bloquant), Cisco recommande d'activer le mode agressif d'UDLD pour les liaisons FE/GE point à point entre les commutateurs Cisco. Dans ce cas, l'intervalle de messages est défini à sept secondes, et STP 802.1D utilise des temporisateurs par défaut.

UDLD sur des EtherChannels

Si la protection contre les boucles STP est déployée ou n'est pas déployée, le mode agressif d'UDLD est recommandé pour toutes les configurations d'EtherChannel, avec le mode canal approprié. Dans les configurations EtherChannel, une défectuosité de la liaison du canal qui porte les BPDU Spanning-tree et le trafic de contrôle PAgP peut entraîner des boucles immédiates entre les partenaires du canal si les liaisons sont dégroupées. UDLD en mode agressif arrête un port en échec. PAgP (mode auto/recommandé) peut alors négocier une nouvelle liaison de contrôle et supprimer efficacement du canal une liaison en échec.

UDLD avec 802.1w spanning-tree

Afin d'empêcher les boucles quand vous utilisez de nouvelles versions de Spanning-tree, utilisez UDLD en mode normal et le dispositif STP de protection contre les boucles avec les RSTP tels que 802.1w. UDLD peut assurer la protection contre les liaisons unidirectionnelles pendant une phase d'établissement de la liaison, et le dispositif STP de protection contre les boucles peut empêcher les boucles STP au cas où les liaisons deviendraient unidirectionnelles *après que l'UDLD ait établi les liaisons comme étant bidirectionnelles.* Puisque vous ne pouvez pas configurer UDLD pour afficher une valeur inférieure à celle des temporisateurs par défaut 802.1w, le dispositif STP de protection contre les boucles est requis pour empêcher entièrement la survenue de boucles dans les topologies redondantes.

Référez-vous à Comprendre et configurer le protocole Unidirectional Link Detection (UDLD) pour plus de détails.

Test et surveillance d'UDLD

UDLD n'est pas facile à tester sans composant véritablement défectueux/unidirectionnel dans le laboratoire, tel qu'un GBIC défectueux. Le protocole a été conçu pour détecter les scénarios de panne moins communs que les scénarios qui sont habituellement utilisés dans un laboratoire. Par exemple, si vous exécutez un simple test comme débrancher un fil de fibre afin de voir l'`état errdisable souhaité, vous devez arrêter d'abord l'autonégociation de la couche 1.` Autrement, le port physique se `désactive`, ce qui réinitialise la communication de messages UDLD. L'extrémité distante accède à l'état `indéterminé dans le mode normal d'UDLD, et n'accède à l'état errdisable qu'avec l'utilisation du mode agressif d'UDLD.`

Une autre méthode de test consiste à simuler la perte PDU pour le voisin. Cette méthode consiste à utiliser des filtres de couche Mac afin de bloquer l'adresse matérielle UDLD/CDP, tandis que

vous laissez passer les autres adresses. Certains commutateurs n'envoient pas de trames UDLD quand le port est configuré pour être une destination de Switched Port Analyzer (SPAN), ce qui simule un voisin UDLD qui ne répond plus.

Pour la surveillance d'UDLD, utilisez cette commande :

```
show udld gigabitethernet1/1
Interface Gi1/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5
```

En outre, dans le mode enable du Logiciel Cisco IOS Version 12.2(18)SXD (ou versions ultérieures), vous pouvez exécuter la commande masquée **show udld neighbor afin de contrôler le contenu de cache UDLD (exactement comme le fait CDP).** Il est souvent très utile de comparer le cache UDLD et le cache CDP afin de vérifier s'il y a une anomalie au niveau du protocole. Toutes les fois que le CDP est également affecté, cela signifie généralement que tous les BPDU/PDU sont affectés. Par conséquent, contrôlez STP également. Par exemple, vérifiez les modifications récentes d'identité de racine ou de placement de racine/port désigné.

Vous pouvez surveiller l'état UDLD et la cohérence de configuration grâce aux variables Cisco UDLD SNMP MIB.

Commutation multicouches

Aperçu

Dans le logiciel Cisco IOS, la commutation multicouches (MLS) est prise en charge sur les gammes Catalyst 6500/6000, et seulement en interne. Ceci signifie que le routeur doit être installé dans le commutateur. Les nouveaux Supervisor Engine Catalyst 6500/6000 prennent en charge MLS CEF, dans lequel la table de routage est téléchargée dans chaque carte. Ceci exige un matériel supplémentaire, qui inclut la présence d'une carte de transfert distribué (DFC). Les DFC ne sont pas pris en charge dans le logiciel CatOS, même si vous choisissez d'utiliser le Logiciel Cisco IOS sur la carte du routeur. Les DFC sont uniquement pris en charge dans le logiciel système Cisco IOS.

Le cache du MLS qui est utilisé pour activer les statistiques Netflow sur les commutateurs Catalyst est le cache utilisé par la carte du Supervisor Engine I et par les commutateurs Catalyst existants pour activer la commutation de couche 3. MLS est activé par défaut sur le Supervisor Engine 1 (ou moteur 1A) avec MSFC ou MSFC2. Aucune configuration supplémentaire n'est requise pour les fonctions MLS par défaut. Vous pouvez configurer le cache MLS selon l'un des trois modes suivants :

- destination
- source-destination
- port source-destination

Le masque de flux est utilisé pour déterminer le mode MLS du commutateur. Ces données seront ultérieurement utilisées pour activer les écoulements de la couche 3 des commutateurs Catalyst

Supervisor Engine IA. Les lames de Supervisor Engine II n'utilisent pas le cache MLS pour la commutation des paquets, car cette carte est une carte matérielle CEF, ce qui correspond à une technologie beaucoup plus évolutive. Le cache MLS est mis à jour dans la carte de Supervisor Engine II afin d'activer l'exportation statistique Netflow seulement. Par conséquent, Supervisor Engine II peut être activé pour le flux complet si nécessaire, sans impact négatif sur le commutateur.

Configuration

Le vieillissement MLS s'applique à toutes les entrées de cache MLS. La valeur de vieillissement est appliquée directement à la destination. Vous divisez MLS la valeur de vieillissement par deux afin de dériver le vieillissement source-destination. Divisez la valeur de vieillissement MLS par huit pour trouver le vieillissement de flux complet. La valeur de vieillissement MLS par défaut est égale à 256 secondes.

Vous pouvez configurer le vieillissement normal de l'ordre de 32 à 4092 secondes selon des incréments de huit secondes. Toute valeur de durée de vieillissement qui n'est pas un multiple de huit secondes est ajustée sur le multiple le plus proche de 8 secondes. Par exemple, une valeur de 65 est ajustée à 64 et une valeur de 127 est ajustée à 128.

D'autres événements peuvent entraîner la purge des entrées MLS. Ces événements incluent :

- Les modifications de routage
- Un changement de l'état de la liaisonPar exemple, la liaison PFC est inactive.

Afin de garder la taille de cache du MLS au-dessous de 32.000 entrées, activez ces paramètres après avoir émis la commande **mls le vieillissement :**

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

Configuration

Généralement, une entrée de cache supprimée est une entrée qui est acheminée de et vers un serveur DNS (Domain Name Server) ou un server TFTP ne pouvant être réutilisé une fois l'entrée créée. La détection et la suppression de ces entrées permet d'économiser de l'espace dans le cache MLS pour le trafic d'autres données.

Si vous devez activer le vieillissement rapide MLS, définissez la valeur initiale à 128 sec. Si la taille du cache MLS continue à se développer au-delà de 32.000 entrées, diminuez la configuration jusqu'à ce que la taille de cache reste au-dessous de 32.000. Si le cache continue à se développer au-dessus de 32.000 entrées, diminuez la durée de vieillissement normal de MLS.

Configuration MLS recommandée par Cisco

Laissez la valeur par défaut MLS (destination seulement), à moins que l'exportation de Netflow ne soit requise. Si Netflow est requis, activez le flux complet MLS uniquement sur les systèmes de Supervisor Engine II.

Émettez cette commande afin d'activer la destination de flux MLS :

```
Switch(config)#mls flow ip destination
```

Trames jumbo

Unité de transmission maximale

Le MTU (Maximum Transmission Unit) correspond au plus grand datagramme ou à la plus grande taille de paquet qu'une interface peut envoyer ou recevoir sans fragmenter le paquet.

Selon la norme IEEE 802.3, la taille maximale de trame Ethernet est la suivante :

- **1518 octets pour les trames régulières (1500 octets plus 18 octets supplémentaires d'en-tête Ethernet et de queue de bande CRC)**
- **1522 octets pour les trames encapsulées 802.1Q (1518 plus 4 octets de balisage)**

Baby giant : La fonction Baby giants laisse le commutateur transmettre des paquets légèrement plus volumineux que le MTU IEEE Ethernet, plutôt que de déclarer les trames surdimensionnées et de les jeter.

Jumbo : La définition de la taille de la trame dépend du constructeur, car elle ne fait pas partie de la norme IEEE. Les trames Jumbo sont des trames qui sont plus grandes que la taille de trame Ethernet standard (qui est de 1518 octets, en incluant l'en-tête de la couche 2 et la séquence de contrôle de trame [FCS]).

La taille de MTU par défaut est de 9 216 octets après l'activation de la prise en charge de trames étendues sur le port individuel.

Quand prévoir des paquets plus volumineux que 1518 octets

Pour acheminer un trafic sur des réseaux commutés, vérifiez que le trafic MTU transmis ne dépasse pas le trafic pris en charge par les plates-formes des commutateurs. Il existe plusieurs raisons expliquant que la taille MTU de certaines trames puisse être tronquée :

- **Conditions spécifiques au constructeur — Les applications et certains NIC peuvent spécifier une taille de MTU en dehors de la norme de 1500 octets.** Cette modification s'est produite en raison des études qui montrent qu'une augmentation de la taille d'une trame Ethernet peut augmenter le débit moyen.
- **Agrégation de liens - Afin de diffuser les informations ID de VLAN entre les commutateurs ou d'autres périphériques réseau, l'agrégation a été utilisée pour augmenter la trame Ethernet standard.** Aujourd'hui, les deux formes les plus communes d'agrégation de liens sont :L'encapsulation ISL Cisco802.1Q
- **MPLS (Multiprotocol Label Switching) - Après avoir activé MPLS sur une interface, MPLS a le potentiel d'augmenter la taille de la trame d'un paquet, qui dépend du nombre d'étiquettes présent dans la pile d'étiquettes pour un paquet balisé MPLS.** La taille totale d'une étiquette

est de 4 octets. La taille totale d'une pile d'étiquettes est :

```
n * 4 bytes
```

Si une pile d'étiquettes est formée, les trames peuvent dépasser le MTU.

- **Transmission tunnel 802.1Q — Les paquets de transmission tunnel 802.1Q contiennent deux étiquettes 802.1Q, dont seulement une à la fois est habituellement visible au niveau du matériel.** Par conséquent, l'étiquette interne ajoute 4 octets à la valeur de MTU (taille de charge utile).
- **UTI (Universal Transport Interface)/Layer 2 Tunneling Protocol Version 3 (Layer 2TPv3)** - UTI/Layer 2TPv3 encapsule les données de couche 2 à transmettre sur le réseau IP. UTI/Layer 2TPv3 peut augmenter la taille de la trame initiale jusqu'à 50 octets. La nouvelle trame inclut un nouvel en-tête IP (20 octets), un en-tête 2TPv3 (12 octets) et un nouvel en-tête de la couche 2. La charge utile 2TPv3 comprend la trame complète de la couche 2, qui inclut l'en-tête de la couche 2.

Objectif

La commutation réalisée par matériel ultra-rapide (1-Gbps et 10-Gbps) a fait des trames Jumbo une solution très concrète aux problèmes de débit non optimal. Bien qu'il n'y ait aucune norme officielle pour la taille des trames Jumbo, une valeur assez commune qui est souvent adoptée est 9216 octets (9 Ko).

Considération d'efficacité du réseau

Vous pouvez calculer l'efficacité du réseau pour une transmission de paquets si vous divisez sa taille de charge utile par la somme de la valeur de surcharge et de la taille de charge utile.

Même si l'augmentation de l'efficacité de mise en réseau avec les trames Jumbo est modeste (elle va de 94,9 pour cent (1500 octets) à 99,1 pour cent (9216 octets), le temps système de traitement (utilisation du microprocesseur) des périphériques réseau et des hôtes d'extrémité diminue proportionnellement à la taille de paquet. C'est pourquoi les technologies de mise en réseau LAN et WAN à rendement élevé tendent à privilégier des tailles de trame maximales.

L'amélioration des performances est seulement possible quand de longs transferts de données sont exécutés. Les exemples d'applications incluent :

- Communication serveur dos à dos (par exemple, transactions NFS (Network File System)
- Mise en cluster de serveurs
- Sauvegardes de données à vitesse élevée
- Interconnexion ultra-rapide de superordinateur
- Transferts de données d'applications graphiques

Considération de performances du réseau

La performance du TCP sur les WAN (Internet) a été intensivement étudiée. Cette équation explique comment le débit TCP a une limitation supérieure qui est basée sur :

- La taille maximale du segment (MSS), qui est la longueur du MTU moins la longueur des en-têtes TCP/IP
- La durée aller-retour (RTT)
- La perte de paquets

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

Selon cette formule, le débit maximum de TCP qui est réalisable est directement proportionnel au MSS. Ceci signifie que, avec le RTT constant et la perte de paquets, vous pouvez doubler le débit TCP si vous la doublez la taille de paquet. De même, quand vous utilisez les trames étendues au lieu des trames 1518 octets, une augmentation sextuple de taille peut apporter une amélioration sextuple potentielle du débit TCP d'une connexion Ethernet.

Aperçu opérationnel

Le cahier des charges IEEE 802.3 standard définit une taille de trame Ethernet maximum de **1518**. Les trames encapsulées 802.1Q, d'une longueur comprise entre 1519 et 1522 octets, ont été ajoutées ultérieurement au cahier des charges 802.3 via l'avenant IEEE 802.3ac-1998. Elles sont parfois appelées **baby giants**.

Généralement, les paquets sont classifiés en tant que **trames géantes quand ils dépassent la longueur maximale Ethernet pour une connexion Ethernet spécifique.** Les paquets géants sont également connus en tant que **trames étendues**.

Le point principal de confusion au sujet des trames Jumbo est lié à la configuration : différentes interfaces prennent en charge différentes tailles maximales de paquets et, parfois, traitent de grand paquets de façon légèrement différente.

Gamme Catalyst 6500

Ce tableau récapitule les tailles du MTU qui sont actuellement prises en charge par différentes cartes sur la plate-forme Catalyst 6500 :

Carte de ligne	Taille de MTU
Par défaut	9216 octets
WS-X6248-RJ-45, WS-X6248A-RJ-45, WS-X6248-TEL, WS-X6248A-TEL, WS-X6348-RJ-45, WS-X6348-RJ45V, WS-X6348-RJ-21, et WX-X6348-RJ21V	8092 octets (limités par la puce PHY)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V), WS-X6148-45AF et WS-X6148-21AF	9 100 octets (à 100 Mbits/s) 9 216 octets (à 10 Mbits/s)
WS-X6516-GE-TX	8 092 octets (à 100 Mbits/s) 9 216 octets (à 10 ou 1 000 Mbits/s)
WS-X6148(V)-GE-TX, WS-X6148-GE-TX, WS-45AF,-GE-45AF, WS-X6548(V)-GE-TX, WS-X6548V-GE-TX et WS-X6548-GE-45AF	1500 bytes
OSM ATM (OC12c)	9180 octets
OSM CHOC3, CHOC12, CHOC48, et	9 216 octets

CT3	(OCx et DS3) 7 673 octets (T1/E1)
FlexWAN	7 673 octets (CT3 T1/DS0) 9 216 octets (OC3c POS) 7 673 octets (T1)
WS-X6148-GE-TX, et WS-X6548-GE-TX	Pas de prise en charge

Référez-vous à Configuration de la commutation Ethernet, Fast Ethernet, Gigabit Ethernet et Ethernet 10 Gigabits pour plus d'informations.

Prise en charge Jumbo de couche 2 et de couche 3 dans Catalyst 6500/6000 - Logiciel Cisco IOS

Il y a prise en charge Jumbo de la couche 2 et de la couche 3 avec PFC/MSFC1, PFC/MSFC2, et PFC2/MSFC2 sur tous les ports GE qui sont configurés comme interfaces physiques de la couche 2 et de la couche 3. Cette prise en charge existe indépendamment du fait que ces ports soient des ports de jonction ou de canalisation. Cette fonction est disponible dans le logiciel Cisco IOS 12.1.1E et versions ultérieures.

- Les tailles du MTU de tous les ports physiques Jumbo sont attachées ensemble. Un changement de l'un change la totalité. Ils gardent toujours la même taille de trame Jumbo une fois activés.
- Pendant la configuration, activez tous les ports dans le même VLAN que les trames Jumbo, ou n'en activez aucun.
- La taille MTU de l'interface virtuelle commutée (SVI) (interface VLAN) est définie séparément des MTU des ports physiques. Un changement de MTU des ports physiques ne change pas la taille du MTU SVI. En outre, un changement du MTU SVI n'affecte pas le MTU des ports physiques.
- La prise en charge des trames Jumbo de la couche 2 et de la couche 3 sur les interfaces FE a commencé dans le logiciel Cisco IOS Version 12.1(8a) EX01. La commande **mtu 1500 désactive les trames Jumbo sur l'interface FE et la commande mtu 9216 les active sur FE.** Référez-vous à ID de bogue Cisco CSCdv90450 (clients inscrits uniquement).
- Les trames Jumbo sur interfaces VLAN sont prises en charge uniquement sur :PFC/MSFC2 (logiciel Cisco IOS 12.1(7a)E et versions ultérieures)PFC2/MSFC2 (logiciel Cisco IOS version 12.1(8a)E4 et versions ultérieures)
- Il n'est pas recommandé d'utiliser des trames Jumbo avec PFC/MSFC1 pour des interfaces VLAN (SVIs) parce que MSFC1 peut ne pas savoir manipuler la fragmentation comme souhaité.
- Aucune fragmentation n'est supportée pour les paquets situés au sein du même réseau VLAN (Jumbo de couche 2).
- Les paquets devant être fragmentés sur des VLAN/sous-réseaux (Jumbo de couche 3) sont envoyées au logiciel pour fragmentation.

Présentation du support de trames Jumbo dans le logiciel Cisco IOS Catalyst 6500/6000

Une trame Jumbo est une trame plus volumineuse que la taille des trames Ethernet par défaut. Pour activer le support de la trame étendue, vous configurez la taille du MTU plus grande que par défaut sur un port ou interface VLAN et, avec le logiciel Cisco IOS version 12.1(13)E et plus tard,

vous configurez la taille du MTU globale de port de réseau local.

Contrôle de la taille du trafic traversier et du trafic routé dans le logiciel Cisco IOS

Carte de ligne	Entrée	Sortie
Ports 10-, 10/100-, 100-Mbps	Le contrôle de taille du MTU est fait. La prise en charge des trames Jumbo compare la taille du trafic entrant avec la valeur MTU de port LAN global en entrée (ports Ethernet 10-, 10/100- et 100-Mbps) et avec les ports LAN 10-GE possédant une taille MTU configurée (autre que la valeur par défaut). Le port supprime le trafic surdimensionné.	Le contrôle de taille du MTU n'est pas fait. Les ports qui sont configurés avec une taille du MTU autre que la valeur par défaut transmettent des trames qui contiennent des paquets de toute taille supérieure à 64 octets. Avec une valeur de taille MTU autre que la valeur par défaut, les ports LAN Ethernet 10-, 10/100-, and 100-Mbps ne vérifient pas les trames en sortie surdimensionnées.
Ports GE	Le contrôle de taille du MTU n'est pas fait. Les ports qui sont configurés avec une valeur de taille MTU autre que la valeur par défaut acceptent des trames contenant des paquets de toute taille supérieure à 64 octets et ne contrôlent pas les trames en entrée surdimensionnées.	Le contrôle de taille du MTU est fait. La prise en charge des trames Jumbo compare la taille du trafic en sortie à la valeur MTU de port LAN en sortie GE et aux ports LAN 10-GE pour lesquels une valeur MTU autre que la valeur par défaut a été configurée. Le port supprime le trafic surdimensionné.
Ports 10-GE	Le contrôle de taille du MTU est fait. Le port supprime le trafic surdimensionné.	Le contrôle de taille du MTU est fait. Le port supprime le trafic surdimensionné.
SVI	Le contrôle de taille du MTU n'est pas fait. Le SVI ne vérifie pas la taille de la trame du côté entrée.	Le contrôle de taille du MTU est fait. La taille du MTU est vérifiée du côté sortie du SVI.
	PFC	
Tout le	Pour le trafic qui doit être routé, la prise en charge des trames Jumbo sur PFC compare les tailles de	

trafic routé	trafic aux tailles MTU configurées, puis effectue une commutation de la couche 3 pour le trafic Jumbo entre les interfaces configurées avec des tailles MTU suffisamment élevées pour ce niveau de trafic. Entre les interfaces qui ne sont pas configurées avec des tailles MTU suffisamment élevées : • Si le bit DF (Don't Fragment) n'est pas défini, PFC envoie le trafic à MSFC afin de le fragmenter et de le router dans le logiciel. • Si le bit DF est défini, PFC supprime le trafic.

Recommandations Cisco

Si elles sont correctement mises en application, les trames Jumbo peuvent fournir une amélioration potentielle du débit TCP par rapport à une connexion Ethernet (débit six fois plus élevé), un temps système de fragmentation réduit (ainsi qu'un temps système plus faible sur les périphériques d'extrémité).

Vous devez vous assurer qu'il n'y a aucun périphérique au milieu incapable de manipuler la taille de MTU spécifique. Si ce périphérique fragmente et achemine les paquets, cela annule le processus entier. Ceci peut avoir comme conséquence un ajout de temps système sur ce périphérique à des fins de fragmentation et de réassemblage de paquets.

Dans ce cas, la découverte de chemins IP MTU aide les expéditeurs à rechercher la longueur minimale de paquet commun qui convient pour transmettre le trafic le long de chaque chemin. Vous pouvez également configurer des périphériques hôte prenant en charge les trames Jumbo avec une taille de MTU correspondant à la valeur minimale de toutes celles qui sont supportés sur le réseau.

Vous devez soigneusement contrôler chaque périphérique afin de vous assurer qu'il peut supporter la taille de MTU utilisée. Reportez-vous au tableau de tailles de MTU de cette section.

Le support de trames Jumbo peut être activé sur ces types d'interfaces :

- Interface de canal de port
- SVI
- Interface physique (couche 2/couche 3)

Vous pouvez activer les trames Jumbo sur le canal de port ou sur les interfaces physiques qui participent au canal de port. Il est très important de vérifier que le MTU est le même sur toutes les interfaces physiques. Sinon, une interface suspendue peut en résulter. Vous devez changer le MTU d'une interface de canal de port, car cela modifie le MTU de tous les ports membres.

Remarque : si le MTU d'un port membre ne peut pas être modifié en valeur nouvelle car le port membre est le port de blocage, le canal de port est suspendu.

Assurez-vous toujours que toutes les interfaces physiques d'un VLAN sont configurées pour les trames Jumbo avant de configurer le support de trames Jumbo sur un SVI. Le MTU d'un paquet n'est pas vérifié sur le côté entrée d'un SVI. En revanche, il est vérifié sur le côté sortie. Si le MTU du paquet est plus grand que le MTU SVI de sortie, le paquet est fragmenté par le logiciel (si le bit DF n'est pas défini), ce qui entraîne des performances médiocres. La fragmentation de logiciel se produit seulement pour la commutation de couche 3. Quand un paquet est expédié à un port de

couche 3 ou à un SVI portant une valeur MTU plus faible, une fragmentation logicielle a lieu.

Le MTU d'un SVI doit toujours être plus petit que le plus petit MTU de tous les ports de commutation du VLAN.

Gamme Catalyst 4500

Les trames Jumbo sont supportées principalement sur les ports non bloquants des cartes de ligne Catalyst 4500. Ces ports non bloquants GE ont des connexions directes à la matrice de commutation de Supervisor Engine et supportent les trames Jumbo :

- Moteurs Supervisor EngineWS-X4515, WS-X4516 - Deux ports de la liaison montante GBIC sur Supervisor Engine IV ou VWS-X4516-10GE - Deux liaisons montantes 10-GE et les quatre liaisons montantes 1-GE SFP (Small Form Factor)WS-X4013+ - Deux liaisons montantes 1-GEWS-X4013+10GE - Deux liaisons montantes 10-GE et les quatre liaisons montantes 1-GE SFPWS-X4013+TS - 20 ports 1-GE
- Cartes de ligneWS-X4306-GB - Module GE à six ports 1000BASE-X (GBIC)WS-X4506-GB-T - 10/100/1000-Mbps six ports et SFP six portsWS-X4302-GB - Module GE 1000BASE-X (GBIC) à deux portsLes deux premiers ports GBIC d'un serveur 18 ports commutant le module GE (WS-X4418-GB) et les ports GBIC du module WS-X4232-GB-RJ
- Commutateurs de configuration fixeWS-C4948 - Chacun des 48 ports 1-GEWS-C4948-10GE - Chacun des 48 ports 1-GE et deux ports 10-GE

Vous pouvez utiliser ces ports GE non bloquants pour la prise en charge de trames Jumbo 9-KB ou la suppression de diffusion de matériel (Supervisor Engine IV uniquement). Toutes les autres cartes de ligne supportent les trames Baby Giant. Vous pouvez utiliser des trames Baby Giant pour la transition du MPLS ou pour le passthrough Q dans Q avec une charge utile maximum de 1552 octets.

Remarque : la taille de trame augmente avec les balises ISL/802.1Q.

Les trames Baby Giant et les trames Jumbo sont transparentes pour les autres fonctions Cisco IOS avec Supervisor Engine IV et V.

Fonctions de sécurité du logiciel Cisco IOS

Fonctions de sécurité de base

Auparavant, la sécurité était souvent négligée dans les conceptions campus. Mais la sécurité est désormais un composant essentiel de tout réseau d'entreprise. Normalement, le client a déjà établi une stratégie de sécurisation pour définir les outils et les technologies Cisco applicables.

Protection par mot de passe de base

La plupart des équipement fonctionnant avec le logiciel Cisco IOS sont configurés avec deux niveaux de mots de passe. Le premier niveau est pour l'accès de Telnet au périphérique, qui est également connu en tant qu'accès vty. Une fois l'accès vty autorisé, vous devez accéder au mode d'activation ou au mode EXEC privilégié.

Sécurisez le mode d'activation du commutateur

Le mot de passe d'activation permet à un utilisateur de bénéficier d'un accès complet à un périphérique. Fournissez le mot de passe d'activation aux personnes de confiance uniquement.

```
Switch(config)#enable secret password
```

Soyez sûr que le mot de passe se conforme à ces règles :

- Le mot de passe doit contenir entre un et 25 caractères alphanumériques (majuscules et minuscules).
- Le mot de passe ne doit pas avoir un numéro comme premier caractère.
- Vous pouvez utiliser des espaces, mais ils sont ignorés. Les espaces intermédiaires et finaux sont reconnus.
- Le contrôle de mot de passe distingue les majuscules et minuscules. Par exemple, le mot de passe Secret est différent du mot de passe secret.

Remarque : la commande **enable secret** utilise une fonction de hachage MD5 (Unidirectionnel Message Digest 5). Si vous émettez la commande **show running-config , vous pouvez voir ce mot de passe crypté.** L'utilisation de la commande **enable password est un autre moyen de définir le mot de passe d'activation.** Mais l'algorithme de chiffrement qui est utilisé avec la commande **enable password est faible et peut être facilement inversé pour obtenir le mot de passe.** Par conséquent, n'utilisez pas la commande **enable password .** Utilisez la commande **enable secret qui offre une meilleure sécurité.** Référez-vous à Faits sur le cryptage de mot de passe de Cisco IOS pour plus d'informations.

Sécurisez l'accès Telnet/VTY au commutateur

Par défaut, le logiciel Cisco IOS supporte cinq sessions Telnet actives. Ces sessions portent le nom de vty 0 à 4. Vous pouvez activer ces lignes pour l'accès. Mais pour activer la connexion, vous avez besoin également du mot de passe défini pour ces lignes.

```
Switch(config)#line vty 0 4
Switch(config-line)#login
Switch(config-line)#password password
```

La commande **login configure ces lignes pour l'accès Telnet.** La commande **password configure un mot de passe.** Soyez sûr que le mot de passe se conforme à ces règles :

- Le premier caractère ne peut pas être un numéro.
- La chaîne peut contenir tous les caractères alphanumériques, jusqu'à 80 caractères. Les caractères incluent les espaces.
- Vous ne pouvez pas spécifier le mot de passe au format chiffre-espace-caractère. L'espace figurant après le numéro entraîne des problèmes. Par exemple, hello 21 est un mot de passe valide, tandis que 21 hello ne l'est pas.
- Le contrôle de mot de passe distingue les majuscules et minuscules. Par exemple, le mot de passe Secret est différent du mot de passe secret.

Remarque : avec cette configuration de ligne vty, le commutateur stocke le mot de passe en texte clair. Si quelqu'un émet la commande **show running-config , ce mot de passe est visible.** Afin d'éviter cette situation, utilisez la commande **service password-encryption .** Cette commande permet de crypter légèrement le mot de passe. En effet, la commande crypte seulement le mot de passe de la ligne vty et le mot de passe d'activation configuré à l'aide de la commande **enable**

password . Le mot de passe d'activation configuré à l'aide de la commande **enable secret utilise un cryptage plus fort.** La méthode recommandée est la configuration à l'aide de la commande **enable secret .**

Remarque : afin d'avoir plus de flexibilité dans la gestion de la sécurité, assurez-vous que tous les périphériques du logiciel Cisco IOS implémentent le modèle de sécurité AAA (Authentication, Authorization, and Accounting). AAA peut utiliser des bases de données locales, RADIUS et TACACS+. Pour plus d'informations, reportez-vous à la section Configuration de l'authentification TACACS+.

Services de sécurité AAA

Aperçu opérationnel AAA

Les contrôles d'accès contrôlent les personnes autorisées à accéder au commutateur et les services que les utilisateurs peuvent utiliser. Les services de sécurité réseau AAA fournissent l'infrastructure permettant de configurer le contrôle d'accès sur votre commutateur.

Cette section détaille les différents aspects liés à AAA :

- Authentification - Ce processus valide l'identité réclamée d'un utilisateur final ou d'un périphérique. Tout d'abord, les différentes méthodes qui peuvent être utilisées pour authentifier l'utilisateur sont spécifiées. Ces méthodes définissent le type d'authentification à exécuter (par exemple, TACACS+ ou RADIUS). L'ordre dans lequel essayer ces méthodes d'authentification est également défini. Les méthodes sont alors appliquées aux interfaces appropriées, ce qui active l'authentification.
- Autorisation - Ce processus accorde des droits d'accès à un utilisateur, à des groupes d'utilisateurs, à un système ou à un processus. Le processus AAA peut exécuter l'autorisation en une fois ou l'autorisation tâche par tâche. Le processus définit les attributs (sur le serveur AAA) sur ce que l'utilisateur a l'autorisation d'exécuter. Toutes les fois que des tentatives utilisateur de démarrage d'un service, le commutateur interroge le serveur AAA et demande l'autorisation pour l'utilisateur. Si le serveur AAA approuve, l'utilisateur est autorisé. Si le serveur AAA n'approuve pas, l'utilisateur n'a pas l'autorisation d'exécuter ce service. Vous pouvez utiliser ce processus afin de spécifier que certains utilisateurs ne peuvent exécuter que certaines commandes.
- Gestion des comptes - Ce processus permet de suivre les services auxquels les utilisateurs accèdent et la quantité de ressources réseau que les utilisateurs consomment. Quand la gestion des comptes est activée, le commutateur enregistre l'activité des utilisateurs sur le serveur AAA sous forme d'enregistrements statistiques. Des exemples de l'activité d'utilisateur enregistrée incluent la durée de session, ou encore l'heure de début et de fin. Ensuite, l'analyse de cette activité peut avoir lieu dans un but de gestion ou de facturation.

Bien qu'AAA représente la principale méthode de contrôle d'accès (et la méthode recommandée), le logiciel Cisco IOS fournit des fonctionnalités supplémentaires pour le contrôle d'accès simple qui sont hors de portée d'AAA. Ces fonctionnalités supplémentaires incluent :

- Authentification de nom d'utilisateur local
- Authentification de mot de passe de ligne
- Activation d'authentification de mot de passe

Mais ces caractéristiques ne fournissent pas le même degré de contrôle d'accès que celui offert

par AAA.

Afin de mieux comprendre AAA, référez-vous à ces documents :

- Authentification, autorisation et comptabilité (AAA)
- Configuration de la fonction AAA de base sur un serveur d'accès
- Comparaison entre TACACS+ et RADIUS

Ces documents ne mentionnent pas nécessairement des commutateurs. Mais les concepts d'AAA que les documents décrivent s'appliquent aux commutateurs.

TACACS+

Objectif

Par défaut, les mots de passe en mode privilégié et non privilégié sont globaux. Ces mots de passe s'appliquent à chaque utilisateur qui accède au commutateur ou au routeur, à partir du port de console ou via une session Telnet sur le réseau. La mise en place de ces mots de passe sur des équipements réseau est longue et non centralisée. En outre, vous pouvez avoir des difficultés avec la mise en place des restrictions d'accès liées à l'utilisation des listes de contrôle d'accès (ACL) qui peuvent être sources d'erreurs de configuration. Afin de résoudre ces problèmes, adoptez une approche centralisée quand vous configurez des noms d'utilisateurs, des mots de passe et des politiques d'accès sur un serveur central. Ce serveur peut être le serveur Cisco ACS (Secure Access Control Server) ou n'importe quel serveur tiers. Les périphériques sont configurés pour utiliser ces bases de données centralisées pour des fonctions AAA. Dans ce cas, les périphériques sont des commutateurs du logiciel Cisco IOS. Le protocole qui est utilisé entre les périphériques et le serveur central peut être :

- TACACS+
- RADIUS
- Kerberos

TACACS+ est un déploiement commun sur les réseaux Cisco et constitue l'objet de cette section. TACACS+ offre les fonctions suivantes :

- Authentification - Le processus qui identifie et vérifie un utilisateur. Plusieurs méthodes peuvent être utilisées afin d'authentifier un utilisateur. Mais la méthode la plus commune inclut une combinaison de nom d'utilisateur et de mot de passe.
- Autorisation - Quand l'utilisateur tente d'exécuter une commande, le commutateur peut contrôler avec le serveur TACACS+ si l'utilisateur a l'autorisation d'utiliser cette commande spécifique.
- Gestion des comptes - Ce processus enregistre ce qu'un utilisateur fait ou a fait sur le périphérique.

Référez-vous à Comparaison entre TACACS+ et RADIUS pour obtenir la comparaison de TACACS+ et de RADIUS.

Aperçu opérationnel

Le protocole TACACS+ achemine les noms d'utilisateur et les mots de passe vers le serveur centralisé. Les informations sont cryptées sur le réseau à l'aide d'un hachage MD5 à sens unique. Référez-vous à RFC 1321 pour plus d'informations. TACACS+ utilise le port TCP 49 comme

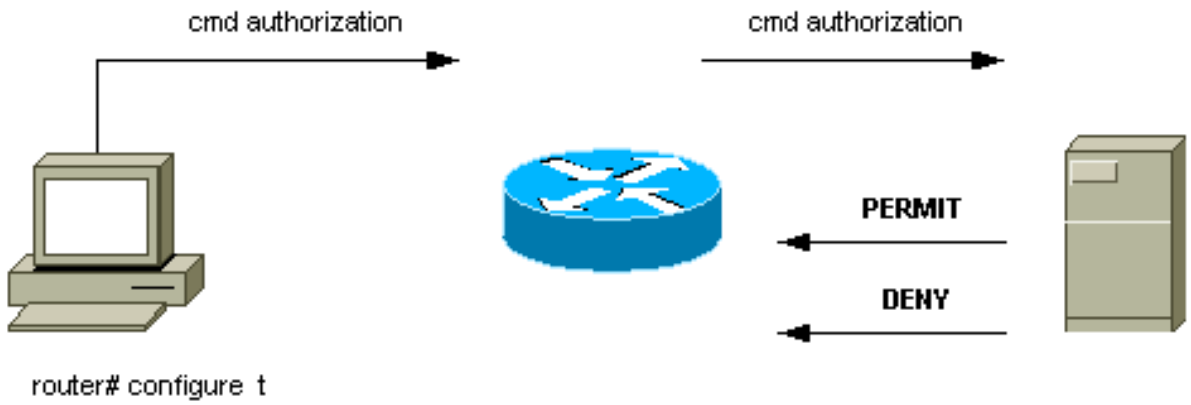
protocole de transport, ce qui offre les avantages suivants par rapport à UDP :

Remarque : RADIUS utilise le protocole UDP.

- Transport orienté connexion
- Séparation de l'accusé de réception indiquant qu'une demande a été reçue (accusé de réception TCP [ACK]), indépendamment du chargement du mécanisme d'authentification
- Indication immédiate d'une panne serveur (paquets réinitialisés [RST])

Pendant une session, si un contrôle d'autorisation supplémentaire est nécessaire, le commutateur vérifie avec TACACS+ pour déterminer si on accorde à l'utilisateur l'autorisation d'utiliser une commande particulière. Cette étape fournit un plus grand contrôle sur les commandes qui peuvent être exécutées sur le commutateur et fournit le découplage du mécanisme d'authentification. Avec l'utilisation de la gestion des commandes, vous pouvez auditer les commandes qu'un utilisateur a émises pendant qu'il était connecté à un périphérique réseau spécifique.

Ce diagramme montre le processus d'autorisation impliqué :



Quand un utilisateur s'authentifie à un périphérique réseau avec TACACS+ dans une tentative de procédure de connexion ASCII simple, ce processus se produit généralement :

- Quand la connexion est établie, le commutateur contacte le démon TACACS+ afin d'obtenir une invite de nom d'utilisateur. Ensuite, le commutateur affiche l'invite de l'utilisateur. L'utilisateur saisit un nom d'utilisateur, et le commutateur contacte le daemon TACACS+ afin d'obtenir une invite de mot de passe. Le commutateur affiche l'invite de mot de passe à l'utilisateur, qui saisit alors un mot de passe qui est également envoyé au daemon TACACS+.
- Le périphérique réseau reçoit par la suite une de ces réponses du daemon TACACS+ :`ACCEPT — L'utilisateur est authentifié et le service peut commencer.` Si le périphérique réseau est configuré pour exiger l'autorisation, celle-ci commence à ce moment.`REJECT — L'utilisateur n'a pas réussi à s'authentifier.` L'utilisateur se voit refuser l'accès ou doit réessayer la séquence d'ouverture de session. Le résultat dépend du démon TACACS+.`ERROR — Une erreur s'est produite à un moment donné pendant l'authentification.` Cette erreur peut se produire au niveau du daemon ou dans la connexion réseau entre le daemon et le commutateur. Si une réponse `ERROR est reçue, le périphérique réseau essaye typiquement d'employer une méthode alternative afin d'authentifier l'utilisateur.CONTINUE - L'utilisateur est incité à fournir des informations d'authentification supplémentaires.`
- Les utilisateurs doivent d'abord avec succès compléter l'authentification TACACS+ avant de

passer à l'autorisation TACACS+.
- Si une autorisation TACACS+ est requise, le démon TACACS+ est de nouveau contacté. Le démon TACACS+ renvoie une réponse `ACCEPT ou REJECT d'autorisation.` Si une réponse `ACCEPT est retournée, la réponse contient des données sous forme d'attributs qui sont utilisés pour diriger la session EXEC ou la session NETWORK pour cet utilisateur.` Cela détermine les commandes auxquelles l'utilisateur peut accéder.

Étapes de base de la configuration AAA

La configuration AAA est relativement simple une fois que vous avez bien compris le processus de base. Afin de configurer la sécurité sur un routeur Cisco ou un serveur d'accès avec l'utilisation d'AAA, exécutez ces étapes :

1. Afin d'activer AAA, émettez la commande de configuration globale **aaa new-model .**
   `Switch(config)#aaa new-model`

   Conseil : enregistrez votre configuration avant de configurer vos commandes AAA. Sauvegardez la configuration de nouveau une fois que vous avez terminé toutes vos configurations AAA et que vous êtes satisfait du fonctionnement de la configuration. Ensuite, vous pouvez recharger le commutateur afin de récupérer des verrouillages imprévus (avant la sauvegarde de la configuration), s'il y a lieu.
2. Si vous décidez d'utiliser un serveur de sécurité distinct, configurez les paramètres du protocole de sécurité (RADIUS, TACACS+, ou Kerberos, par exemple).
3. Utilisez la commande **aaa authentication afin de définir les listes de méthodes pour l'authentification.**
4. Utilisez la commande **login authentication** afin d'appliquer les listes de méthodes à une interface ou à une ligne particulière.
5. Emettez la commande facultative **aaa authorization afin de configurer l'autorisation.**
6. Émettez la commande facultative **aaa accounting afin de configurer la gestion des comptes.**
7. Configurez le serveur externe AAA pour traiter les demandes d'authentification et les requêtes d'autorisation du commutateur.**Remarque :** reportez-vous à la documentation de votre serveur AAA pour plus d'informations.

Configuration de l'authentification TACACS+

Exécutez ces étapes afin de configurer l'authentification TACACS+ :

1. Émettez la commande **aaa new-model en mode de configuration globale afin d'activer AAA sur le commutateur.**
2. Définissez le serveur TACACS+ et la clé associée.Cette clé est utilisée pour crypter le trafic entre le serveur TACACS+ et le commutateur. Dans la commande **tacacs-server host 1.1.1.1 key mysecretkey , le serveur TACACS+ se trouve à l'adresse IP 1.1.1.1, et la clé de chiffrement est mysecretkey.** Afin de vérifier que le commutateur peut atteindre le serveur TACACS+, exécutez une commande Ping ICMP (Internet Control Message Protocol) à partir du commutateur.
3. Définissez une liste de méthodes.Une liste de méthodes définit l'ordre des mécanismes d'authentification à essayer pour différents services. Les divers services peuvent être, par exemple :ActiverLogin (pour l'accès vty/Telnet)**Remarque :** Reportez-vous à la section

Fonctions de sécurité de base de ce document pour plus d'informations sur l'accès vty/Telnet.ConsoleCet exemple traite de la commande **login uniquement.** Vous devez appliquer la liste de méthodes aux interfaces/lignes :

```
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line
Switch(config)#line vty 0 4
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

Dans cette configuration, la commande **aaa authentication login utilise le nom de liste préparé METHOD-LIST-LOGIN et la méthode tacacs+ avant d'utiliser la méthode ligne.** Les utilisateurs sont authentifiés avec l'utilisation du serveur TACACS+ en tant que première méthode. Si le serveur TACACS+ ne répond pas ou envoie un message d'erreur, le mot de passe qui est configuré sur la ligne est utilisé en tant que deuxième méthode. Mais si le serveur TACACS+ rejette l'utilisateur et répond avec un message REJECT, AAA considère que la transaction a abouti et n'utilise pas la deuxième méthode.**Remarque :** la configuration n'est pas terminée tant que vous n'avez pas appliqué la liste (MÉTHODE-LIST-LOGIN) à la ligne vty. Émettez la commande **login authentication METHOD-LIST-LOGIN en mode de configuration de ligne, comme l'illustre l'exemple.Remarque :** l'exemple crée une porte dérobée lorsque le serveur TACACS+ n'est pas disponible. Les administrateurs de sécurité peuvent ou ne peuvent pas accepter la mise en place d'une porte dérobée. Vérifiez que la décision de mettre en application ces portes dérobées est conforme aux stratégies de sécurité du site.

Configuration de l'authentification RADIUS

La configuration RADIUS est presque identique à la configuration TACACS+. Substituez simplement le mot RADIUS à TACACS dans la configuration. C'est un exemple de configuration de RADIUS pour l'accès au port COM :

```
Switch(config)#aaa new-model
Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line
Switch(config)#line con 0
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

Bannières de connexion

Créez des bannières qui indiquent les actions prises pour un accès non autorisé. N'indiquez pas le nom du site ou les informations réseau aux utilisateurs non autorisés. Ces messages fournissent un recours au cas où un périphérique serait compromis et l'auteur attrapé. Émettez cette commande pour créer des bannières d'ouverture de session :

```
Switch(config)#banner motd ^C
*** Unauthorized Access Prohibited ***
^C
```

Sécurité physique

Assurez-vous qu'une autorisation appropriée est requise pour l'accès physique aux périphériques.

Maintenez le matériel dans un espace (verrouillé) commandé. Pour être sûr que le réseau reste opérationnel et n'est pas affecté par l'influence malveillante de facteurs environnementaux, vérifiez que tout l'équipement possède :

- Une alimentation électrique non interruptible appropriée (UPS), avec des sources redondantes si possible
- Contrôle de température (climatisation)

Rappelez-vous que, si une personne ayant une intention malveillante commet une effraction d'accès physique, une interruption par récupération de mot de passe ou autre moyen est tout à fait possible.

Configuration de la gestion

Diagrammes du réseau

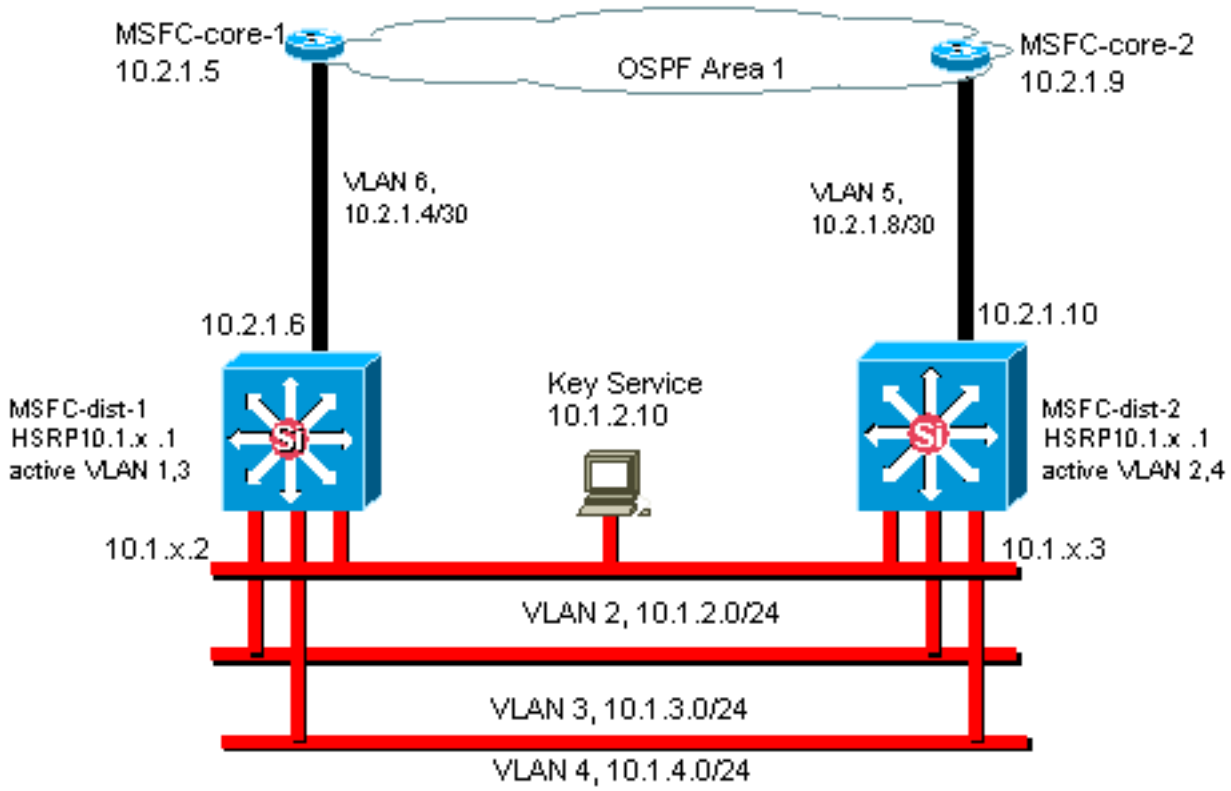
Objectif

Des diagrammes de réseau clairs sont une partie fondamentale du fonctionnement du réseau. Ils deviennent critiques pendant le dépannage et sont le véhicule simple le plus important pour la transmission d'informations une fois remontés aux constructeurs et aux associés pendant une panne. Ne sous-estimez pas la préparation, la promptitude, et l'accessibilité que les diagrammes de réseau fournissent.

Recommandation

Ces trois types de diagrammes sont nécessaires :

- **Diagramme global - Même pour les plus grands réseaux, un diagramme qui montre la connectivité physique ou logique de bout en bout est important.** Souvent, les entreprises qui ont mis en application une conception hiérarchique documentent chaque couche séparément. Lorsque vous effectuez un dépannage, une bonne connaissance des liaisons entre les domaines est essentielle.
- **Diagramme physique — Ce diagramme illustre le matériel et le câblage de tous les commutateurs et routeurs.** Assurez-vous que le diagramme fait apparaître chacun des aspects suivants :AgrégationsLiensVitessesGroupes de canauxNuméros de portEmplacementsTypes de châssisle logiciel Cisco IOSDomaines VTPPont racinePriorité de pont racine de secoursAdresse MAC :Ports bloqués par VLANPour une meilleure clarté, décrivez les périphériques internes tels que le routeur MSFC Catalyst 6500/6000 MSFC connecté via une jonction.
- **Diagramme logique - Ce diagramme montre seulement la fonctionnalité de la couche 3, ce qui signifie qu'il montre les routeurs comme des objets et les VLAN comme des segments Ethernet.** Assurez-vous que le diagramme fait apparaître les aspects suivants :Adresses IP Sous-réseauxAdressage secondaireHSRP actif et standbyCouches de distribution d'accèsInformations de routage



Interface de gestion de la commutation et VLAN natif

Objectif

Cette section décrit l'importance et les problèmes potentiels liés à l'utilisation du VLAN par défaut (VLAN 1). Cette section couvre également les problèmes potentiels qui peuvent survenir quand vous exécutez le trafic d'administration sur le commutateur du même réseau VLAN que le trafic utilisateur des commutateurs de la gamme 6500/6000.

Les processeurs des moteurs Supervisor Engine et les MSFC pour la gamme Catalyst 6500/6000 utilisent le réseau VLAN 1 pour un certain nombre de protocoles de contrôle et de gestion. Exemples :

- Protocoles de contrôle de processeurs :BPDU STPVTPDTPCDP
- Protocoles de gestion :SNMPTelnetSecure Shell Protocol (SSH)Syslog

Quand le VLAN est utilisé de cette façon, il est désigné sous le nom de VLAN natif. La configuration du commutateur par défaut définit le VLAN 1 comme VLAN natif par défaut sur les ports de jonction Catalyst. Vous pouvez laisser VLAN 1 comme VLAN natif. Mais souvenez-vous que tous les commutateurs qui exécutent le logiciel Cisco IOS sur votre réseau définissent toutes les interfaces configurées en tant que ports de commutation de couche 2 pour l'accès aux ports du réseau VLAN 1 par défaut. Très probablement, un commutateur du réseau utilise VLAN 1 comme VLAN destiné au trafic utilisateurs.

Le problème principal avec l'utilisation du VLAN 1 est qu'en général, le NMP de Supervisor Engine ne doit pas être interrompu par le trafic de diffusion et multicast généré par les stations d'extrémité. Les applications multicast en particulier tendent à envoyer beaucoup de données entre les serveurs et les clients. Supervisor Engine n'a pas besoin de voir ces données. Si les ressources ou les mémoires tampon du Supervisor Engine sont occupées lorsque le moteur

écoute un trafic inutile, Supervisor Engine peut ne pas voir les paquets de gestion qui entraînent une boucle Spanning Tree ou une panne d'EtherChannel (dans le pire des cas).

La commande **show interfaces *interface_type slot/port counters*** et la commande **show ip traffic peuvent vous fournir certaines indications liées à :**

- La proportion de diffusion par rapport au trafic unicast
- La proportion de trafic IP et non IP (qui ne se voit généralement pas sur les VLAN de gestion)

VLAN 1 balise et traite la plupart du trafic de contrôle. VLAN 1 est activé sur toutes les liaisons agrégées par défaut Avec de plus grands réseaux campus, vous devez faire attention au diamètre du domaine STP du VLAN 1. L'instabilité dans une part du réseau peut affecter le VLAN 1 et peut influencer la stabilité du plan de contrôle et la stabilité STP de tous les autres VLAN. Vous pouvez limiter la transmission sur le VLAN 1 des données utilisateur et du fonctionnement STP d'une interface. Ne configurez pas le VLAN sur l'interface de jonction.

Cette configuration n'arrête pas la transmission des paquets de contrôle de commutateur à commutateur au sein du réseau VLAN 1, comme avec un analyseur de réseau. Cependant, aucune donnée n'est expédiée, et STP n'est pas exécuté sur cette liaison. Par conséquent, cette technique peut être utilisée pour diviser VLAN 1 en plus petits domaines de panne.

Remarque : Vous ne pouvez pas effacer VLAN 1 des agrégations vers les Catalyst 2900XL/3500XL.

Même si vous faites attention à limiter les VLAN utilisateur aux domaines relativement petits et également aux bornes de la couche 3, certains clients tentent malgré tout de traiter différemment le VLAN de gestion. Ces clients essayent de couvrir le réseau entier à l'aide d'un seul sous-réseau de gestion. Il n'y a aucune raison technique pour qu'une application NMS centrale soit adjacente de la couche 2 aux périphériques qu'elle contrôle, et il ne s'agit pas d'un argument de sécurité acceptable. Limitez le diamètre des VLAN de gestion à la même structure de domaines routés que celle des VLAN utilisateur. Envisagez une gestion hors bande et/ou un support SSH comme moyen d'augmenter la sécurité de l'administration réseau.

Autres options

Il faut prendre en compte des considérations de conception pour ces recommandations Cisco dans certaines topologies. Par exemple, une conception Cisco multicouche désirable et commune est une qui évite l'utilisation d'un spanning tree actif. De cette façon, la conception nécessite de limiter chaque sous-réseau/VLAN IP à un commutateur de la couche d'accès simple (ou cluster de commutateurs). Dans ces conceptions, aucune liaison de jonction ne peut être configurée par rapport à la couche d'accès.

Est-ce qu'il convient de créer un VLAN de gestion distinct en activant la jonction plutôt que de l'acheminer entre la couche d'accès (L2) et la couche de distribution (L3) ? Il n'y a aucune réponse facile à cette question. Voici deux options pour l'étude de conception avec votre ingénieur Cisco :

- **Option 1 — Agrégez deux ou trois VLAN uniques de la couche de distribution vers chaque commutateur de la couche d'accès.** Cette configuration permet d'avoir un VLAN de données, un VLAN voix et un VLAN de gestion, par exemple, en gardant l'avantage d'un STP inactif. Une étape de configuration supplémentaire est nécessaire pour supprimer VLAN 1 des jonctions réseau. Dans cette solution, il y a également des points de conception à considérer afin d'éviter la formation de trous noirs temporaires dans le trafic routé pendant la reprise après panne. Utilisez STP PortFast pour les jonctions réseau (à l'avenir) ou la synchronisation

VLAN avec acheminement STP.

- **Option 2- Un VLAN simple pour les données et la gestion peut être acceptable.** Si vous voulez séparer l'interface sc0 des données utilisateur, un nouveau commutateur rend ce scénario moins problématique que par le passé. Ce nouveau matériel offre :Des CPU plus puissantes et des contrôles de plan de contrôleUne conception avec des domaines de diffusion relativement petits comme préconisé par la conception multicoucheAfin de prendre une décision finale, examinez le profil du trafic de diffusion du VLAN et discutez des capacités du commutateur avec votre ingénieur Cisco. Si le VLAN de gestion contient tous les utilisateurs de ce commutateur de la couche d'accès, utilisez des filtres IP afin de sécuriser le commutateur, conformément aux indications de la section Fonctions de sécurité du logiciel Cisco IOS .

Recommandation Cisco liée à l'interface de gestion et au VLAN natif

Interface de gestion

Le logiciel système Cisco IOS vous permet de configurer des interfaces en tant qu'interfaces de la couche 3 ou que ports de commutation de la couche 2 au sein d'un VLAN. Quand vous utilisez la commande **switchport dans le logiciel Cisco IOS, tous les ports de commutation sont par défaut des ports d'accès du VLAN 1.** Ainsi, à moins que vous n'adoptiez une autre configuration, les données utilisateur peuvent également exister par défaut sur le VLAN 1.

Faites du VLAN de gestion un VLAN autre que VLAN 1. Conservez toutes les données utilisateur hors du VLAN de gestion. Au lieu de cela, configurez un une interface loopback0 comme interface de gestion sur chacun des commutateurs.

Remarque : si vous utilisez le protocole OSPF, il s'agit également de l'ID de routeur OSPF.

Assurez-vous que l'interface de bouclage a un masque de sous-réseau de 32 bits, et configurez l'interface de bouclage comme interface de la couche 3 sur le commutateur. Voici un exemple :

```
Switch(config)#interface loopback 0
Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end
Switch#
```

VLAN natif

Configurez le VLAN natif pour qu'il soit un VLAN factice évident qui n'est jamais activé sur le routeur. Cisco recommandait auparavant l'utilisation du VLAN 999, mais ce choix est purement arbitraire.

Émettez ces commandes d'interface afin d'établir un VLAN en tant que VLAN natif (valeur par défaut) pour l'agrégation 802.1Q sur un port particulier :

```
Switch(config)#interface type slot/port
Switch(config-if)#switchport trunk native vlan 999
```

Pour plus d'informations sur les recommandations de configuration de jonction, reportez-vous à la section Dynamic Trunking Protocol de ce document.

Gestion extrabande

Objectif

Vous pouvez rendre l'administration réseau hautement disponible si vous construisez une infrastructure de gestion distincte autour du réseau de production. Cette configuration permet à des périphériques d'être accessibles à distance, en dépit du trafic ou des événements de plan de contrôle. Ces deux approches sont typiques :

- Gestion hors bande avec LAN exclusif
- Gestion hors bande avec des serveurs de terminaux

Aperçu opérationnel

Chaque routeur et commutateur du réseau peut être équipé d'une interface de gestion Ethernet hors bande sur un VLAN de gestion. Vous configurez dans ce cas un port Ethernet sur chaque périphérique du VLAN de gestion et vous le câblez hors du réseau de production à un réseau de gestion commuté séparé.

Remarque : les commutateurs Catalyst 4500/4000 disposent d'une interface me1 spéciale sur le Supervisor Engine qui doit être utilisée uniquement pour la gestion hors bande et non comme port de commutateur.

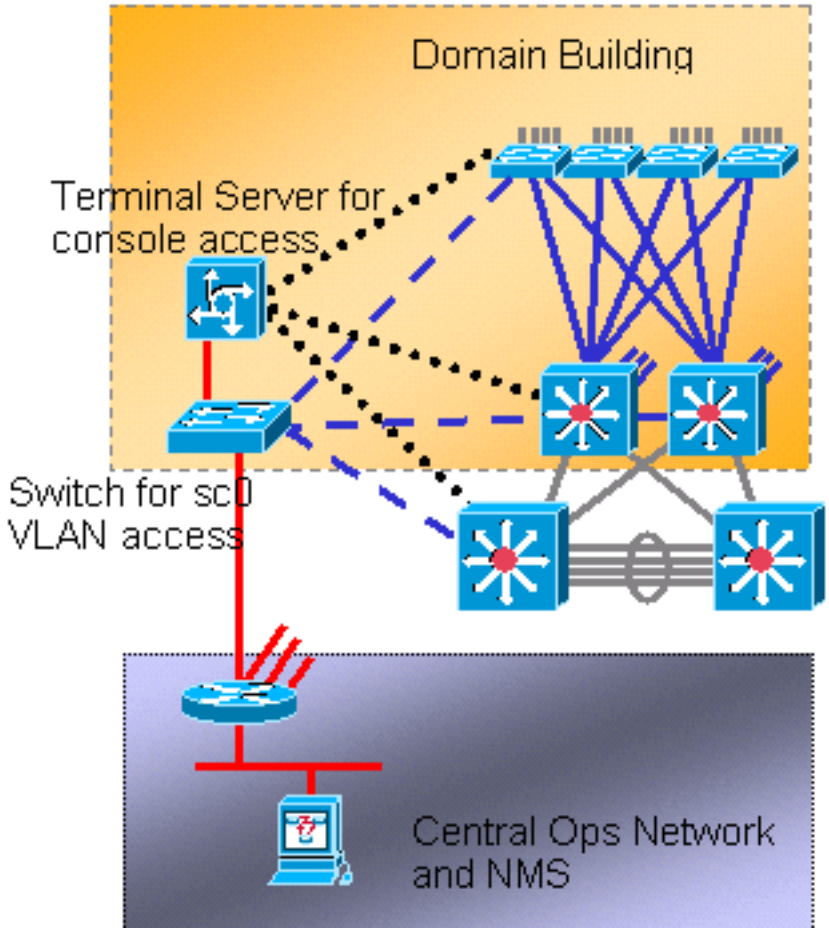
En outre, la connectivité du serveur de terminal peut être réalisée par configuration d'un routeur Cisco 2600 ou 3600 avec des câbles RJ-45-à-série pour accéder au port de console de chaque routeur et commutateur dans l'installation. L'utilisation d'un serveur de terminal évite également le besoin de configuration des scénarios de secours, tels que des modems sur les ports auxiliaires pour chaque périphérique. Vous pouvez configurer un modem simple sur le port auxiliaire du serveur de terminal. Cette configuration offre un service à accès commuté aux autres périphériques pendant une panne de connectivité réseau. Référez-vous à Connexion d'un modem au port de la console sur des commutateurs Catalyst pour plus d'informations.

Recommandation

Avec cet agencement, deux chemins hors bande à chaque commutateur et routeur sont possibles, outre de nombreux chemins intrabande. Cet agencement active la gestion de réseaux hautement disponibles. Les avantages sont les suivants :

- Cet agencement sépare le trafic de gestion du trafic de données utilisateurs.
- L'adresse IP de gestion se trouve dans des sous-réseaux, VLAN et commutateurs différents, pour des questions de sécurité.
- Il y a une garantie plus élevée de remise des données de gestion pendant les pannes réseau.
- Il n'y a aucun spanning-tree actif dans le VLAN de gestion. Ici, la redondance n'est pas critique.

Ce diagramme montre la gestion hors bande :



Journalisation système

Objectif

Les messages Syslog sont spécifiques à Cisco et peuvent fournir des informations plus sensibles et plus précises que les informations SNMP standard. Par exemple, les plates-formes de gestion telles que Cisco RME (Resource Manager Essentials) ou NATKit (Network Analysis Toolkit) font une utilisation puissante de l'information de Syslog afin de rassembler l'inventaire et les modifications de configuration.

Recommandation Cisco pour la configuration de Syslog

La journalisation système est une pratique opérationnelle courante et acceptée. Un Syslog UNIX peut saisir et analyser les informations/événements sur le routeur telles comme :

- État de l'interface
- Alertes de Sécurité
- Conditions d'environnement
- Monopolisation de processus CPU
- Autres événements

Le logiciel Cisco IOS peut effectuer une journalisation UNIX sur un serveur Syslog UNIX. Le format Cisco UNIX Syslog est compatible avec la distribution BSD (Berkeley Standard Distribution) 4.3 UNIX. Utilisez ces paramètres de journalisation du logiciel Cisco IOS :

- **no logging console - Par défaut, tous les messages système sont envoyés à la console système.** La journalisation console est une tâche prioritaire dans le logiciel Cisco IOS. Cette

fonction a été principalement conçue pour fournir des messages d'erreur à l'opérateur système avant une panne système. Désactivez la journalisation pour toutes les configurations de périphériques afin d'éviter une situation dans laquelle le routeur/commutateur peut s'arrêter tandis que le périphérique attend une réponse d'un terminal. Mais les messages sur la console peuvent être utiles pendant l'isolement d'incident. Dans ces cas, activez la journalisation console. Émettez la commande **logging console level afin d'obtenir le niveau désiré de journalisation.** Les niveaux de journalisation vont de 0 à 7.

- **no logging monitor - Cette commande désactive la journalisation pour les lignes du terminal autres que la console système.** La journalisation peut être requise (avec l'utilisation de la commande **logging monitor debugging ou d'une autre commande).** Dans ce cas, activez la journalisation au niveau requis pour l'activité. Voir l'élément **no logging console dans cette liste pour plus d'informations sur les niveaux de journalisation.**
- **logging buffered 16384 - La commande logging buffered doit être ajoutée pour enregistrer les messages système dans la mémoire tampon de log interne.** Le tampon de journalisation est circulaire. Une fois que le tampon de journalisation est rempli, les entrées plus anciennes sont remplacées par les nouvelles entrées. La taille du tampon de journalisation est configurable par l'utilisateur et est spécifiée en octets. La taille du tampon système varie selon les plates-formes. 16384 est une bonne valeur par défaut, qui fournit une journalisation adéquate dans la plupart des cas.
- **logging trap notifications- Cette commande fournit la transmission de messages du niveau notification (5) au serveur Syslog spécifié.** Le niveau de journalisation par défaut de tous les périphériques (console, moniteur, mémoire tampon et pièges) est le niveau de débogage (niveau 7). Si vous laissez le niveau de journalisation de pièges au niveau 7, de nombreux messages étrangers sont produits, qui ne concernent pas ou peu la santé du réseau. Affectez le niveau 5 à la journalisation par défaut des pièges.
- **logging facility local7 - Cette commande définit le niveau de journalisation par défaut des messages Syslog UNIX.** Configurez le serveur de Syslog qui reçoit ces messages en affectant le même niveau.
- **logging host - Cette commande définit l'adresse IP du serveur de journalisation UNIX.**
- **logging source-interface loopback 0 - Cette commande définit le SA IP par défaut applicable aux messages Syslog.** Codez en dur le SA de journalisation, afin de faciliter l'identification de l'hôte expéditeur du message.
- **service timestamps debug datetime localtime show-timezone msec - Par défaut, les messages de journalisation ne font pas l'objet d'un horodatage.** Vous pouvez utiliser cette commande pour activer l'horodatage des messages de journalisation et configurer l'horodatage des messages de débogage système. L'horodatage indique la temporisation relative des événements enregistrés et améliore le débogage en temps réel. Cette information est particulièrement utile quand les clients envoient les résultats de débogage au personnel de support technique pour obtenir de l'aide. Afin d'activer l'horodatage des messages de débogage système, utilisez cette commande en mode de configuration globale. Cette commande ne produit un effet que lorsque le débogage est activé.

Remarque : En outre, activez la journalisation pour l'état de la liaison et de l'offre groupée sur toutes les interfaces Gigabit de l'infrastructure.

Le logiciel Cisco IOS fournit un mécanisme simple pour définir le niveau de journalisation applicable à tous les messages système destinés à un serveur Syslog. Définissez le niveau de journalisation des pièces au niveau 5 (notification). Si vous définissez le niveau notification, vous pouvez minimiser le nombre de messages informationnels acheminés vers le serveur Syslog.

Cette configuration peut diminuer de manière significative la quantité de trafic Syslog sur le réseau et réduire l'impact sur les ressources serveur Syslog.

Ajoutez ces commandes à chaque routeur et commutateur exécutant le logiciel Cisco IOS afin d'activer la transmission de messages Syslog :

- Commandes de configuration globale Syslog :

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

- Commandes de configuration de l'interface Syslog :

```
logging event link-status
logging event bundle-status
```

SNMP

Objectif

Vous pouvez utiliser SNMP pour l'extraction des statistiques, des compteurs, et des tables qui sont enregistrés dans les MIB des périphériques réseau. Les NMS tels que HP OpenView peuvent utiliser l'information pour :

- Générer des alertes en temps réel
- Mesurer la disponibilité
- Produire des informations de planification de capacité
- Exécuter des contrôles de configuration et de dépannage

Fonctionnement de l'interface de gestion SNMP

SNMP est un protocole de la couche applicative qui fournit un format de message pour les communications entre les gestionnaires et les agents SNMP. SNMP fournit un cadre normalisé et un langage commun pour la surveillance et la gestion des périphériques d'un réseau.

L'infrastructure SNMP contient les trois composants suivants :

- Un gestionnaire SNMP
- Un agent SNMP
- Un MIB

Le gestionnaire SNMP est le système qui utilise SNMP pour contrôler et surveiller les activités réseau des serveurs. Le système de gestion le plus commun s'appelle NMS. Vous pouvez appliquer le terme NMS à un périphérique dédié qui est utilisé pour l'administration de réseau ou aux applications qui sont utilisées sur ce périphérique. Un grand choix d'applications de gestion de

réseau sont disponibles pour une utilisation avec SNMP. Ces applications vont des applications simples CLI aux interfaces graphiques telles que celles de la gamme CiscoWorks.

L'agent SNMP est le composant logiciel du périphérique géré qui met à jour les données pour le périphérique et enregistre ces données, selon les besoins, sur les systèmes de gestion. L'agent et le MIB résident sur le périphérique de routage (routeur, serveur d'accès, ou commutateur). Afin d'activer l'agent SNMP sur un périphérique de routage Cisco, vous devez définir le rapport entre le gestionnaire et l'agent.

Le MIB est une zone de stockage d'informations virtuelles utilisée pour les informations de gestion réseau. Le MIB se compose d'ensembles d'objets gérés. Dans le MIB, il existe des ensembles d'objets connexes définis dans des modules MIB. Les modules MIB sont écrits dans le langage de module MIB SNMP, comme défini par DST 58, RFC 2578 , RFC 2579 et RFC 2580 .

Remarque : les modules MIB individuels sont également appelés MIB. Par exemple, le groupe d'interfaces MIB (IF-MIB) est un module MIB contenu dans le MIB de votre système.

L'agent SNMP contient des variables MIB, dont les valeurs peuvent être demandées ou modifiées par le gestionnaire SNMP via des opérations get ou set. Un gestionnaire peut obtenir une valeur d'un agent ou stocker une valeur dans cet agent. L'agent recueille les données du MIB, qui est le référentiel des informations sur des paramètres des périphériques et sur les données réseau. L'agent peut également répondre aux demandes du gestionnaire pour obtenir ou définir des données.

Un gestionnaire peut envoyer les demandes d'agent pour obtenir et définir des valeurs MIB. L'agent peut répondre à ces demandes. L'agent, indépendant de cette interaction, peut envoyer des avis non sollicités (pièges ou informations) au gestionnaire afin de l'informer des conditions du réseau. Avec certains mécanismes de sécurité, un NMS peut extraire des informations des MIB à l'aide de demandes `get et` **get next , et peut émettre la commande set afin de changer des paramètres.** Vous pouvez également configurer un périphérique réseau pour la génération d'un message de piège envoyé au NMS pour des alertes en temps réel. Les ports IP UDP 161 et 162 sont utilisés pour les pièges.

Aperçu opérationnel des notifications SNMP

Une fonctionnalité principale de SNMP est la capacité de produire des notifications à partir d'un agent SNMP. Ces notifications n'exigent pas que les demandes soient envoyées à partir du gestionnaire SNMP. Les notifications non sollicitées (asynchrones) peuvent être produites en tant que pièges ou demandes d'informations. Les pièges sont des messages qui alertent le gestionnaire SNMP au sujet d'une condition présente sur le réseau. Les demandes d'informations (informs) sont des pièges qui incluent une demande de confirmation de réception de la part du gestionnaire SNMP. Les notifications peuvent indiquer des événements significatifs comme :

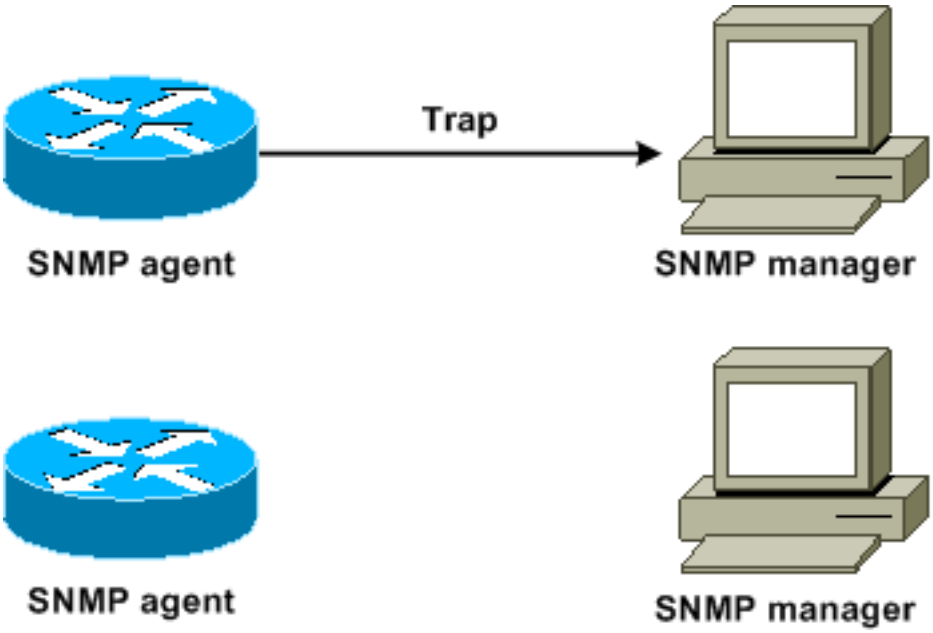
- Authentification utilisateur inexacte
- Redémarre
- Clôture d'une connexion
- Perte de connexion à un routeur voisin
- Autres événements

Les pièges sont moins fiables que les demandes d'informations, parce que le récepteur n'envoie aucun accusé de réception quand il reçoit un piège. L'expéditeur ne peut pas déterminer si le piège était a été reçu. Un gestionnaire SNMP qui reçoit une demande d'information accuse réception du message dans une unité PDU (Protocol Data Unit) de réponse SNMP. Si le

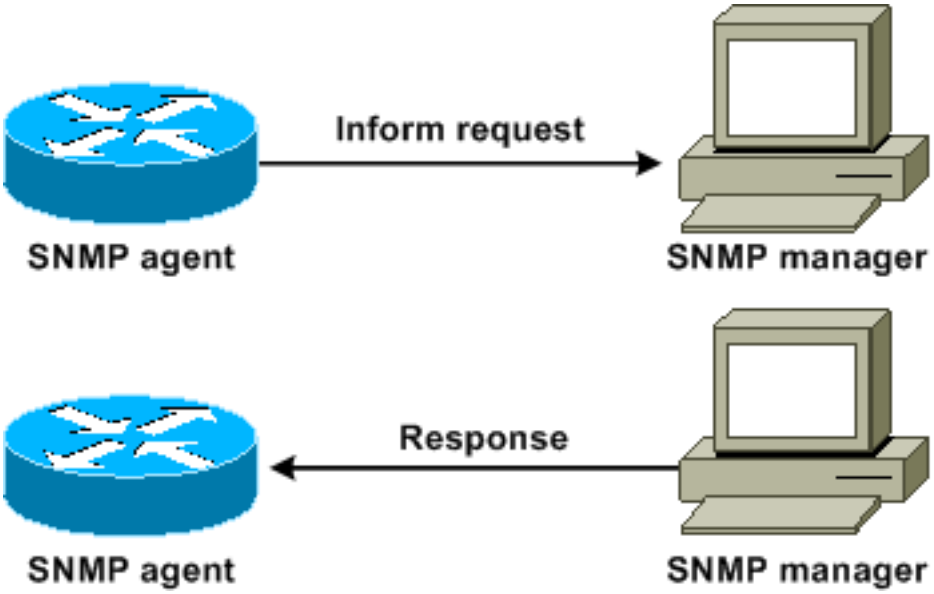
gestionnaire ne reçoit pas de demande d'informations, il n'envoie pas de réponse. Si l'expéditeur ne reçoit jamais de réponse, il peut envoyer de nouveau la demande d'information. Les demandes d'informations atteignent plus souvent la destination prévue.

Mais les pièges sont souvent préférés parce que les demandes d'informations consomment davantage de ressources au sein du routeur et du réseau. Un piège est jeté dès qu'il a été envoyé. En revanche, une demande d'information doit être conservée dans la mémoire jusqu'à ce qu'une réponse soit reçue ou jusqu'à expiration du délai d'attente. En outre, les pièges sont envoyés seulement une fois, alors qu'une demande d'information peut faire l'objet de plusieurs tentatives. Les nouvelles tentatives augmentent le trafic et contribuent à un temps système plus élevé sur le réseau. Par conséquent, les pièges et les demandes d'information fournissent un compromis entre la fiabilité et les ressources. Si le gestionnaire SNMP doit recevoir chaque notification, utilisez les demandes d'information. Mais si vous avez des problèmes de trafic sur votre réseau ou dans la mémoire du routeur et que vous n'avez pas besoin de recevoir chaque notification, utilisez plutôt les pièges.

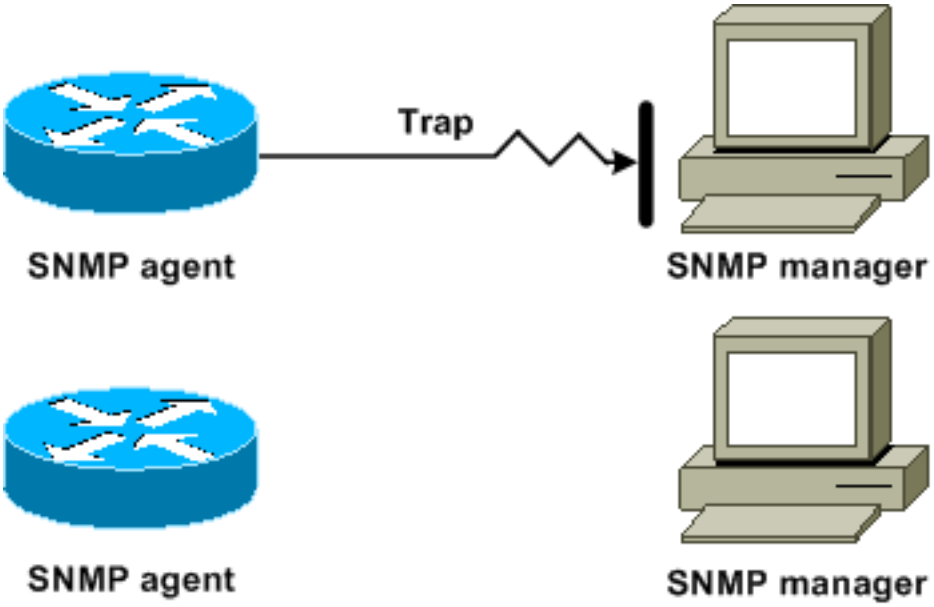
Ces diagrammes illustrent les différences entre les pièges et les demandes d'information :



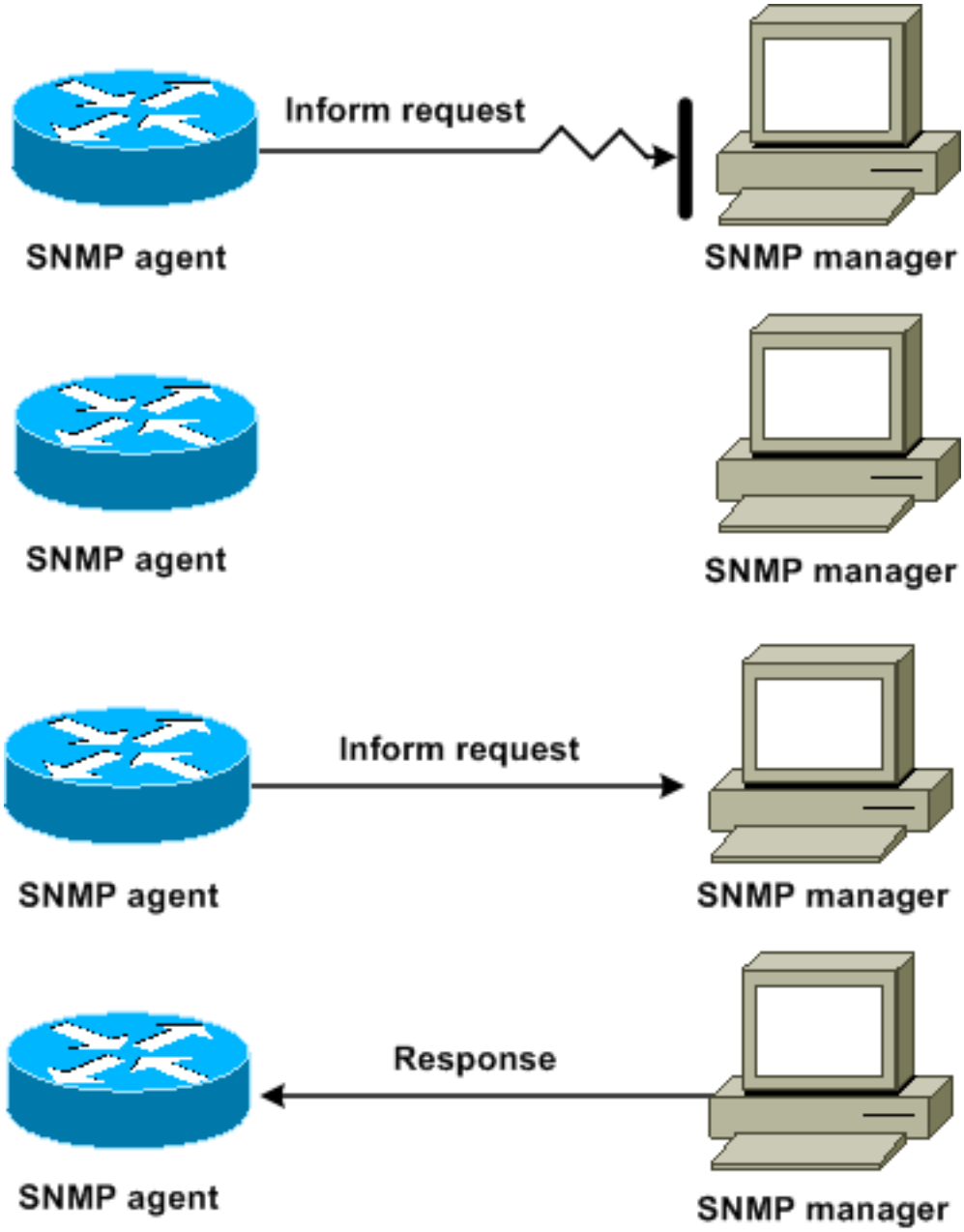
Ce diagramme illustre la méthode d'envoi de piège au gestionnaire SNMP par le routeur de l'agent. Bien que le gestionnaire reçoive le piège, il n'envoie aucun accusé de réception à l'agent. L'agent n'a aucun moyen de savoir que le piège a atteint la destination.



Ce diagramme illustre comment le routeur de l'agent envoie une demande d'information au gestionnaire. Quand le gestionnaire reçoit la demande d'information, il envoie une réponse à l'agent. De cette façon, l'agent sait que la demande d'information a atteint la destination. Notez que, dans cet exemple, il y a deux fois plus de trafic. Mais l'agent sait que le gestionnaire a reçu la notification.



Dans ce diagramme, l'agent envoie un piège au gestionnaire, mais le piège n'atteint pas ce dernier. L'agent n'a aucun moyen de savoir que le piège n'a pas atteint la destination, et le piège n'est donc pas renvoyé. Le gestionnaire ne reçoit jamais le piège.



Dans ce diagramme, l'agent envoie une demande d'information au gestionnaire, mais elle n'atteint jamais ce dernier. Puisque le gestionnaire n'a pas reçu la demande d'information, il n'y a aucune réponse. Après une période donnée, l'agent renvoie la demande d'information. Une deuxième fois, le gestionnaire reçoit la demande d'information et répond avec une réponse. Dans cet exemple, il y a davantage de trafic. Mais la notification atteint le gestionnaire SNMP.

MIB Cisco et références RFC

Les documents RFC définissent les modules MIB. Les documents RFC sont soumis à l'IETF (Internet Engineering Task Force), un organisme de normalisation international. Les personnes ou les groupes écrivent des RFC et les soumettent à l'ISOC (Internet Society) et à la communauté Internet dans son ensemble. Référez-vous à la page d'accueil d'Internet Society pour plus d'informations sur le processus de normalisation et sur les activités de l'IETF. Référez-vous à la page d'accueil de l'IETF afin de lire le texte intégral de tous les RFC, projets Internet (I-Ds), et STD que les documents Cisco mettent en référence.

L'implémentation Cisco de SNMP utilise :

- Les définitions de variables MIB II décrites dans RFC 1213
- Les définitions de pièges SNMP décrites dans RFC 1215

Cisco fournit ses propres extensions privées MIB avec chaque système. Les MIB d'entreprise Cisco sont conformes aux directives décrites dans les RFC appropriés, sauf mention contraire dans la documentation. Vous pouvez rechercher les fichiers de définition de modules MIB et la liste des MIB pris en charge sur chaque plate-forme Cisco dans la page d'accueil Cisco MIB.

Versions SNMP

Le logiciel Cisco IOS supporte ces versions de SNMP :

- SNMPv1 - Une norme Internet standard définie par RFC 1157 . RFC 1157 remplace les versions antérieures qui ont été publiées sous le nom de RFC 1067 et de RFC 1098 . La sécurité est basée sur des chaînes de caractères de la communauté.
- SNMPv2c - SNMPv2c est l'infrastructure administrative basée sur les chaînes de caractères de la communauté pour SNMPv2. SNMPv2c (C représentant la communauté) est un protocole Internet expérimental défini dans RFC 1901 , RFC 1905 et RFC 1906 . SNMPv2c est une mise à jour des opérations de protocole et des types de données SNMPv2p (snmpv2 classique). SNMPv2c utilise le modèle de sécurité à caractère communautaire SNMPv1.
- SNMPv3 — SNMPv3 est un protocole basé sur les normes interopérable défini dans RFC 2273 , RFC 2274 et RFC 2275 . SNMPv3 fournit un accès sécurisé aux périphériques avec une combinaison d'authentification et de chiffrement de paquets sur le réseau.Les fonctions de sécurité offertes par SNMPv3 sont :Intégrité des messages - Garantit qu'un paquet n'a pas été altéré pendant le transit.Authentification - Détermine que le message provient d'une source valide.Cryptage - Brouille le contenu d'un paquet, ce qui empêche la découverte par une source non autorisée.

SNMPv1 et SNMPv2c utilisent tous deux une forme de sécurité à caractère communautaire. Une liste de contrôle d'accès d'adresse IP et un mot de passe définissent la communauté de gestionnaires capables d'accéder au MIB de l'agent.

Le support SNMPv2c inclut un mécanisme de récupération en bloc et un message d'erreur plus détaillé faisant un reporting aux stations de gestion. Le mécanisme de récupération en bloc supporte la recherche des tables et de grandes quantités d'information, ce qui réduit au minimum le nombre d'allers-retour qui sont nécessaires. L'amélioration du support des erreurs-manipulations SNMPv2c inclut des codes d'erreur élargis qui distinguent différents genres de conditions d'erreur. Ces conditions sont enregistrées par le code d'erreur simple dans SNMPv1. Les codes d'erreur indiquent désormais le type d'erreur.

SNMPv3 prévoit des modèles de sécurité et des niveaux de sécurité. Un modèle de sécurité est une stratégie d'authentification définie pour un utilisateur et pour le groupe auquel il appartient. Un niveau de sécurité est le niveau de sécurité permis dans un modèle de sécurité. La combinaison d'un modèle de sécurité et d'un niveau de sécurité détermine quel mécanisme de sécurité est à utiliser quand un paquet SNMP est manipulé.

Configuration générale de SNMP

Émettez ces commandes sur tous les commutateurs clients afin d'activer la gestion SNMP :

- Commande pour ACL SNMP :
  `Switch(config)#`**`access-list 98 permit`** *`ip_address`*

```
!--- This is the SNMP device ACL.
```

- Commandes SNMP globales :

```
!--- These are sample SNMP community strings. Switch(config)#snmp-server community RO-
community ro 98
snmp-server community RW-community rw 98
snmp-server contact Glen Rahn (Home Number)
snmp-server location text
```

Recommandation concernant les pièges SNMP

SNMP est la base de toute l'administration de réseau et est activée et utilisée sur tous les réseaux.

L'agent SNMP peut communiquer avec plusieurs gestionnaires. Pour cette raison, vous pouvez configurer un logiciel pour supporter des transmissions avec une station de gestion via l'utilisation de SNMPv1, et une station de gestion différente via l'utilisation de snmpv2. La plupart de clients et des NMS utilisent toujours SNMPv1 et SNMPv2c, parce que le support de l'équipement réseau SNMPv3 sur les plates-formes NMS est insatisfaisant.

Activez les pièges SNMP pour toutes les fonctions qui sont en service. Vous pouvez désactiver d'autres fonctions, si vous le désirez. Une fois que vous avez activé un piège, vous pouvez émettre la commande **test snmp et configurer la manipulation appropriée sur le NMS pour l'erreur.** Les exemples d'une telle manipulation incluent une alerte par radiomessagerie ou un instantané.

Tous les pièges sont désactivés par défaut. Activez tous les pièges sur les commutateurs de base, comme le montre cet exemple :

```
Switch(config)#snmp trap enable
Switch(config)#snmp-server trap-source loopback0
```

Activez également les pièges de port pour les ports principaux (liaisons d'infrastructure avec les routeurs et les commutateurs, par exemple) et pour les ports serveur clés. Cette activation n'est pas nécessaire pour les autres ports (tels que les ports d'hôtes). Émettez cette commande afin de configurer le port et d'activer la notification de liaison active/inactive :

```
Switch(config-if)#snmp trap link-status
```

Ensuite, spécifiez les périphériques qui doivent recevoir les pièges et agir sur les pièges de manière appropriée. Vous pouvez maintenant configurer chaque destination de piège en tant que destinataire SNMPv1, snmpv2, ou SNMPv3. Pour les périphériques SNMPv3, des informations fiables peuvent être envoyées plutôt que des pièges UDP. Voici la configuration :

```
Switch(config)#snmp-server host ip_address [traps | informs] [version {1 | 2c | 3}] community-
string
!--- This command needs to be on one line. !--- These are sample host destinations for SNMP
traps and informs. snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 172.16.1.111 informs version 3 public
snmp-server host 172.16.1.33 public
```

Recommandations concernant l'interrogation SNMP

Assurez-vous que ces MIB sont les MIB principales interrogées ou surveillées au sein des réseaux campus :

Remarque : Cette recommandation provient du groupe Cisco Network Management Consulting.

Object Name	Object Description	OID	Period	Max
MIB-II				
SysUpTime	system uptime in 1/100ths of seconds	1.3.6.1.2.1.1.3	5 min	< 30000
CISCO-STACK-MIB				
ChassisPs1status	Status of power supply 1	1.3.6.1.4.1.9.5.1.2.4	10 min	≠ 2
ChassisPs2Status	Status of power supply 2	1.3.6.1.4.1.9.5.1.2.7	10 min	≠ 2
ChassisFanStatus	Status of Chassis Fan	1.3.6.1.4.1.9.5.1.2.9	10 min	≠ 2
ChassisMinorAlarm	Chassis Minor Alarm Status	1.3.6.1.4.1.9.5.1.2.11	10 min	≠ 1
chassis MajorAlarm	Chassis Major Alarm Status	1.3.6.1.4.1.9.5.1.2.12	10 min	≠ 1

Object Name	Object Description	OID	Period	Max
ChassisTempAlarm	Chassis Temperature Alarm status	1.3.6.1.4.1.9.5.1.2.13	10 min	≠ 1
ModuleStatus	Operational Status of the module	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min	≠ 2
CISCO-PROCESS-MIB				
CpmCPUTotal5min	The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5	5 min	
CISCO-STACK-MIB				
SysTraffic	% of bandwidth utilization for the previous polling interval	1.3.6.1.4.1.9.5.1.1.8	30 min	

Object Name	Object Description	OID	Period	Max
SysTrafficPeak	Peak traffic meter value since the last time the port counters were cleared or the system started	1.3.6.1.4.1.9.5.1.1.19	30 min	
BRIDGE-MIB				
CiscoEsStackSwitchBufferOverruns	Number of times the switch was out of buffers	1.3.6.1.4.1.9.5.14.2.1.1.17	30 min	

Protocole NTP

Objectif

Le protocole NTP (Network Time Protocol), RFC 1305 , synchronise la mesure du temps parmi un ensemble de serveurs et clients distribués. NTP permet pour la corrélation des événements à la création des journaux système et lorsque des événements liés au temps se produisent.

Aperçu opérationnel

RFC 958 a documenté NTP tout d'abord. Mais NTP a évolué avec RFC 1119 (NTP version 2). RFC 1305 définit maintenant le protocole NTP, qui est dans sa troisième version.

NTP synchronise l'heure d'un ordinateur client ou du serveur par rapport à une autre source temporelle de serveur ou de référence, telle qu'une radio, un récepteur satellite, ou un modem. NTP fournit au client l'exactitude d'une ms sur les LAN et jusqu'à quelques dizaines de ms sur les WAN, pour un serveur principal synchronisé. Par exemple, vous pouvez utiliser NTP pour coordonner le temps UTC via un récepteur GPS (Global Positioning Service).

Les configurations typiques NTP utilisent plusieurs serveurs redondants et des chemins réseau divers afin de réaliser une grande précision et fiabilité. Quelques configurations incluent l'authentification cryptographique afin d'empêcher des attaques de protocole malveillantes ou accidentelles.

NTP est exécuté sur UDP, qui à son tour, fonctionne sur IP. Toute la transmission NTP utilise l'UTC, qui est identique à l'heure du méridien de Greenwich.

Actuellement, des mises en oeuvre NTP version 3 (NTPv3) et NTP version 4 (NTPv4) sont disponibles. La dernière version de logiciel utilisée est NTPv4, mais la norme Internet officielle est

toujours NTPv3. En outre, quelques constructeurs de systèmes d'exploitation personnalisent la mise en place du protocole.

Sauvegardes de NTP

La mise en place de NTP tente également d'éviter la synchronisation sur une machine sur laquelle l'heure ne peut pas être précise. NTP fait ceci de façons :

- NTP ne fait pas de synchronisation sur une machine qui n'est pas elle-même synchronisée.
- NTP compare toujours l'heure enregistrée par plusieurs machines, et ne fait pas de synchronisation sur une machine sur laquelle l'heure est sensiblement différente des autres, même si cette machine a une strate inférieure.

Associations

Les transmissions entre les machines qu'exécute NTP, qui sont connues sous le nom d'associations, sont habituellement configurées de manière statique. Chaque machine reçoit les IP address de toutes les machines avec lesquelles elle doit former des associations. La mesure du temps précise est possible par l'échange de messages NTP entre chaque paire de machines avec une association. Mais dans un environnement de réseau local, vous pouvez configurer NTP pour utiliser les messages de diffusion sur IP. De cette façon, vous pouvez configurer la machine pour envoyer ou recevoir les messages de diffusion, mais la précision de la mesure du temps est réduite parce que le flux d'informations est à sens unique.

Si le réseau est isolé d'Internet, la mise en oeuvre Cisco de NTP permet de configurer une machine de telle sorte qu'elle agisse comme si elle était synchronisée avec l'utilisation du protocole NTP, quand elle a réellement déterminé l'heure avec l'utilisation d'autres méthodes. D'autres machines se synchronisent avec cette machine via l'utilisation de NTP.

Une association NTP peut être soit :

- Une association d'homologuesCela signifie que ce système peut se synchroniser avec l'autre système ou autoriser l'autre système à se synchroniser avec lui.
- Une association de serveursCela signifie que seul ce système se synchronise avec l'autre système. L'autre système ne se synchronise pas avec ce système.

Si vous voulez former une association NTP avec d'autres systèmes, utilisez l'une de ces commandes en mode de configuration globale :

Commande	Objectif
ntp peer *ip-address [normal-sync] [version number] [key key-id]* [source interface] [prefer]	Forme une association d'homologues avec d'autres systèmes
ntp server *ip-address [version number] [key key-id]* [source interface] [prefer]	Forme une association de serveurs avec d'autres systèmes

Remarque : Une seule extrémité d'une association doit être configurée. L'autre système établit automatiquement l'association.

Accès aux serveurs temporels publics

Le sous-réseau NTP inclut actuellement plus de 50 serveurs principaux publics synchronisés

directement à l'UTC par la radio, le satellite, ou le modem. Normalement, les postes de travail client et les serveurs avec un nombre relativement réduit de clients ne sont pas synchronisés aux serveurs principaux. Il y a environ 100 serveurs secondaires publics qui sont synchronisés sur les serveurs principaux. Ces serveurs fournissent une synchronisation à un total de plus de 100 000 clients et serveurs sur Internet. La page Serveurs NTP publics de NTP met à jour les listes actuelles et est mise à jour fréquemment.

Il y a aussi de nombreux serveurs primaires et secondaires privés qui ne sont pas normalement disponibles au public. Référez-vous au projet Network Time Protocol (université du Delaware) pour obtenir les listes de serveurs NTP publics et des informations sur la façon de les utiliser. Il n'y a aucune garantie que ces serveurs NTP Internet publics soient disponibles et produisent l'heure correcte. Par conséquent, vous devez considérer d'autres options. Par exemple, servez-vous des divers périphériques autonomes GPS qui sont directement connectés à un certain nombre de routeurs.

Une autre possibilité consiste à utiliser différents routeurs, définis en tant que master de la strate 1. Mais l'utilisation d'un tel routeur n'est pas recommandée.

Stratum

NTP emploie une strate afin de décrire le nombre de sauts NTP entre une machine et une source temporelle. Un serveur de la strate 1 a une radio ou une horloge atomique qui est directement connectée. Un serveur de la strate 2 reçoit l'heure d'un serveur de la strate 1, etc. Une machine qui exécute NTP automatiquement choisit en tant que source temporelle la machine avec le nombre le plus faible de strates configurées pour communiquer via NTP. Cette stratégie construit une organisation autonome efficace de haut-parleurs NTP.

NTP évite la synchronisation à un périphérique sur lequel l'heure n'est probablement pas précise. Pour plus d'informations, reportez-vous à la section *Sauvegardes de NTP de* Network Time Protocol .

Relation de partenariat entre serveurs

- Un serveur répond aux requêtes client, mais n'essaye pas d'incorporer d'informations sur la date dans source temporelle client.
- Un homologue répond aux requêtes client et essaye d'utiliser la requête client en tant que candidat potentiel pour une meilleure source temporelle et pour faciliter la stabilisation de sa fréquence d'horloge.
- Afin d'être des véritables partenaires, les deux côtés de la connexion doivent entrer dans un rapport de partenariat, plutôt qu'une situation dans laquelle un utilisateur est homologue et l'autre est serveur. Procurez-vous les clés d'échange d'homologues de sorte que seulement les hôtes de confiance puissent parler à d'autres comme homologues.
- Dans une requête client à un serveur, le serveur répond au client et oublie que le client a posé une question ;
- Dans une requête client à un homologue, le serveur répond au client. Le serveur garde les informations d'état sur le client afin de suivre la mesure du temps effectuée par le client et la strate exécutée par le client.

Un serveur NTP peut gérer des milliers de clients sans problème. Mais quand un serveur NTP gère plus de quelques clients (jusqu'à quelques centaines), il y a un impact mémoire sur la capacité du serveur à conserver les informations d'état. Quand un serveur NTP manipule plus que la quantité recommandée, il consomme plus de ressources CPU et de bande passante.

Modes de communication avec le serveur NTP

Voici deux modes distincts permettant de communiquer avec le serveur :

- Mode diffusion
- Mode client/serveur

En mode diffusion, les clients écoutent. En mode client/serveur, les clients interrogent le serveur. Vous pouvez utiliser la diffusion NTP si aucune liaison WAN n'est impliquée en raison de sa vitesse. Afin d'accéder à une liaison WAN, utilisez le mode client/serveur (via l'interrogation). Le mode diffusion a été conçu pour les LAN, sur lesquels de nombreux clients doivent interroger le serveur. Sans mode diffusion, cette interrogation peut probablement produire un grand nombre de paquets sur le réseau. NTP multicast n'est pas encore disponible dans NTPv3, mais est disponible dans NTPv4.

Par défaut, le logiciel Cisco IOS communique avec l'utilisation de NTPv3. Mais ce logiciel est compatible avec des versions antérieures de NTP.

Sondage

Le protocole NTP permet à un client de questionner un serveur quand il le souhaite.

Quand vous configurez d'abord NTP dans Cisco, NTP envoie huit requêtes à intervalles rapides (`NTP_MINPOLL (2^4=16 secondes)`. `Le NTP_MAXPOLL est égal à 2^14 secondes (16 384 sec ou 4 heures, 33 minutes, 4 sec)`. Cette période est la plus longue période avant la nouvelle interrogation NTP visant à obtenir une réponse. Actuellement, Cisco n'a pas de méthode pour permettre à l'utilisateur de forcer manuellement `POLL` .

Le compteur d'interrogation NTP commence à 2^6 (64) sec, ou 1 minute, 4 sec. Cette durée est incrémentée par des puissances de 2, comme deux serveurs se synchronisent mutuellement, à 2^10. Vous pouvez prévoir l'envoi des messages de synchronisation à un intervalle de 64, 128, 256, 512, ou 1024 sec, selon la configuration du serveur ou du partenaire. L'intervalle le plus long entre les interrogations a lieu lorsque l'horloge devient plus stable en raison des boucles à verrouillage déphasé. Les boucles à verrouillage déphasé équilibrent le cristal d'horloge locale, jusqu'à 1024 secondes (17 minutes).

La durée varie entre 64 secondes et 1024 secondes comme puissance de 2 (qui équivaut à une fois à toute les 64, 128, 256, 512, ou 1024 sec). Le temps est basé sur la boucle à verrouillage déphasé qui envoie et reçoit les paquets. S'il y a beaucoup d'instabilité, l'interrogation est plus fréquente. Si l'horloge de référence est précise et la connectivité réseau cohérente, les durée d'interrogation convergent sur 1024 secondes entre chaque interrogation.

L'intervalle entre deux interrogations NTP change comme la connexion entre le client et le serveur. Avec une meilleure connexion, l'intervalle entre deux interrogations est plus long. Dans ce cas, une meilleure connexion signifie que le client NTP a reçu huit réponses pour les huit dernières demandes. L'intervalle entre deux interrogations est alors doublé. Une seule réponse manquée réduit de moitié l'intervalle entre deux interrogations. L'intervalle entre deux interrogations commence à 64 secondes, pour un maximum de 1024 secondes. Dans les meilleures circonstances, la durée requise pour que l'intervalle entre deux interrogations passe de 64 secondes à 1024 est égale à un peu plus de 2 heures.

Diffusions

Les diffusions NTP ne sont jamais expédiées. Si vous émettez la commande **ntp broadcast , le routeur commence les diffusions NTP sur l'interface sur laquelle il est configuré.**

Généralement, vous émettez la commande **ntp broadcast afin d'envoyer des diffusions NTP sur un LAN pour entretenir les stations et les serveurs d'extrémité client.**

Synchronisation temporelle

La synchronisation d'un client par rapport à un serveur se compose de plusieurs échanges de paquets. Chaque échange est une paire de demande/réponse. Quand un client envoie une demande, il enregistre son heure locale dans le paquet envoyé. Quand un serveur reçoit le paquet, il enregistre sa propre évaluation de l'heure actuelle dans le paquet, et le paquet est retourné. Quand la réponse est reçue, le récepteur enregistre une fois de plus sa propre heure de réception afin d'estimer la durée d'acheminement du paquet.

Ces différences d'heure peuvent être utilisées afin d'estimer la durée nécessaire pour que le paquet communique du serveur au demandeur. Cette durée aller-retour est prise en compte pour l'évaluation de l'heure actuelle. Plus l'aller-retour est court, plus la précision de l'estimation est élevée.

L'heure n'est pas acceptée tant que plusieurs échanges de paquets n'ont pas eu lieu. Certaines valeurs essentielles sont placées dans des filtres à plusieurs étages afin d'estimer la qualité des échantillons. Habituellement, environ 5 minutes sont nécessaires pour qu'un client NTP soit synchronisé à un serveur. Cela vaut également pour les horloges de référence locales qui n'ont aucun retard du tout par définition, et c'est là un point intéressant.

En outre, la qualité de la connexion réseau influence également la précision finale. Les réseaux lents et imprévisibles avec des retards variables exercent un effet néfaste sur la synchronisation temporelle.

Une différence temporelle de moins de 128 ms est requise pour la synchronisation NTP. En général, sur Internet, la précision est comprise entre 5 et 100 ms, ce qui peut varier en fonction des retards sur le réseau.

Niveaux de trafic NTP

La bande passante utilisée par NTP est minime. L'intervalle entre les messages d'interrogation que s'échangent les homologues ne dépasse pas un message toutes les 17 minutes (1024 sec). Avec une planification rigoureuse, vous pouvez maintenir cette valeur au sein de réseaux de routeurs sur des liaisons WAN. Associez les clients NTP aux serveurs NTP locaux (et non sur tout le parcours compris entre le WAN et les routeurs principaux), soit les serveurs de la strate 2.

Un client NTP en convergence utilise environ 0,6 bits par seconde (bps) par serveur.

Recommandation Cisco relative à NTP

- Cisco recommande d'utiliser plusieurs serveurs et chemins réseau différents, afin d'obtenir une précision et une fiabilité optimales. Quelques configurations incluent l'authentification cryptographique afin d'empêcher des attaques de protocole malveillantes ou accidentelles.
- Conformément au RFC, NTP est vraiment conçu pour permettre d'interroger différents serveurs et d'utiliser des analyses statistiques complexes afin d'obtenir une heure valide, même si vous n'êtes pas certain que tous les serveurs que vous interrogez sont bien fondés.

NTP estime les erreurs de toutes les horloges. Par conséquent, tous les serveurs NTP renvoient l'heure avec une estimation d'erreur. Quand vous utilisez des serveurs différents, NTP veut également que ces serveurs conviennent d'une certaine heure.

- L'implémentation Cisco du protocole NTP ne supporte pas le service de la strate 1. Vous ne pouvez pas vous connecter à une radio ou à une horloge atomique. Cisco recommande que le service horaire pour le réseau soit dérivé des serveurs publics NTP qui sont disponibles sur Internet IP.
- Activez tous les commutateurs client pour envoyer régulièrement des demandes d'heure à un serveur NTP. Vous pouvez configurer jusqu'à 10 adresses serveur/homologue par client, afin d'obtenir une synchronisation rapide.
- Afin de réduire le temps système du protocole, les serveurs secondaires distribuent l'heure via NTP aux autres hôtes locaux. A des fins de fiabilité, vous pouvez équiper les serveurs sélectionnés d'horloges moins précises mais moins chères pour utiliser la sauvegarde en cas de panne des serveurs primaire et/ou secondaire ou des voies de communication entre eux.
- **ntp update-calendar - Le NTP change habituellement uniquement l'horloge système.** Cette commande permet à NTP de mettre à jour les informations de date/heure sur le calendrier. Cette mise à jour n'est effectuée que si l'heure NTP est synchronisée. Sinon, le calendrier garde son heure et n'est pas affecté par l'heure NTP ou par l'horloge système. Utilisez toujours cette solution sur les routeurs haut de gamme.
- **clock calendar-valid - Cette commande permet de déclarer que les informations du calendrier sont valides et synchronisées.** Utilisez cette option sur le NTP maître. Si cela n'est pas configuré, le routeur haut de gamme qui possède le calendrier pense que son heure est non fondée, même s'il a le NTP maître.
- Tout numéro de strate supérieur à 15 est considéré comme non synchronisé. C'est pourquoi vous voyez la strate 16 dans la sortie de la commande **show ntp status sur les routeurs pour lesquels les horloges sont non synchronisées.** Si le master est synchronisé avec un serveur NTP public, assurez-vous que le numéro de strate sur le NTP maître est supérieur d'un ou deux au numéro de strate le plus élevé des serveurs publics interrogés.
- Beaucoup de clients font configurer NTP en mode serveur sur leurs plates-formes de logiciel Cisco IOS, synchronisées à partir de plusieurs alimentations fiables issues d'Internet ou d'une horloge radio. En interne, une alternative plus simple au mode serveur quand vous exécutez un grand nombre de commutateurs est d'activer NTP en mode client de diffusion sur le VLAN de gestion dans un domaine commuté. Ce mécanisme laisse Catalyst recevoir une horloge à partir de messages de diffusion. Cependant, la précision de la mesure du temps est marginalement réduite parce que le flux d'information est à sens unique.
- L'utilisation d'adresses de bouclage en tant que source des mises à jour peut également favoriser la cohérence. Vous pouvez résoudre les problèmes de sécurité de deux façons :Avec le contrôle des mises à jour de serveur, ce que Cisco recommandePar authentification

Commandes de configuration globale NTP

```
!--- For the client: clock timezone EST  -5  ????
ntp source loopback 0 ?????
ntp server ip_address key 1
ntp peer ip_address
!--- This is for a peer association. ntp authenticate
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1
```

```
!--- For the server: clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ntp source loopback0
ntp update-calendar

!--- This is optional: interface vlan_id ntp broadcast
!--- This sends NTP broadcast packets. ntp broadcast client
!--- This receives NTP broadcast packets. ntp authenticate
ntp authentication-key 1 md5 xxxxx
ntp trusted-key 1
ntp access-group access-list
!--- This provides further security, if needed.
```

Commande NTP status

```
show ntp status

Clock is synchronized, stratum 8, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18
reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

C'est l'adresse d'horloge de référence pour le routeur Cisco quand ce dernier est un serveur NTP maître. Si le routeur n'a pas été synchronisé avec un serveur NTP, le routeur utilise cette adresse comme ID de référence. Pour plus d'informations sur la configuration et sur les commandes, reportez-vous à la section Configuration de NTP de Exécuter la gestion système de base.

Cisco Discovery Protocol

Objectif

CDP est exécuté sur la couche 2 (couche liaison de données) sur tous les routeurs, passerelles, serveurs d'accès et commutateurs Cisco. CDP permet aux applications de gestion de réseau d'identifier les périphériques Cisco voisins de périphériques connus. En particulier, les applications de gestion de réseau peuvent identifier les voisins qui exécutent des protocoles transparents de couche inférieure. Avec CDP, les applications de gestion de réseau peuvent apprendre le type de périphérique et l'adresse de l'agent SNMP des périphériques voisins. Cette fonction permet à des applications d'envoyer des requêtes SNMP aux périphériques voisins.

Les commandes **show associées à la fonction CDP permettent aux ingénieurs réseau de déterminer les informations suivantes :**

- Le numéro de module/port des autres périphériques CDP adjacents
- Les adresses suivantes du périphérique contigu :Adresse MAC :Adresse IPAdresse port-canal
- Version du logiciel de périphérique contigu
- Informations suivantes sur le périphérique contigu :VitesseDuplexDomaine VTPConfiguration de VLAN natif

La section Aperçu opérationnel décrit certaines améliorations de la version 2 de CDP (CDPv2) par rapport à la version 1 (CDPv1).

Aperçu opérationnel

CDP est exécuté sur tous les supports de LAN et de WAN prenant en charge SNAP.

Chaque périphérique configuré pour CDP envoie des messages périodiques à une adresse multicast. Chaque périphérique annonce au moins une adresse à laquelle le périphérique peut recevoir des messages SNMP. Ces annonces contiennent également les informations Time to Live, ou temps de maintien. Ces informations indiquent la durée de maintien des informations du protocole CDP par un périphérique récepteur avant abandon.

CDP utilise l'encapsulation SNAP avec un code 2000. Sur Ethernet, ATM et FDDI, l'adresse multicast de destination 01-00-0c-cc-cc-cc est utilisée. Sur des Token Ring, l'adresse fonctionnelle c000.0800.0000 est utilisée. Des trames CDP sont envoyées périodiquement chaque minute.

Les messages CDP contiennent un ou plusieurs sous-messages qui permettent au périphérique de destination de recueillir et stocker des informations au sujet de chaque périphérique voisin.

Ce tableau indique les paramètres que CDPv1 supporte :

Paramètre	Type	Description
1	l'identifiant,	Nom d'hôte du périphérique ou numéro de série du matériel dans l'ASCII.
2	Adresse	L'adresse de couche 3 de l'interface qui envoie la mise à jour
3	ID du port	Le port sur lequel la mise à jour de CDP est envoyée
4	Fonctionnalités	Décrit les capacités du périphérique fonctionnel de cette façon : • Routeur: 0x01 • Pont SR[1] : 0x04 • Commutateur : 0x08 (fournit la commutation de couche 2 et/ou 3) • Hôte : 0x10 • Filtrage IGMP conditionnel : 0x20 • Le pont ou le commutateur n'expédie pas les paquets IGMP sur des ports non routeurs.
5	Version	Chaîne de caractères contenant la version logicielle **Remarque :** La sortie de la commande **show version** affiche les mêmes informations.
6	Plateforme	Plate-forme matérielle, par exemple WS-C5000, WS-C6009 et Cisco RSP[2]

[1] SR = route-source.

[2] RSP = Route Switch Processor.

Dans CDPv2, un type supplémentaire, la longueur, les valeurs TLV ont été introduits. CDPv2 supporte tout TLV. Mais ce tableau fournit les paramètres qui peuvent être particulièrement utiles dans les environnements commutés et qui le logiciel Catalyst utilise.

Quand un commutateur exécute CDPv1, il supprime les trames CDPv2. Quand un commutateur exécutant CDPv2 reçoit une trame CDPv1 sur une interface, il commence à envoyer les trames CDPv1 hors de cette interface en plus des trames CDPv2.

Paramètre	Type	Description
9	Domaine VTP	Le domaine VTP, si configuré sur le périphérique.
10	VLAN natif	Dans dot1q, les trames pour le VLAN dans lequel le port se trouve s'il n'est pas un port de liaison de jonction ne sont pas balisées. Cela porte habituellement le nom de VLAN natif.
11	Mode bidirectionnel simultané/en alternat	Ce TLV contient la configuration duplex du port émetteur.
14	ID VLAN d'appareil	Permet au trafic VoIP d'être différencié du reste du trafic via un ID de VLAN distinct (VLAN auxiliaire).
16	Consommation électrique	La quantité maximale de puissance consommée prévue, exprimée en mW, par le périphérique connecté.
17	MTU	Le MTU de l'interface via laquelle la trame CDP est transmise.
18	Confiance étendue	Indique que le port est en mode de confiance étendue.
19	COS pour les ports non approuvés	La valeur de Classe de service (Cos) à utiliser pour marquer tous les paquets reçus sur le port non approuvé d'un dispositif de commutation connecté.
20	NomSys	Nom de domaine complet du périphérique (0, si inconnu).
25	Puissance	Transmis par un périphérique afin de négocier un niveau de puissance

	demandée	approprié.
26	Puissance disponible	Transmis par un commutateur. Permet à un périphérique de négocier et de sélectionner un paramètre de puissance approprié.

CDPv2/Power sur Ethernet

Certains commutateurs, tels que Catalyst 6500/6000 et 4500/4000, ont la capacité d'assurer la puissance aux périphériques par l'intermédiaire de câbles UTP (Unshielded Twisted Pair). Les informations reçues via CDP (paramètres 16, 25, 26) aide à l'optimisation de la gestion de l'alimentation.

Interaction téléphone IP CDPv2/Cisco

Les téléphones IP Cisco offrent une connectivité aux périphérique Ethernet 10/100-Mbps externes. Cette connectivité est réalisée par l'intégration d'une couche interne 2 de trois ports dans le téléphone sur IP. Les ports de commutation interne sont mentionnés en tant que :

- P0 (périphérique interne de téléphone sur IP)
- P1 (port 10/100-Mbps externe)
- P2 (port 10/100-Mbps externe qui se connecte au commutateur)

Vous pouvez transférer le trafic voix sur un VLAN séparé du port de commutation si vous configurez les ports d'accès dot1q. Ce VLAN supplémentaire est connu en tant que VLAN auxiliaire (CatOS) ou VLAN voix (Logiciel Cisco IOS). Par conséquent, le trafic dot1q marqué du téléphone sur IP peut être envoyé sur le VLAN auxiliaire/Voix, et le trafic non balisé peut être envoyé par l'intermédiaire du port 10/100-Mbps externe du téléphone via le VLAN d'accès.

Les commutateurs Catalyst peuvent informer un téléphone sur IP de l'ID de VLAN Voix par l'intermédiaire du CDP (Parameter-14 : ID VLAN d'appareil). En conséquence, le téléphone sur IP marque tous les paquets VoIP à l'aide de l'ID de VLAN approprié et de la priorité 802.1p. Ce TLV CDP est également utilisé pour déterminer si un téléphone IP est connecté via le paramètre d'ID d'appareil.

Ce concept peut être exploité quand vous développez une politique QoS. Vous pouvez configurer le commutateur Catalyst en vue d'une interaction avec le téléphone IP de l'une des trois manières suivantes :

- Téléphone IP Cisco (appareil autorisé)Vous ne devez faire confiance au CoS que lorsqu'un téléphone IP est détecté via CDP. Chaque fois qu'un téléphone sur IP est détecté via le paramètre CDP 14, l'état de confiance du port est défini de façon à faire confiance au COS. Si aucun téléphone sur IP n'est détecté, le port est Non approuvé.
- Confiance étendueLe commutateur peut informer le téléphone sur IP via CDP (paramètre 18) qu'il doit faire confiance à toutes les trames reçues sur son port de périphérique externe 10/100-Mbps.
- Réécrivez le COS pour les ports non approuvésLe commutateur peut informer le téléphone IP via CDP (paramètre 19) en vue de la réécriture des valeurs CoS 802.1p reçues sur son port de périphérique externe 10/100 Mbps.**Remarque :** Par défaut, tout le trafic reçu sur les ports externes 10/100 Mbits/s du téléphone IP n'est pas approuvé.

Note: Voici un exemple de configuration pour connecter le téléphone IP non Cisco à un

commutateur.

Remarque : par exemple,

```
Switch(config)#interface gigabitEthernet 2/1
Switch(config-if)#switchport mode trunk

!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
Switch(config-if)#spanning-tree portfast trunk

!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Recommandation de configuration Cisco

Les informations fournies par CDP peuvent être extrêmement utiles quand vous effectuez un dépannage suite à des problèmes de connectivité de la couche 2. Activez CDP sur tous les périphériques qui le prennent en charge. Émettez les commandes suivantes :

- Pour activer CDP globalement sur le commutateur :
  ```
  Switch(config)#cdp run
  ```
- Pour activer CDP port par port :
  ```
  Switch(config)#interface type slot#/port#
  Switch(config-if)#cdp enable
  ```

Liste de contrôle de la configuration

Commandes globales

Pour commencer le processus de configuration du commutateur, connectez-vous, activez le mode de configuration globale et entrez dans ce mode.

```
Switch>enable
Switch#
Switch#configure terminal
Switch(Config)#
```

Commandes génériques globales (à l'échelle de l'entreprise)

La section Commandes globales répertorie les commandes globales à appliquer à tous les commutateurs du réseau d'entreprise du client.

Cette configuration contient les commandes globales recommandées à ajouter à la configuration d'origine. Vous devez changer les valeurs de la sortie avant de copier et coller le texte dans la CLI. Émettez ces commandes afin d'appliquer la configuration globale :

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
ip domain-name domain_name
ip name-server name_server_ip_address
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

This is a proprietary system, NOT for public or personal use.  All work products,
communications, files, data or information directly or indirectly created, input
or accessed on this system are and shall become the sole property of the company.
This system is actively monitored and accessed by the company.  By logging onto
this system, the user consents to such monitoring and access.

USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

^C
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

Commandes globales qui sont spécifiques à chaque châssis de commutateur

Les commandes globales décrites dans cette section sont spécifiques à chaque châssis de commutateur installé sur le réseau.

Variables de configuration spécifiques aux châssis

Pour définir la date et l'heure, émettez cette commande :

```
Switch#clock set hh:mm:ss day month year
```

Pour définir le nom d'hôte du périphérique, émettez ces commandes :

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Cat6500
```

Pour configurer l'interface de bouclage à des fins de gestion, émettez ces commandes :

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#exit
```

Pour afficher la révision du logiciel Cisco IOS (Supervisor Engine), émettez ces commandes :

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
cat6500#
```

Pour afficher la révision du fichier de démarrage MSFC, émettez cette commande :

```
Cat6500#dir bootflash:
Directory of bootflash:/
 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a

15990784 bytes total (14111616 bytes free
```

Pour spécifier les informations de contact et les emplacements liés au serveur SNMP, émettez ces commandes :

```
Cat6500(config)#snmp-server contact contact_information
Cat6500(config)#snmp-server location location_of_device
```

Afin de copier la configuration de démarrage d'un Supervisor Engine existant vers un nouveau Supervisor Engine, il peut y avoir une perte de configuration, par exemple, la configuration sur les interfaces du superviseur existant. Cisco recommande de copier la configuration dans un fichier texte et de la coller en segments dans la console afin de voir s'il y a des problèmes de configuration.

Commandes d'interface

Types de ports Cisco fonctionnels

Les ports de commutation en Logiciel Cisco IOS sont appelés interfaces. Il y a deux types de modes d'interface dans le logiciel Cisco IOS :

- L'interface routée de couche 3
- L'interface commutateur de couche 2

La fonction d'interface se rapporte à la façon dont vous avez configuré le port. La configuration du port peut être :

- Interface routée
- SVI (Switched virtual interface)
- Port d'accès
- Trunk
- EtherChannel
- Une combinaison de ces derniers

Le type d'interface se rapporte à un type de port. Le type de port peut être soit :

- FE
- GE
- Canal de port

Cette liste décrit brièvement différentes fonctions d'interface du logiciel Cisco IOS :

- Interface physique routée (valeur par défaut) - Chaque interface du commutateur est par défaut une interface routée de couche 3, qui est semblable à n'importe quel routeur Cisco. L'interface routée doit être sur un seul sous-réseau IP.
- Interface de port de commutation d'accès - Cette fonction est utilisée pour placer des interfaces dans le même VLAN. Les ports doivent être convertis d'interface routée en interface commutée.
- SVI - Un SVI peut être associé à un VLAN qui contient des ports de commutation d'accès pour le routage interVLAN. Configurez SVI afin qu'il soit associé à un VLAN quand vous voulez disposer d'un pont entre des ports de commutation d'accès situés sur différents VLAN.
- Interface de port de commutation de jonction - Cette fonction est utilisée pour acheminer plusieurs VLAN vers un autre périphérique. Les ports doivent être convertis d'interface routée en interface de commutation de jonction.
- EtherChannel - Un EtherChannel est utilisé pour regrouper des ports individuels en un même port logique, à des fins de redondance et d'équilibrage de charge.

Recommandations Cisco liées aux types de ports fonctionnels

Utilisez les informations de cette section afin de déterminer les paramètres à appliquer aux interfaces.

Remarque : certaines commandes spécifiques à l'interface sont incorporées dans la mesure du possible.

Négociation automatique

N'utilisez pas l'autonégociation dans ces situations :

- Pour les ports qui prennent en charge les périphériques d'infrastructure réseau tels que des commutateurs et des routeurs
- Pour d'autres systèmes d'extrémité non temporaires tels que des serveurs et des imprimantes

Configurez manuellement la vitesse et la configuration duplex de ces liaisons 10/100-Mbps. Les configurations sont habituellement 100-Mbps bidirectionnelles full-duplex :

- Liaison 100 MB commutateur à commutateur
- Liaison 100 MB commutateur à commutateur
- Liaison 100 MB commutateur à routeur

Vous pouvez configurer ces paramètres de cette façon :

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

Cisco recommande les configurations 10/100-Mbps pour les utilisateurs finaux. Les travailleurs mobiles et les hôtes temporaires ont besoin de l'autonégociation, comme l'illustre cet exemple :

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed auto
```

La valeur par défaut sur les interfaces Gigabit est `auto-negotiation`. Cependant, émettez ces commandes afin de vérifier que l'autonégociation est activée. Cisco recommande cisco l'activation de la négociation Gigabit :

```
Cat6500(config-if)#interface gigabitethernet mod#/port#
Cat6500(config-if)#no speed
```

Racine Spanning-tree

Selon la conception du réseau, identifiez le commutateur le plus approprié pour être la racine de chaque VLAN. Généralement, choisissez un commutateur puissant au milieu du réseau. Placez le pont racine au centre du réseau et connectez directement ce pont aux serveurs et aux routeurs. Cette configuration réduit généralement la distance moyenne des clients aux serveurs et aux routeurs. Référez-vous à Problèmes de protocole STP et considérations de conception associées pour plus d'informations.

Afin de forcer un commutateur pour qu'il soit la racine d'un VLAN désigné, émettez cette commande :

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

Spanning-tree PortFast

PortFast ignore le fonctionnement Spanning Tree normal sur les ports d'accès, afin d'accélérer les retards de connectivité initiale qui se produisent lorsque des stations sont connectées à un commutateur. Pour plus d'informations sur PortFast, reportez-vous à Utilisation de PortFast et d'autres commandes pour corriger les retards de connectivité au démarrage de la station de travail .

Activez STP PortFast pour tous les ports d'accès connectés à un hôte. Voici un exemple :

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet3/1 but will only have effect
when the interface is in a non-trunking mode.
```

UDLD

Activez UDLD seulement sur les ports de l'infrastructure fibre ou sur les câbles Ethernet cuivre afin de contrôler la configuration physique des câbles. Émettez ces commandes afin d'activer UDLD :

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#udld enable
```

Informations de configuration de VLAN

Configurez les VLAN avec ces commandes :

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

Répétez les commandes pour chaque VLAN, puis quittez. Émettez la commande suivante :

```
Cat6500(config)#exit
```

Émettez cette commande afin de vérifier tous les VLAN :

```
Cat6500#show vlan
```

SVI routés

Configurez les SVI pour le routage interVLAN. Émettez les commandes suivantes :

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
```

```
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

Répétez ces commandes pour chaque fonction d'interface contenant un SVI routé, puis quittez. Émettez la commande suivante :

```
Cat6500(config-if)#^Z
```

Interface physique simple routée

Émettez ces commandes afin de configurer l'interface routée par défaut de couche 3 :

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

Répétez ces commandes pour chaque fonction d'interface contenant une interface physique routée, puis quittez. Émettez la commande suivante :

```
Cat6500(config-if)#^Z
```

EtherChannel routés (L3)

Afin de configurer l'EtherChannel sur des interfaces de la couche 3, émettez les commandes de cette section.

Configurez une interface port-canal logique de cette façon :

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

Exécutez les étapes décrites dans cette section pour les ports qui forment ce canal particulier. Appliquez les autres informations au canal de port, comme l'illustre cet exemple :

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

Remarque : après avoir configuré un EtherChannel, la configuration que vous appliquez à l'interface de canal de port affecte l'EtherChannel. La configuration que vous appliquez aux ports LAN affecte uniquement le port LAN auquel vous appliquez la configuration.

EtherChannel (L2) avec la liaison de jonction

Configurez l'EtherChannel de la couche 2 pour la liaison de jonction de cette façon :

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Exécutez les étapes décrites dans cette section uniquement pour les ports qui forment ce canal particulier.

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Remarque : après avoir configuré un EtherChannel, la configuration que vous appliquez à l'interface de canal de port affecte l'EtherChannel. La configuration que vous appliquez aux ports LAN affecte uniquement le port LAN auquel vous appliquez la configuration.

Vérifiez la création de tous les EtherChannels et de toutes les jonctions. Voici un exemple :

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

Ports d'accès

Si la fonction d'interface est un port d'accès configuré en tant qu'interface unique, émettez ces commandes :

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

Répétez ces commandes pour chaque interface qui doit être configurée comme port de commutation de la couche 2.

Si le port de commutation doit être connecté aux stations d'extrémité, émettez cette commande :

```
Cat6500(config-if)#spanning-tree portfast
```

Port de jonction (interface physique simple)

Si la fonction d'interface est un port de jonction configuré en tant qu'interface unique, émettez ces commandes :

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport
```

```
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

Répétez ces commandes pour chaque fonction d'interface qui doit être configurée comme port de jonction.

Informations relatives aux mots de passe

Émettez ces commandes pour les informations relatives aux mots de passe :

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password

CbrCat6500(config)#line con 0
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

Enregistrez la configuration

Émettez cette commande afin de sauvegarder la configuration :

```
Cat6500#copy running-config startup-config
```

Nouvelles fonctionnalités logicielles dans le Logiciel Cisco IOS Version 12.1(13)E

Référez-vous à Configuration du support de téléphone IP Cisco pour plus d'informations sur le support de téléphone sur IP.

Référez-vous à l'identification des applications de réseau et à l'identification des applications de réseau distribuée pour plus d'informations sur le Network-Based Application Recognition (NBAR) pour des ports de réseau local.

Remarques :

- NBAR pour des ports de réseau local est supporté dans le logiciel sur MSFC2.
- PFC2 fournit la prise en charge de matériel pour les listes de contrôle d'accès en entrée sur des ports de réseau local sur lesquels vous configurez NBAR.
- Quand PFC QoS est activé, le trafic sur les ports de réseau local sur lesquels vous configurez NBAR passe par les files d'attente d'entrée et de sortie et les seuils de baisse.
- Quand PFC QoS est activé, MSFC2 place le CoS (classe de service) de sortie égal à la précédence de sortie IP.
- Après le passage du trafic dans une file d'attente d'entrée, tout le trafic est traité dans le logiciel sur MSFC2 sur des ports de réseau local sur lesquels vous configurez NBAR.
- NBAR distribué est disponible sur les interfaces FlexWAN avec le Logiciel Cisco IOS Version 12.1(6)E et versions ultérieures.

Les améliorations de l'exportation des données Netflow (NDE) incluent :

- Interface source-destination et masques de flux d'interface
- NDE version 5 du PFC2
- Netflow échantillonné
- Une option permettant d'alimenter de ces zones supplémentaires dans les enregistrements NDE :Adresse IP du routeur du prochain sautInterface d'entrée (ifIndex SNMP)Interface de sortie (ifIndex SNMP)Numéro de système autonome source

Référez-vous à Configuration de NDE pour plus d'informations sur ces améliorations.

D'autres améliorations de fonctionnalités incluent :

- Configuration de UDLD
- Configuration de VTP
- Configuration des services de cache web utilisant WCCP

Ces commandes sont de nouvelles commandes :

- **standby delay minimum reload**
- **link debounce**
- **vlan internal allocation policy {ascending | décroissant}**
- **system jumbomtu**
- **clear catalyst6000 traffic-meter**

Ces commandes sont des commandes améliorées :

- **show vlan internal usage - Cette commande a été améliorée pour inclure les VLAN utilisées par les interfaces WAN.**
- **show vlan id - Cette commande a été améliorée pour supporter l'entrée d'une plage de VLAN.**
- **show l2protocol-tunnel - Cette commande a été améliorée pour supporter l'entrée d'une identification de VLAN**

Le logiciel Cisco IOS Version 12.1(13)E supporte ces fonctionnalités logicielles, qui ont été précédemment supportées dans les versions EX du logiciel Cisco IOS Version 12.1 :

- Configuration des EtherChannels de la couche 2 qui incluent des interfaces sur différents modules de commutation DFCRéférez-vous aux oppositions générales résolues dans la section consacrée à la version 12.1(13)E de l'ID de bogue Cisco CSCdt27074 (clients inscrits uniquement).
- Redondance RPR+ (Route Processor Redundancy Plus)Référez-vous à Configuration de la redondance de Supervisor Engine RPR ou RPR+.**Remarque :** dans le logiciel Cisco IOS Version 12.1(13)E et ultérieure, les fonctions de redondance RPR et RPR+ remplacent la redondance EHSA (High System Availability) améliorée.
- VLAN de couche 2 4096Référez-vous à Configuration de VLAN.**Remarque : la** version 12.1(13)E et les versions ultérieures du logiciel Cisco IOS prennent en charge la configuration de 4 096 interfaces VLAN de couche 3. Configurez un total combiné de 2 000 interfaces VLAN de couche 3 et ports de couche 3 sur une carte MSFC2 avec un Supervisor Engine II ou un Supervisor Engine I. Configurez un total combiné d'au plus 1 000 interfaces VLAN de couche 3 et ports de couche 3 sur un MSFC.
- Transmission tunnel IEEE 802.1QRéférez-vous à Configuration de la transmission tunnel IEEE 802.1Q et du protocole de couche 2.

- Transmission tunnel du protocole IEEE 802.1QRéférez-vous à Configuration de la transmission tunnel IEEE 802.1Q et du protocole de couche 2.
- IEEE 802.1s MST (Multiple Spanning-Tree)Reportez-vous à Configuration de STP et de IEEE 802.1s MST.
- IEEE 802.1w Rapid STP (RSTP)Reportez-vous à Configuration de STP et de IEEE 802.1s MST.
- IEEE 802.3ad LACPReportez-vous à Configuration d'EtherChannel de couche 2 et 3.
- Filtrage PortFast BPDUReportez-vous à Configuration des fonctionnalités STP.
- Création automatique d'interfaces VLAN 3 pour la prise en charge des ACL VLAN (VACL)Reportez-vous à Configuration de la sécurité réseau.
- Ports de capture VACL qui peuvent être n'importe quel port Ethernet de la couche 2 de tout VLANReportez-vous à Configuration de la sécurité réseau.
- Taille MTU configurable sur les ports de la couche physique individuelle de la couche 3Reportez-vous à Présentation de la configuration d'interfaces.
- Configuration des ports de destination SPAN en tant que jonctions réseau, de sorte que tout le trafic SPAN soit baliséReportez-vous à Configuration des SPAN locaux et distants.

Informations connexes

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