Pratiques recommandées pour la configuration et la gestion des commutateurs Catalyst 4500/4000, 5500/5000 et 6500/6000 s'exécutant sous CatOS

Contenu

Introduction

Ce document traite de la mise en place de commutateurs Cisco de la gamme Catalyst sur votre réseau, spécifiquement les plates-formes Catalyst 4500/4000, 5500/5000 et 6500/6000. Les configurations et les commandes sont discutées dans la supposition que vous exécutez le logiciel de déploiement général pour Catalyst OS (CatOS) 6.4(3) ou ultérieur. Bien que quelques considérations de conception soient présentées, ce document ne couvre pas le modèle campus global.

Conditions préalables

Conditions requises

Ce document suppose la connaissance des références de commandes 7.6 de la gamme Catalyst 6500.

Bien que des références additionnelles à la documentation publique en ligne soient fournies dans tout le document, ce sont d'autres références fondamentales et informatives :

- Cisco ISP Essentials - Fonctionnalités d'IOS essentielles que chaque ISP devrait considérer.
- Directives Cisco de surveillance de réseau et de corrélation d'événements
- Conception de réseau Gigabit Campus - Principes et architecture
- COFFRE-FORT de Cisco : Un modèle de sécurité pour des réseaux d'entreprise

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Ces solutions représentent des années d'expérience sur le terrain des ingénieurs Cisco travaillant avec plusieurs de nos plus grands clients et réseaux complexes. Par conséquent, ce document souligne les configurations réelles qui assurent la réussite des réseaux. Ce document offre les solutions suivantes :

- Des solutions qui ont statistiquement l'exposition la plus large sur le terrain et sont ainsi à plus faible risque.
- Des solutions simples qui sacrifient de la flexibilité pour des résultats déterministes.
- Des solutions faciles à gérer et configurées par des équipes d'exploitation du réseau.

- Des solutions qui favorisent la forte disponibilité et la forte stabilité.

Ce document est divisé en ces quatre sections :

- Configuration de base - fonctionnalités utilisées par une majorité de réseaux tels que le spanning-tree protocol (STP) et la liaison de jonction.
- Configuration de gestion - considérations de conception avec surveillance du système et des événements utilisant le Protocole de gestion de réseau simple (SNMP), le Support de contrôle à distance (RMON), le Syslog, le Cisco Discovery Protocol (CDP) et le Protocole d'Heure Réseau (NTP).
- Configuration de la sécurité - mots de passe, sécurité de port, sécurité physique et authentification utilisant TACACS+.
- Liste de contrôle de la configuration - résumé des modèles de configuration suggérés.

Configuration de base

Les fonctionnalités déployées sur la majorité des réseaux Catalyst sont traitées dans cette section.

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 de ces protocoles est utile pour aborder chacune de ces sections.

Trafic de supervision

La plupart des fonctionnalités activées sur un réseau Catalyst nécessitant la coopération de deux commutateurs ou plusieurs, il doit y avoir un échange contrôlé des messages keepalive, des paramètres de configuration et des modifications de gestion. Que ces protocoles soient propriétaires Cisco, comme le CDP, ou basés sur des normes, comme l'IEEE 802.1d (STP), tous ont certains éléments en commun une fois mis en application sur la gamme Catalyst.

Dans la transmission de trames de base, les trames de données utilisateur proviennent des systèmes d'extrémité et leur adresse source et adresse de destination ne sont pas changées dans les différents domaines commutés de la couche 2 (L2). Les tables de conversion à mémoire associative (CAM) situées sur chaque commutateur Supervisor Engine sont peuplées par un processus d'apprentissage de l'adresse source et indiquent quel port de sortie doit expédier chaque trame reçue. Si le processus d'apprentissage d'adresse est inachevé (la destination est inconnue ou la trame est destinée à une diffusion ou à une adresse multicast), il est transmis (inondé) par tous les ports dans ce VLAN.

Le commutateur doit également identifier les trames à commuter dans le système et celles qui doivent être dirigées au CPU du commutateur lui-même (également connu sous le nom de processeur de gestion de réseau [NMP]).

Le panneau de contrôle Catalyst est créé en utilisant des entrées spéciales dans la table CAM appelées les **entrées système** afin de recevoir et diriger le trafic au NMP sur un port de commutation interne. Ainsi, à l'aide des protocoles dotés d'adresses MAC de destination bien connues, le trafic du panneau de contrôle peut être séparé du trafic de données. Émettez une commande show cam system sur un commutateur pour confirmer ceci, comme indiqué :

```
>show cam system

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -----------------    -----  ----------------------------------------
1     00-d0-ff-88-cb-ff  #          1/3
!--- NMP internal port. 1 01-00-0c-cc-cc-cc # 1/3 !--- CDP and so on. 1 01-00-0c-cc-cc-cd # 1/3
!--- Cisco STP. 1 01-80-c2-00-00-00 # 1/3 !--- IEEE STP. 1 01-80-c2-00-00-01 # 1/3 !--- IEEE
flow control. 1 00-03-6b-51-e1-82 R# 15/1 !--- Multilayer Switch Feature Card (MSFC) router. ...
```

Cisco a une gamme limitée d'adresses Ethernet MAC et de protocoles, comme indiqué. Chacune est couverte plus tard dans ce document. Cependant, un récapitulatif est présenté dans ce tableau pour un aperçu rapide.

Caractéristique	Type de protocole SNAP HDLC	Adresse MAC multipoint de destination
Protocole d'agrégation de ports (PAgP)	0x0104	01-00-0c-cc-cc-cc
Spanning-tree PVSTP+	0x010b	01-00-0c-cc-cc-cd
Pont VLAN	0x010c	01-00-0c-cd-cd-ce
Unidirectional Link Detection (UDLD)	0x0111	01-00-0c-cc-cc-cc
Cisco Discovery Protocol	0x2000	01-00-0c-cc-cc-cc
Dynamic Trunking (DTP)	0x2004	01-00-0c-cc-cc-cc
STP Uplink Fast	0x200a	01-00-0c-cd-cd-cd
IEEE Spanning Tree 802.1d	NON APPLICABLE - DSAP 42 SSAP 42	01-80-c2-00-00-00
Liaison d'intercommutation (ISL)	S/O	01-00-0c-00-00-00
VLAN Trunking (VTP)	0x2003	01-00-0c-cc-cc-cc
IEEE Pause, 802.3x	NON APPLICABLE - DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

La majorité des protocoles de contrôle Cisco utilisent une encapsulation SNAP IEEE 802,3, y compris **LLC 0xAAAA03, OUI 0x00000C**, qui peut être vu sur un traçage d'analyseur LAN. Ces protocoles ont d'autres propriétés communes, dont :

- Ces protocoles assument la connectivité point par point. Notez que l'utilisation délibérée d'adresses de destination multicast permet à deux Catalyst de communiquer d'une manière

transparente via des commutateurs non Cisco, car les périphériques qui ne comprennent pas et interceptent les trames les inondent simplement. Cependant, les connexions point-à-multipoint dans des environnements pluri-constructeurs peuvent avoir comme conséquence un comportement contradictoire et doivent généralement être évitées.
- Ces protocoles se terminent sur des routeurs de couche 3 (L3) ; ils fonctionnent seulement dans un environnement de commutateurs.
- 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).

Après l'introduction des adresses de destination du protocole de contrôle, l'adresse source doit également être renseignée. Les protocoles de commutateurs utilisent une adresse MAC tirée d'une banque d'adresses disponibles fournie par une EPROM sur le châssis. Émettez la commande show module afin d'afficher la plage d'adresses disponibles pour chaque module quand il recherche du trafic comme des unités de données des protocoles BDPU ou des trames ISL.

```
>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
!--- MACs for sourcing traffic. ... VLAN 1
```

VLAN 1

VLAN 1 a une importance spéciale dans les réseaux Catalyst.

Catalyst Supervisor Engine emploie toujours le VLAN par défaut, VLAN 1, pour marquer un certain nombre de protocoles de contrôle et de gestion lors d'une agrégation, comme le CDP, le VTP et le PAgP. Tous les ports, y compris l'interface sc0 interne, sont configurés par défaut pour être des membres du VLAN 1. Toutes les liaisons portent VLAN 1 par défaut, et dans les versions du logiciel CatOS antérieures à 5.4, il n'était pas possible de bloquer les données utilisateur dans le VLAN 1.

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

- sc0 réside dans le VLAN de gestion ; ce VLAN peut être changé.
- Le VLAN natif est défini comme VLAN auquel un port retourne quand aucune agrégation n'est en cours et est le VLAN non balisé sur une liaison 802.1Q. Par défaut, VLAN 1 est le VLAN natif.
- Afin de changer le VLAN natif, émettez la commande set vlan *vlan-id mod/port* .**Remarque:** Créez le VLAN avant de le définir comme VLAN natif de la liaison.

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. Ceci est abordé plus en détails dans la section Gestion intrabande de ce document.

- Les données de panneau de contrôle sur le VLAN 1 doivent être gardées séparément des données utilisateur afin de simplifier le dépannage et de maximiser les cycles CPU disponibles.
- Les boucles L2 dans le VLAN 1 doivent être évitées quand des réseaux multicouche-campus sont conçus sans STP et l'agrégation est nécessaire à la couche d'accès s'il y a plusieurs sous-réseaux VLAN et IP. Pour cela, retirez manuellement 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 est effacé des liaisons réseau et n'est pas le VLAN natif. Si VLAN 1 est effacé pour des données utilisateur, cela n'a aucune incidence sur le trafic de panneau de contrôle qui continue à être transmis à l'aide de VLAN 1.
- Sur une liaison ISL, les paquets DTP sont envoyés sur VLAN1. C'est le cas même si VLAN 1 est 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 est effacé de la liaison.
- Dans PVST+, les **802.1Q IEEE BPDUs** sont expédiés sans balise sur le Spanning Tree VLAN1 commun pour une interopérabilité avec d'autres constructeurs, à moins que VLAN 1 ne soit 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. Référez-vous à la section Protocole Spanning Tree de ce document pour plus de détails.
- 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 est effacé des liaisons.
- N'effacez pas et ne désactivez pas VLAN 1 sur les liaisons entre des ponts MST et des ponts PVST+. 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.

Recommandations

Afin de maintenir un VLAN dans un état **up/up** sans client ou serveur connecté dans ce VLAN, vous devez avoir au moins un périphérique physique connecté dans ce VLAN. Autrement, le VLAN a un état **actif/inactif** . Actuellement, il n'existe aucune commande pour mettre une interface VLAN en état **actif/actif** quand il n'y a aucun port actif dans le commutateur pour ce VLAN.

Si vous ne voulez pas connecter un périphérique, connectez un connecteur de bouclage dans n'importe quel port de ce VLAN. Comme alternative, essayez un câble croisé qui connecte deux ports dans ce VLAN sur le même commutateur. Cette méthode force le port à être actif. Référez-vous à la section Connecteur de bouclage des Tests de bouclage local pour des lignes T1/56K pour plus d'informations.

Quand un réseau est multiconnecté aux fournisseurs de service, le réseau agit comme un réseau de transit entre deux fournisseurs de service. Si le numéro de VLAN reçu dans un paquet doit être traduit ou modifié lorsqu'il est passé d'un fournisseur de service à un autre fournisseur de service, il est recommandé d'employer la fonctionnalité QinQ afin de traduire le numéro de VLAN.

VLAN Trunking Protocol

Avant de créer des VLAN, déterminez le mode VTP à utiliser sur le réseau. VTP permet d'effectuer des modifications de configuration VLAN centralement sur un ou plusieurs

commutateurs. Ces changements se propagent automatiquement à tous les autres commutateurs du domaine.

Aperçu opérationnel

Le VTP est un protocole de messagerie L2 qui maintient la cohérence de la configuration VLAN. VTP gère l'ajout, la suppression et le changement de nom des VLAN à l'échelle du réseau entier. VTP réduit au minimum les erreurs et les incohérences de configuration qui peuvent poser un certain nombre de problèmes, tels que des noms de VLAN en double, des spécifications incorrectes de type de VLAN et des violations de la sécurité. La base de données VLAN est un fichier binaire et est enregistré dans NVRAM sur des serveurs VTP séparément à partir du fichier de configuration.

Le protocole VTP permet aux commutateurs de communiquer en utilisant une adresse MAC Ethernet de destination multicast (**01-00-0c-cc-cc-cc**) et le protocole SNAP HDLC Ox2003. Cela ne fonctionne pas avec des ports de non-liaison (VTP est une charge utile d'ISL ou de 802.1Q), donc les messages ne peuvent pas être envoyés tant que DTP n'a pas mis la liaison en ligne.

Les types de message incluent des annonces résumées toutes les cinq minutes, des annonces de sous-ensembles et des annonces de requêtes quand il y a des modifications, ainsi que des messages d'enregistrement lorsque l'élagage VTP est activé. Le numéro de révision de configuration VTP est incrémenté d'une unité à chaque modification sur le serveur, ce qui propage alors la nouvelle table à travers le domaine.

Si un VLAN est supprimé, les ports qui étaient auparavant membres de ce VLAN sont placés dans un 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.

Cette table fournit un résumé comparatif des fonctionnalités pour divers modes VTP :

Caractéristique	Serveur	Client	Transparent	Outre de[1]
Messages VTP sources	Oui	Oui	Non	Non
Écouter les messages VTP	Oui	Oui	Non	Non
Transférer les messages VTP	Oui	Oui	Oui	Non
Créer des VLAN	Oui	Non	Oui (significatif uniquement localement)	Oui (significatif uniquement localement)
Rappeler les VLAN	Oui	Non	Oui (significatif uniquement localement)	Oui (significatif uniquement localement)

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

[1] version de logiciel 7.1 de CatOS introduit l'option de désactiver le VTP avec l'utilisation `hors fonction du` mode. En mode VTP off , le commutateur se comporte de manière semblable au mode VTP transparent , sauf que le mode off supprime également le transfert des mises à jour VTP.

Cette table fournit un récapitulatif de la configuration initiale :

Caractéristique	Valeur par défaut
Nom de domaine VTP	Null
Mode VTP	Serveur
Version VTP	La version 1 est activée
Mot de passe VTP	Aucun
Élagage VTP	Handicapé

Le VTP version 2 (VTPv2) inclut cette flexibilité fonctionnelle. Cependant, il n'est pas interopérable avec le VTP version 1 (VTPv1) :

- Prise en charge de Token Ring
- Prise en charge des information VTP non reconnues ; les commutateurs peuvent maintenant propager des valeurs qu'ils ne peuvent pas analyser.
- Mode transparent dépendant de la version ; le mode transparent ne vérifie 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 peuvent être activés par configuration d'un commutateur unique.

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

VTP Version 3

Le logiciel CatOS version 8.1 introduit la prise en charge du VTP version 3 (VTPv3). VTPv3 fournit des améliorations par rapport aux versions actuelles. Ces améliorations permettent :

- La prise en charge des VLAN étendus
- La prise en charge de la création et de la publicité des VLAN privés
- La prise en charge des instances de VLAN et des instances de propagation du mappage MST (qui sont pris en charge dans CatOS version 8.3)
- L'authentification de serveur améliorée
- La protection contre la mise en place accidentelle d'une « mauvaise » base de données dans un domaine VTP.
- L'interaction avec VTPv1 et VTPv2
- La capacité d'être configuré sur une base par port

Une des principales différences entre la mise en oeuvre VTPv3 et la version antérieure est

l'introduction d'un serveur principal de VTP. Dans le meilleur des cas, il doit y avoir seulement un serveur principal dans un domaine VTPv3 si le domaine n'est pas partitionné. Toutes les modifications que vous apportez au domaine VTP doivent être exécutées sur le serveur VTP principal afin d'être propagées au domaine VTP. Il peut y avoir plusieurs serveurs dans un domaine VTPv3, qui sont également connus en tant que serveurs secondaires. Quand un commutateur est configuré pour être un serveur, il devient un serveur secondaire par défaut. Le serveur secondaire peut enregistrer la configuration du domaine mais ne peut pas la modifier. Un serveur secondaire peut devenir un serveur principal grâce à une prise de contrôle réussie à partir du commutateur.

Les commutateurs qui exécutent VTPv3 acceptent seulement une base de données VTP avec un numéro de révision plus élevé que celui du serveur principal actuel. Ce processus diffère de manière significative de VTPv1 et de VTPv2, dans lesquels un commutateur accepte toujours une configuration supérieure d'un voisin situé dans le même domaine. Cette modification avec VTPv3 assure une protection. Un nouveau commutateur qui est introduit dans le réseau avec un numéro de révision VTP plus élevé ne peut pas remplacer la configuration VLAN du domaine tout entier.

Le VTPv3 introduit également une amélioration de la façon dont le VTP gère les mots de passe. Si vous utilisez l'option de configuration du mot de passe masqué afin de configurer un mot de passe comme « masqué », ces événements se produisent :

- Le mot de passe n'apparaît pas en texte seul dans la configuration. Le format hexadécimal secret du mot de passe est enregistré dans la configuration.
- Si vous essayez de configurer le commutateur en tant que serveur principal, le mot de passe vous est demandé. Si votre mot de passe correspond au mot de passe secret, le commutateur devient un serveur principal, ce qui vous permet de configurer le domaine.

Remarque: Il est important de noter que le serveur principal est seulement nécessaire quand vous avez besoin de modifier la configuration VTP configuration pour une instance. Un domaine VTP peut fonctionner sans aucun serveur principal actif parce que les serveurs secondaires assurent la persistance de la configuration à chaque rechargement. L'état de serveur principal est quitté pour ces raisons :

- Un rechargement du commutateur
- Une commutation haute disponibilité entre les supervisor engines actifs et redondants
- Une reprise d'un autre serveur
- Un changement de la configuration du mode
- Toute modification de la configuration du domaine VTP, telle qu'une modification de :Versionle nom de domainele mot de passe du domaine

VTPv3 permet également aux commutateurs de participer à plusieurs instances de VTP. Dans ce cas, le même commutateur peut être le serveur VTP pour une instance et client pour une autre instance parce que les modes VTP sont spécifiques à différentes instances de VTP. Par exemple, un commutateur peut fonctionner en mode transparent pour une instance MST alors qu'il est configuré en server mode pour une instance VLAN.

En termes d'interaction avec VTPv1 et VTPv2, le comportement par défaut dans toutes les versions de VTP a été que les versions antérieures de VTP suppriment simplement les nouvelles mises à jour de version. À moins que les commutateurs VTPv1 et VTPv2 soient en mode transparent , toutes les mises à jour VTPv3 sont abandonnées. En revanche, une fois que les commutateurs VTPv3 ont hérité d'une trame VTPv1 ou VTPv2 sur une liaison, les commutateurs transmettent une version réduite de leur mise à jour de base de données aux commutateurs VTPv1 et VTPv2. Cependant, cet échange d'informations est unidirectionnel dans le sens

qu'aucune mise à jour des commutateurs VTPv1 et VTPv2 n'est acceptée par les commutateurs VTPv3. Sur des connexions de liaison, les commutateurs VTPv3 continuent à envoyer les mises à jour réduites aussi bien que les véritables mises à jour VTPv3 afin de répondre à l'existence d'un voisinage VTPv2 et VTPv3 à travers les ports de liaison.

Afin de fournir une prise en charge VTPv3 pour VLAN étendus, le format de la base de données VLAN dans lequel le VTP assigne 70 octets par VLAN est modifié. La modification permet uniquement le codage des valeurs autres que par défaut et non le transport des champs non modifiés pour les protocoles traditionnels. En raison de cette modification, la prise en charge du VLAN 4K est la taille de la base de données VLAN en résultant.

Recommandation

Il n'existe aucune recommandation spécifique dans le choix du mode client/serveur VTP ou VTP transparent. Quelques clients préfèrent la facilité de gestion du VTP client/server mode en dépit de quelques considérations mentionnées plus loin. La recommandation est d'avoir deux commutateurs en server mode dans chaque domaine pour la redondance, généralement les deux commutateurs de la couche distribution. Le reste des commutateurs du domaine doit être défini sur client mode. Quand vous mettez en oeuvre client/server mode avec l'utilisation de VTPv2, soyez conscient qu'un numéro de révision plus élevé est toujours accepté dans le même domaine VTP. Si un commutateur qui est configuré en mode VTP client 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 s'assurer que les commutateurs client ou serveur ont toujours un numéro de révision de configuration inférieur à celui du serveur, donnez au domaine VTP client un nom différent du nom standard. Retournez alors de nouveau au 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 l'approche prudente du mode VTP transparent pour les raisons suivantes :

- Elle encourage la bonne pratique en matière de contrôle de modification, car la modification d'un VLAN sur commutateur ou port de liaison doit être effectuée commutateur par commutateur.
- Elle limite le risque d'une erreur d'administrateur qui affecte le domaine tout entier, comme la suppression d'un VLAN accidentellement.
- 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.
- Elle encourage les VLAN à être séparés des liaisons joignant des commutateurs qui n'ont pas de ports dans ce VLAN. Cela optimise l'utilisation de la bande passante lors de l'inondation de trames. L'élagage manuel est également salutaire parce qu'il réduit le diamètre du spanning tree (voir la section DTP de ce document). Avant d'élaguer des VLAN inutilisés sur les liaisons de canal de port, assurez-vous que tous les ports connectés aux téléphones IP sont configurés comme ports d'accès avec VLAN voix.
- La plage VLAN étendue dans CatOS 6.x et CatOS 7.x, les numéros 1025 à 4094, peut seulement être configurée de cette façon. Pour plus d'information, voyez la section Réduction des adresses VLAN et MAC étendues de ce document.
- Le mode VTP transparent est pris en charge dans Campus Manager 3.1, qui fait partie de

Cisco Works 2000. La vieille restriction qui nécessitait au moins un serveur dans un domaine VTP a été retirée.

Exemples de commandes VTP	Commentaires
set vtp domain name password x	CDP contrôle les noms afin de détecter un mauvais câblage entre les domaines. Un mot de passe simple est une précaution utile contre les modifications involontaires. Prenez garde des noms sensibles à la casse ou des espaces si vous faites un copier-coller.
set vtp mode transparent	
set vlan vlan number name name	Par commutateur qui a des ports dans le VLAN.
set trunk mod/port vlan range	Permet aux liaisons de transporter des VLAN si nécessaire - la valeur par défaut est tous les VLAN.
clear trunk mod/port vlan range	Limite le diamètre STP par élagage manuel, comme sur les liaisons entre la couche de distribution er la couche d'accès, où le VLAN n'existe pas.

Remarque: En spécifiant des VLAN avec la commande **set** , vous ajoutez seulement des VLAN, vous ne les effacez pas. Par exemple, la commande set trunk x/y 1-10 ne définit pas la liste autorisée seulement aux VLAN 1-10. Émettez la commande clear trunk x/y 11-1005 pour atteindre le résultat désiré.

Bien que la commutation Token Ring ne soit pas couverte dans ce document, notez que le mode VTP transparent n'est pas recommandé pour les réseaux TR-ISL. La base de la commutation Token Ring est que l'ensemble du domaine forme un pont multiport distribué simple, donc chaque commutateur doit avoir les mêmes informations de VLAN.

Autres options

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

VTPv3 fournit la capacité de mettre en oeuvre une authentification et un contrôle de révision de configuration plus stricts. VTPv3 fournit essentiellement le même niveau de fonctionnalité, mais avec la sécurité optimisée qu'offre le mode VTPv1/VTPv2 transparent . En outre, VTPv3 est partiellement compatible avec les versions VTP traditionnelles.

Les avantages de l'élagage de VLAN pour réduire l'inondation inutile des trames sont présentés dans ce document. La commande d'enable de set vtp pruning taille des VLAN automatiquement, qui arrête l'inondation inefficace des trames où elles ne sont pas nécessaires. À la différence de l'élagage manuel de VLAN, l'élagage automatique ne limite pas le diamètre du spanning tree.

Àpartir de CatOS 5.1, les commutateurs Catalyst peuvent associer des numéros de VLAN 802.1Q plus grands que 1000 aux numéros de VLAN ISL. Dans CatOS 6.x, les commutateurs Catalyst 6500/6000 prennent en charge les VLAN 4096 selon la norme IEEE 802.1Q. Ces VLAN sont organisés en trois plages, dont certaines seulement sont propagées à d'autres commutateurs du réseau avec VTP :

- VLAN à plage normale : 1 – 1001
- VLAN à plage étendue : 1025 - 4094 (peut seulement être propagé par VTPv3)
- VLAN à plage réservée : 0, 1002 — 1024, 4095

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

Remarque: CatOS 7.x introduit la possibilité de définir VTP en mode off, mode très semblable à transparent. Cependant, le commutateur ne transfère pas les trames VTP. Ceci peut être utile dans quelques conceptions quand vous établissez une liaison à des commutateurs en dehors de votre contrôle administratif.

Réduction des adresses VLAN et MAC étendues

Le programme de réduction des adresses MAC active l'identification des VLAN à plage étendue. L'activation de la réduction des adresses MAC désactive le pool d'adresses MAC utilisées par le Spanning Tree du VLAN et laisse une adresse MAC unique. Cette adresse MAC identifie le commutateur. Le logiciel CatOS version 6.1(1) introduit la prise en charge de la réduction des adresses MAC pour que les commutateurs Catalyst 6500/6000 et Catalyst 4500/4000 prennent en charge les VLAN 4096 conformément à la norme IEEE 802.1Q.

Aperçu du fonctionnement

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+. Les commutateurs Catalyst 6500/6000 et Catalyst 4500/4000 prennent en charge les adresses MAC 1024 ou 64, selon le type de châssis.

Les commutateurs Catalyst avec des adresses MAC 1024 n'activent pas la réduction des adresses MAC par défaut. Les adresses MAC sont allouées séquentiellement. La première adresse MAC de la plage est allouée à VLAN 1. La seconde adresse MAC de la plage est allouée

à 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	64[1]
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	64[1]

[1] réduction d'adresse MAC est activée par défaut pour les Commutateurs qui ont 64 adresses MAC, et la caractéristique ne peut pas être désactivée.

Pour les commutateurs de la gamme Catalyst avec des adresses MAC 64, une activation de la réduction des adresses MAC permet aux VLAN 4096 qui exécutent PVST+ ou 16 instances STP multiples (MISTP) d'avoir des identifiants uniques sans augmentation dans le nombre d'adresses MAC nécessaires sur le commutateur. La réduction des adresses MAC réduit le nombre d'adresses MAC requises par le STP d'une par instance de VLAN ou MISTP à une par commutateur.

Cette image montre que la réduction des adresses MAC sur l'identifiant de pont n'est pas activée. L'identifiant de pont se compose d'une priorité de pont à 2 octets et d'une adresse MAC à 6 octets :

La réduction des adresses MAC modifie la partie identifiante du pont STP du BPDU. Le champ de priorité à 2 octets initial est coupé en deux zones. Ce fractionnement a comme conséquence un champ de priorité de pont 4 bits et une extension d'ID système 12 bits qui permet de numéroter les VLAN de 0 à 4095.

Quand la réduction des adresses MAC est activée sur les commutateurs Catalyst afin d'exploiter des VLAN à plage étendue, activez la réduction des adresses MAC sur tous les commutateurs dans le même domaine. Cette étape est nécessaire afin de maintenir la cohérence des calculs de racine STP sur tous les commutateurs. Une fois que vous avez activé la réduction des adresses MAC, la priorité du pont racine devient un multiple de 4096 plus l'ID VLAN. Les commutateurs sans réduction des adresses MAC peuvent réclamer la racine par accident parce que ces commutateurs ont une granularité plus fine dans la sélection de l'identifiant de pont.

Directives de configuration

Vous devez suivre certaines directives quand vous configurez une plage étendue de VLAN. Le commutateur peut allouer un bloc de VLAN de la plage étendue pour des buts internes. Par exemple, le commutateur peut allouer les VLAN pour les ports routés ou les modules Flex WAN. L'allocation du bloc de VLAN commence toujours à partir du VLAN 1006 et va en augmentant. Si vous avez des VLAN dans la plage que le module Flex WAN exige, tous les VLAN requis ne sont pas alloués parce que les VLAN ne sont jamais alloués à partir de la zone VLAN utilisateur. **Émettez la commande show vlan ou show vlan summary sur un commutateur pour afficher les VLAN assignés à l'utilisateur et internes.**

```
>show vlan summary

Current Internal Vlan Allocation Policy - Ascending

Vlan status    Count  Vlans
-------------  -----  -----------------------------------------
VTP Active         7   1,17,174,1002-1005

Internal           7   1006-1011,1016
!--- These are internal VLANs. >show vlan
---- -------------------------------- --------- ------- --------

1    default                          active    7       4/1-48


!--- Output suppressed. 1006 Online Diagnostic Vlan1 active 0 internal 1007 Online Diagnostic
Vlan2 active 0 internal 1008 Online Diagnostic Vlan3 active 0 internal 1009 Voice Internal Vlan
active 0 internal 1010 Dtp Vlan active 0 internal 1011 Private Vlan Internal Vlan suspend 0
internal 1016 Online SP-RP Ping Vlan active 0 internal !--- These are internal VLANs.
```

En outre, avant d'utiliser les VLAN à plage étendue, vous devez supprimer tous les tracés 802.1Q-to-ISL existants. De plus, dans les versions antérieures à VTPv3, vous devez statiquement configurer le VLAN étendu sur chaque commutateur avec l'utilisation du mode VTP transparent. Référez-vous à la section *Directives de configuration des VLAN à plage étendue* de Configuration des VLAN pour plus d'informations.

Remarque: Dans les versions du logiciel antérieures à 8.1(1), vous ne pouvez pas configurer le nom du VLAN pour des VLAN à plage étendue. Cette capacité est indépendante de la version ou du mode VTP.

Recommandation

Essayez de maintenir une configuration cohérente pour la réduction des adresses MAC au sein du même domaine. Cependant, l'application de la réduction des adresses MAC sur tous les périphériques réseau peut être impraticable quand de nouveaux châssis avec des adresses MAC 64 sont introduits dans le domaine STP. La réduction des adresses MAC est activée par défaut pour les commutateurs qui ont des adresses MAC 64, et la fonctionnalité ne peut pas être désactivée. Comprenez que, quand deux systèmes sont configurés avec la même priorité de Spanning Tree, le système qui n'a pas de réduction des adresses MAC a une meilleure priorité de Spanning Tree. Émettez cette commande afin d'activer ou désactiver la réduction des adresses MAC :

```
set spantree macreduction enable | disable
```

L'allocation des VLAN internes se fait en ordre croissant et commence à VLAN 1006. Assignez les

VLAN utilisateur aussi près de VLAN 4094 que possible afin d'éviter des conflits entre les VLAN utilisateur et les VLAN internes. Avec les commutateurs Catalyst 6500 qui exécutent le logiciel système Cisco IOS®, vous pouvez configurer l'allocation interne de VLAN dans l'ordre décroissant. L'équivalent d'interface de ligne de commande (CLI) pour CatOS n'est pas officiellement pris en charge.

Négociation automatique

Ethernet/Fast Ethernet

L'autonégociation est une fonction optionnelle de la norme Fast Ethernet IEEE (802.3u) qui permet à des périphériques d'échanger automatiquement des informations sur une liaison au sujet des capacités de **débit et de duplex** . L'autonégociation se déroule à la couche 1 (L1) et cible les ports de la couche d'accès où **les utilisateurs transitoires** comme les PC se connectent au réseau.

Aperçu opérationnel

L'un des problèmes les plus communs de performance sur les liaisons Ethernet 10/100 Mbps/s se produit quand un port sur la liaison fonctionne en mode bidirectionnel à l'alternat tandis que l'autre fonctionne en mode bidirectionnel simultané. Ceci se produit de temps en temps quand un ou les deux ports sur une liaison sont réinitialisés et le processus d'autonégociation ne donne pas la même configuration aux deux partenaires de liaison. Cela se produit également quand des administrateurs reconfigurent un côté de la liaison et oublient de reconfigurer l'autre côté. Les symptômes typiques de cela sont l'augmentation de la séquence de contrôle de trame (FCS), du contrôle de redondance cyclique (CRC), du cadrage ou des compteurs de trames incomplètes sur le commutateur.

L'autonégociation est abordée en détail dans ces documents. Ces documents comportent des explications sur la façon dont l'autonégociation fonctionne et sur la configuration des options.

- Configuration et dépannage de l'autonégociation Ethernet 10/100Mb à alternat et simultanée
- **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 bidirectionnel simultané 100 Mbps/s 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 la conséquence d'un partenaire de liaison qui autonégocie, ne voit aucun paramètre d'autonégociation chez l'autre partenaire de liaison et passe en mode bidirectionnel à alternat.

La plupart des modules Ethernet Catalyst prennent en charge 10/100 Mbps/s et les modes bidirectionnels à alternat et simultanés, mais la commande de capacité de show port mod/port confirme cela.

FEFI

L'indication de panne d'extrémité lointaine (FEFI) protège 100BASE-FX (fibre) et les interfaces Gigabit, alors que l'autonégociation protège 100BASE-TX (cuivre) et empêche la couche physique de signaler les pannes associées.

Un défaut d'extrémité lointaine est une erreur de liaison qu'une station peut détecter alors que

l'autre ne peut pas, comme un câble TX déconnecté. Dans cet exemple, la station émettrice peut encore recevoir des données valides et détecter que la liaison est bonne via le contrôleur d'intégrité de liaison. Elle ne détecte pas que sa transmission n'est pas reçue par l'autre station. 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 (désigné sous le nom de structure FEFI IDLE) pour informer le voisin de la panne distante ; le schéma FEFI-IDLE déclenche ensuite un arrêt du port distant (errdisable). Référez-vous à la section UDLD de ce document pour plus d'informations sur la protection contre les pannes.

FEFI est pris en charge par ce matériel et ces modules :

- Catalyst 5500/5000 : WS-X5201R, WS-X5305, WS-X5236, WS-X5237, WS-U5538 et WS-U5539
- Catalyst 6500/6000 et 4500/4000 : Tous les modules 100BASE-FX et modules GE

Recommandation

Le choix entre la configuration de l'autonégociation sur des liaisons 10/100 et l'encodage de la vitesse et du mode bidirectionnel dépend du type de partenaire de liaison ou du 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, des problèmes peuvent se produire quand le NIC ou les commutateurs du constructeur ne se conforment pas exactement. L'incompatibilité matérielle et d'autres questions peuvent également se poser en raison de fonctions avancées spécifiques au constructeur, telles que l'auto-polarité ou l'intégrité de câblage, qui ne sont pas décrites dans le cahier des charges IEEE 802.3u pour l'autonégociation 10/100 Mbps/s. Référez-vous aux notes de terrain : Problème de performances avec des NIC d'Intel Pro/1000T se connectant à CAT4K/6K pour un exemple de ceci.

Prévoyez qu'il y aura quelques situations qui exigent une configuration de l'hôte, de la vitesse de port et du mode bidirectionnel. Suivez généralement 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 publication de CatOS.
- Vérifiez la version du pilote NIC ou du système d'exploitation que vous exécutez, car le dernier pilote ou le dernier correctif sont souvent requis.

En règle générale, 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 transitoires comme les ordinateurs portables. Dans le meilleur des cas, l'autonégociation fonctionne bien également avec les périphériques non-transitoires tels que les serveurs et les postes de travail fixes ou de commutateur à commutateur et de commutateur à routeur. Pour certaines des raisons mentionnées, des problèmes de négociation peuvent se poser. Dans ces cas, suivez les étapes de dépannage de base mentionnées dans les liens TAC fournis.

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

```
set port speed port range auto
!--- This is the default.
```

Si vous encodez le port, émettez ces commandes de configuration :

set port speed *port range 10 | 100* **set port duplex** *port range full | half*

Dans CatOS 8.3 et ultérieurs, Cisco a introduit le mot clé optionnel **auto-10-100** . Utilisez le mot clé **auto-10-100** sur les ports qui supportent des vitesses de 10/100/1000 Mbps/s mais où l'autonégociation à 1000 Mbps/s est indésirable. L'utilisation du mot clé **auto-10-100** oblige le port à se comporter de la même manière qu'un port 10/100-Mbps/s port dont la vitesse est définie sur **auto**. La vitesse et le mode bidirectionnel sont négociés pour les ports 10/100-Mbps/s seulement, et la vitesse 1000-Mbps/s ne participe pas à la négociation.

set port speed *port_range* **auto-10-100**

Autres options

Quand aucune autonégociation n'est utilisée entre les commutateurs, l'indication de panne L1 peut également être perdue pour certains problèmes. Il est utile d'employer les protocoles L2 pour augmenter la détection de panne, telle que la détection UDLD agressive.

Gigabit Ethernet

L'Ethernet Gigabit (GE) a une procédure d'autonégociation (IEEE 802.3z) qui est plus détaillée que celle de l'Ethernet 10/100 Mbps/s et est utilisé pour échanger des paramètres de régulation de débit, des informations sur une panne distante et des informations sur le mode bidirectionnel (quoique les ports GE de la gamme Catalyst supportent seulement le mode bidirectionnel simultané).

Remarque: 802.3z a été remplacé par des spec. IEEE de 802.3:2000. Référez-vous aux normes IEEE sur l'abonnement aux normes LAN/MAN de ligne : Archives pour plus d'informations.

Aperçu opérationnel

La négociation de port GE est activée par défaut et les ports des deux extrémités d'une liaison GE doivent avoir la même configuration. À la différence du FE, la liaison GE ne peut pas s'établir si la configuration de l'autonégociation diffère sur les ports à chaque extrémité de la liaison. Cependant, la seule condition requise pour qu'un port à autonégociation désactivée établisse une liaison est un signal gigabit valide de l'extrémité lointaine. Ce comportement est indépendant de la configuration de l'autonégociation de l'extrémité lointaine. Par exemple, supposez qu'il y a deux périphériques, A et B. Chaque périphérique peut avoir l'autonégociation activée ou désactivée. Cette table présente une liste des configurations possibles et des états de liaison respectifs :

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.

Remarque: Il y a un dictionnaire des mots valides et tous les mots ne sont pas forcément valides sur 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.

La spécification GE cuivre (1000BASE-T) prend en charge l'autonégociation par Next Page Exchange. Next Page Exchange permet l'autonégociation des vitesses 10/100/1000 Mbps/s sur des ports cuivre.

Remarque: La spécification de la fibre GE prend des dispositions seulement pour la négociation du mode bidirectionnel, du contrôle de flux et de la détection de panne distante. 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 set port sync-restart-delay a seulement un effet quand l'autonégociation est définie sur enable.

Recommandation

Activer l'autonégociation est beaucoup plus important dans un environnement GE que dans un environnement 10/100. En fait, l'autonégociation doit seulement être désactivée sur les ports de commutation qui s'attachent aux périphériques non capables de prendre en charge une négociation ou lorsque des problèmes de connectivité résultent de problèmes d'interopérabilité. Cisco vous recommande d'activer la négociation Gigabit (par défaut) sur toutes les liaisons commutateur-à-commutateur et généralement sur tous les périphériques GE. Émettez cette commande afin d'activer l'autonégociation :

```
set port negotiation port range enable
!--- This is the default.
```

Une exception connue se produit quand il y a une connexion à un routeur de commutation Gigabit (GSR) qui exécute une version du logiciel Cisco IOS antérieure à 12.0(10)S, la version où sont

venus s'ajouter le contrôle de flux et l'autonégociation. Dans ce cas, arrêtez ces deux fonctions, ou les états de port de commutation not connected, et les rapports d'erreurs GSR. Voici un exemple de séquence de commande :

```
set port flowcontrol receive port range off set port flowcontrol send port range off set port negotiation port range disable
```

Les connexions de commutateur-à-commutateur doivent être étudiées au cas par cas. Les clients Cisco ont rencontré des problèmes avec la négociation Gigabit sur des serveurs Sun, HP et IBM.

Autres options

Le contrôle de flux est une partie facultative de la spécification 802.3x et doit être négocié si utilisé. Les périphériques peuvent ou ne peuvent pas être capables d'envoyer et/ou de répondre à une trame PAUSE (**MAC 01-80-C2-00-00-00 0F bien connu**). En outre, ils ne peuvent pas être d'accord sur la demande de contrôle de flux du voisin distant. Un port avec un tampon d'entrée qui se remplit envoie une trame PAUSE à son partenaire de liaison, qui arrête la transmission et retient toutes les trames supplémentaires dans les tampons de sortie du partenaire de liaison. Ceci ne résout aucun problème équilibré de sursouscription, mais rend effectivement le tampon d'entrée plus grand par une certaine fraction de la mémoire tampon de sortie du partenaire durant les rafales de transmission.

Cette fonctionnalité est très 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 leur mémoire virtuelle. L'utilisation du commutateur à commutateur a des avantages limités.

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

```
set port flowcontrol mod/port 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 négociés. Quelques modules (par exemple, WS-X5410, WS-X4306) n'envoient jamais de trames PAUSE même s'ils négocient pour cela, car ils sont non-bloquants.

Dynamic Trunking Protocol

Type d'encapsulation

Les jonctions étendent des VLAN entre les périphériques en identifiant et en marquant temporairement (liaison locale) les trames Ethernet originales, ce qui leur permet d'être multiplexées sur une même liaison. Cela 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.

La jonction est prise en charge sur plusieurs types de médias L2, y compris ATM LANE, FDDI 802,10, et Ethernet, bien que seulement ce dernier soit présenté ici.

Aperçu opérationnel de l'ISL

L'identification ou le schéma de balisage propriétaire Cisco, ISL, est en service depuis de nombreuses années. Le standard IEEE 802.1Q est également disponible.

En encapsulant totalement la trame originale dans un schéma de balisage à deux niveaux, l'ISL est effectivement un protocole de transmission tunnel et a l'avantage supplémentaire des trames de transport non-Ethernet. Il ajoute un en-tête de 26 octets et une FCS de 4 octets à la trame Ethernet standard - les trames Ethernet plus grandes sont prévues et traitées par des ports configurés pour être des jonctions. ISL prend en charge les VLAN 1024.

Format de trame ISL

40 bits	**4 bits**	**4 bits**	**48 bits**	**16 bits**	**24 bits.**	**24 bits.**	**15 bits.**	**Bit**	**16 bits**	**16 bits**	**Longueur variable**	**32 bits**
DEST. Adr	Type	UTILISATEUR	SA	LEN	LLC INSTANTANÉ	A	VLAN	BPDU	INDEX	Réserve	Trame encapsulée	FCS
01-00-0c-00-00					AAAA03	00000C						

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

Aperçu opérationnel du 802.1Q

La norme IEEE 802.1Q spécifie beaucoup plus que des types d'encapsulation, y compris des améliorations de spanning tree et des marquages GARP (voir la section VTP de ce document) et Qualité de service 802.1p (QoS).

Le format de trame 802.1Q préserve l'adresse source et l'adresse de destination Ethernet originales, mais les commutateurs doivent maintenant s'attendre à recevoir des trames baby-giant, même sur des ports d'accès où les hôtes peuvent utiliser un marquage afin d'exprimer la priorité utilisateur 802.1p pour la signalisation QoS. Le marqueur est de 4 octets, ainsi les trames Ethernet v2 802.1Q sont de 1522 octets, une réalisation du groupe de travail IEEE 802.3ac. 802.1Q prend en charge également l'espace de numérotation pour 4096 VLAN.

Toutes les trames de données transmises et reçues portent le marqueur 802.1Q exceptées celles sur le VLAN natif (il y a un marqueur implicite basé sur la configuration du port de commutation d'entrée). Les trames sur le VLAN natif sont toujours transmises sans marqueur et normalement reçues sans marqueur. Cependant, elles peuvent également être reçues marquées.

Référez-vous à Standardisation VLAN via IEEE 802.10 et Obtenir IEEE 802 pour plus de détails.

format de trame 802.1Q/801.1p

		En-tête de marqueur						
		TPID	TCI					
48 bits	48 bits	**16 bits**	**3 bits**	**1 bit**	**12 bits**	16 bits	Longueur variable	32 bits
LEDA	SA	**TPID**	**Priorité**	**TPI**	**ID de VLAN**	Longueur / type	Données avec PAD	FCS
		0x8100	**0 - 7**	**0-1**	**0-4095**			

Recommandation

Comme tous les nouveaux matériels prennent en charge 802.1Q (et certains supportent seulement 802.1Q, tels que la gamme Catalyst 4500/4000 et CSS 11000), Cisco recommande à toutes les nouvelles installations de suivre le standard IEEE 802.1Q et aux réseaux plus anciens de migrer graduellement à partir de l'ISL.

Le standard IEEE permet l'interopérabilité constructeur. C'est avantageux dans tous les environnements Cisco lorsque de nouveaux NIC et périphériques hôtes compatibles avec 802.1p deviennent disponibles. Bien que les installations ISL et 802.1Q soient toutes deux matures, le standard IEEE aura finalement une plus grande exposition et un plus grand support de tiers, tel que la prise en charge d'analyseurs réseau. Le temps d'encapsulation inférieur du 802.1Q comparé à l'ISL est un point mineur également en faveur du 802.1Q.

Comme le type d'encapsulation est négocié entre les commutateurs utilisant le DTP, avec l'ISL choisi en tant que gagnant par défaut si les deux extrémités le prennent en charge, il est nécessaire d'émettre cette commande afin de spécifier dot1q :

```
set trunk mod/port mode dot1q
```

Si VLAN 1 est effacé d'une jonction, comme évoqué dans la section Gestion intrabande de ce document, bien qu'aucune donnée utilisateur ne soit transmise ou reçue, le NMP continue à passer des protocoles de contrôle tels que le CDP et le VTP sur VLAN 1.

En outre, comme évoqué dans la section VLAN 1 de ce document, les paquets CDP, VTP et PAgP sont toujours envoyés sur le VLAN 1 quand il existe une jonction. En utilisant l'encapsulation dot1q, ces trames de contrôle sont marquées avec le VLAN 1 si le VLAN natif du commutateur est changé. Si la jonction 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 marquées et pour fournir une visibilité du voisin CDP sur le routeur.

Remarque: Il faut considérer des problèmes potentiels de sécurité avec dot1q provoqués par le marquage implicite du VLAN natif, car il peut être possible d'envoyer des trames d'un VLAN à

l'autre sans routeur. Référez-vous à Y-a-t'il des vulnérabilités dans les implémentations de VLAN ? pour plus de détails. Une solution de contournement consiste à utiliser une ID de VLAN pour le VLAN natif de la jonction qui n'est pas utilisée pour l'accès d'utilisateur. La majorité de clients Cisco laissent VLAN 1 comme VLAN natif sur une jonction et assignent des ports d'accès aux VLAN autres que le VLAN 1 afin de réaliser ceci simplement.

Mode de jonction

DTP est la seconde génération de Dynamic ISL (DISL) et existe afin de s'assurer que les différents paramètres impliqués dans l'envoi de trames ISL ou 802.1Q, telles que le type d'encapsulation configuré, le VLAN natif et la capacité matérielle, sont convenus par les commutateurs aux deux extrémités de la jonction. Ceci aide également à protéger contre l'inondation de trames marquées par des ports de non-jonction, potentiellement un risque sérieux pour la sécurité, en s'assurant que les ports et leurs voisins sont dans des états cohérents.

Aperçu opérationnel

DTP est un protocole L2 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 protocole de type SNAP 0x2004. Cette table présente un résumé des modes de configuration :

Mode	Fonction	Trames DTP transmises	État final (port local)
`Auto (default)`	Entraîne la tentative de conversion de la liaison en jonction. Le port devient un port de jonction si le port voisin est défini sur le mode on ou desirable .	Oui, périodique.	Jonction
`Sur`	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.	Jonction , **sans réserve**.
`Nonegotiate`	Met le port en mode de jonction des liens permanent mais empêche le port de produire des trames DTP. Vous devez configurer le port voisin manuellement comme port de jonction pour établir une liaison de jonction. C'est utile pour les périphériques qui ne	Non	Jonction , **sans réserve**.

	prennent pas en charge le DTP.		
`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.
`Outrede`	Met le port en mode non-jonction permanent et négocie pour convertir la liaison en liaison non-jonction. Le port devient un port de non-jonction même si le port voisin n'est pas d'accord sur la modification.	Non en état équilibré, mais transmet des informations pour accélérer la détection de l'extrémité distante après la modification d'on.	Non-jonction

Voici les points principaux du protocole :

- Le DTP assume une connexion point-à-point et les périphériques Cisco prennent en charge seulement les ports de jonction 802.1Q qui sont point par point.
- Pendant une négociation DTP, les ports ne participent pas au STP. C'est seulement une fois que le port est devenu un des trois types DTP (access, ISL ou 802.1Q) que le port est ajouté au STP. Autrement PAgP, si configuré, est le processus suivant qui s'exécute avant que le port participe au STP.
- Si le port établit une liaison en mode ISL, les paquets DTP sont envoyés sur le VLAN 1, autrement (pour les ports de jonction ou de non-jonction 802.1Q) ils sont envoyés sur le VLAN natif.
- En mode desirable , les paquets DTP transfèrent le **nom de domaine** VTP (qui doit correspondre pour qu'une jonction négociée s'établisse), plus la configuration de la jonction et l'**état admin**.
- Des messages sont envoyés toutes les secondes pendant la négociation, et toutes les 30 secondes après cela.
- Soyez sûr de comprendre que les modes on, nonegotiate et off spécifient explicitement dans quel état le port finit. Une mauvaise configuration peut mener à un état dangereux/contradictoire où un côté effectue une jonction et l'autre pas.
- Un port en mode on, auto ou desirable envoie des trames DTP périodiquement. Si un port en mode auto ou desirable ne voit pas un paquet DTP pendant cinq minutes, il passe en non-

jonction.

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.

Recommandation

Cisco recommande une configuration de jonction explicite en mode desirable aux deux extrémités. Dans ce mode, les opérateurs réseau peuvent faire confiance au Syslog et aux messages d'état de ligne de commande indiquant qu'un port est actif et a établi une jonction, à la différence du mode on qui peut faire apparaître un port actif bien que le voisin soit mal configuré. En outre, une jonction en mode desirable fournit la stabilité dans les situations où un côté de la liaison ne peut pas devenir une jonction ou relâche l'état de jonction. Émettez cette commande pour définir le mode desirable :

```
set trunk mod/port desirable ISL | dot1q
```

Remarque: Définissez la jonction sur off sur tous les ports de non-jonction. Cela aide à éliminer le temps de négociation gaspillé en activant des ports hôte. Cette commande est également exécutée quand la commande set port host est utilisée ; référez-vous à la section STP pour plus d'informations. Émettez cette commande afin de désactiver une jonction sur une plage de ports :

```
set trunk port range off
!--- Ports are not trunking; part of the set port host command.
```

Autres options

Une autre configuration client commune utilise le mode desirable seulement au niveau de la couche de distribution et la configuration par défaut la plus simple (mode 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 nonegotiate mode sur les commutateurs Catalyst 4500/4000, 5500/5000 et 6500/6000 afin de définir un port en tant que jonction sans réserve avec ces périphériques, ce qui peut permettre d'établir un standard commun à travers tout le campus. En outre, vous pouvez mettre en application le mode nonegotiate afin de réduire le temps d'initialisation « général » de la liaison.

Remarque: Les facteurs tels que le mode de canal et la configuration STP peuvent également affecter le temps d'initialisation.

Émettez cette commande pour définir le mode nonegotiate:

```
set trunk mod/port nonegotiate ISL | dot1q
```

Cisco recommande le mode nonegotiate quand il y a une connexion à un routeur Cisco IOS, car lorsqu'un pontage est établi, certaines trames DTP reçues du mode **on** peuvent revenir dans le port de jonction. À la réception de la trame DTP, le port de commutation essaye de renégocier (ou d'activer/désactiver la jonction) inutilement. Si nonegotiate est activé, le commutateur n'envoie pas

de trames DTP.

protocole STP

Considérations de base

Le protocole Spanning Tree (STP) maintient un environnement L2 sans boucles dans des réseaux redondants commutés et pontés. Sans STP, les trames font une boucle et/ou se multiplient indéfiniment, ce qui entraîne un ralentissement des données sur le réseau car tous les périphériques dans le domaine de diffusion sont interrompus continuellement par le trafic élevé.

Bien qu'à certains égards STP soit un protocole éprouvé développé initialement pour les ponts lents basés sur un logiciel (IEEE 802.1d), il peut être complexe à mettre en application correctement dans de grands réseaux commutés avec beaucoup de VLAN, beaucoup de commutateurs dans un domaine, un support pluri-constructeurs et des améliorations IEEE plus récentes.

Pour future référence, CatOS 6.x continue à supporter les nouveaux développements STP, tels que MISTP, la protection contre les boucles, la protection de la racine et la détection de décalage de livraison du BPDU. En outre, davantage de protocoles normalisés sont disponibles dans CatOS 7.x, tels le spanning tree partagé IEEE 802.1s et le spanning tree IEEE 802.1w à convergence rapide.

Aperçu opérationnel

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.

Au commencement, les BPDU sont envoyés à partir de tous les commutateurs, contenant le BID de chaque commutateur et le coût de chemin pour atteindre ce commutateur. Ceci active le 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.

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 (faisant face au pont racine) est sélectionné 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 Configuration du spanning tree pour plus d'informations.

Paramètres par défaut du timer de base	Nom	Fonction

(secondes)		
2	Bonjour	Contrôle l'envoi de BPDU.
15	Délai de transmission (Fwddelay)	Contrôle combien de temps un port passe dans l'état d'écoute et d'apprentissage et influence le processus de modification de la topologie (voir la section suivante).
20	Maxage	Contrôle combien de temps le commutateur maintient la topologie actuelle avant de rechercher un chemin alternatif. Après les secondes de Maxage, 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, il prétend être la racine elle-même sur les ports indiqués.

États du port	Signification	Temporisation par défaut jusqu'au prochain état
Handicapé	Administrativement inactif.	S/O
Blocage	Reçoit les BPDU et arrête les données utilisateur.	Surveillez la réception des BPDU. Attendez 20 secondes l'expiration du Maxage ou la modification immédiate si une défaillance de liaison directe/locale est détectée.
Écoute	Envoi ou réception des BPDU pour contrôler si un retour au blocage est requis.	Timer de Fwddelay (attendre 15 secondes)
Apprendre	Construit une topologie/table CAM.	Timer de Fwddelay (attendre 15 secondes)
Transmission	Envoi/réception des données.	
	Modification de la topologie de base totale :	**20 + 2 (15) = 50 secondes si vous attendez l'expiration du Maxage, ou 30 secondes pour la défaillance de liaison directe**

Les deux types de BPDU dans STP sont des BPDU de configuration et des BPDU d'avis de modification de la topologie (TCN).

Écoulement de la configuration BPDU

Les BPDU de configuration sont collectés à chaque hello-interval de chaque port sur le pont racine et coulent ultérieurement dans tous les commutateurs de terminal afin de maintenir l'état du spanning tree. En état équilibré, l'écoulement BPDU est unidirectionnel : les ports racine et les ports de blocage reçoivent seulement des BPDU de configuration, alors que les ports désignés envoient seulement des BPDU de configuration.

Pour chaque BPDU reçu par un commutateur de la racine, un nouveau est traité par le NMP Catalyst central et envoyé en contenant l'information de racine. En d'autres termes, si le pont racine est perdu ou si tous les chemins au pont racine sont perdus, les BPDU ne sont plus reçus (jusqu'à ce que le timer de Maxage commence la réélection).

Écoulement TCN BPDU

Les BPDU TCN sont collectés auprès des commutateurs de terminal et coulent vers le pont racine quand une modification de topologie est détectée dans le spanning tree. Les ports racine envoient seulement des TCN et les ports désignés reçoivent seulement des TCN.

Le BPDU TCN voyage vers la dorsale racine et est reconnu at chaque étape, ainsi c'est un mécanisme fiable. Une fois qu'il arrive au pont racine, celui-ci alerte le domaine tout entier qu'une modification s'est produite en collectant des BPDU de configuration avec l'indicateur TCN défini sur la durée **maxage + fwddelay** (35 secondes par défaut). Ceci fait changer à tous les commutateurs leur délai d'expiration de la mémoire CAM normal de cinq minutes (par défaut) à l'intervalle spécifié par **fwddelay** (15 secondes par défaut). Référez-vous à Comprendre les modifications de topologie du protocole Spanning Tree pour plus de détails.

Modes du Spanning Tree

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

- Un spanning tree unique pour tous les VLAN, ou un protocole spanning tree mono, tel qu'IEEE 802.1Q
- Un spanning tree par VLAN, ou un spanning tree partagé, comme Cisco PVST
- Un spanning tree par ensemble de VLAN, ou un spanning tree multiple, comme Cisco MISTP et IEEE 802.1s

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 permet l'équilibrage de charge mais exige plus de traitement par le CPU du BPDU à mesure que le nombre de VLAN augmente. Les notes de publication de CatOS fournissent des conseils sur le nombre de ports logiques recommandé dans le spanning-tree par commutateur. Par exemple, la formule Catalyst 6500/6000 Supervisor Engine 1 est la suivante :

nombre de ports + (nombre de jonctions * nombre de VLAN sur les jonctions) < 4000

Cisco MISTP et la nouvelle norme 802.1s permettent la définition de seulement deux instances/topologies STP actives et le mappage de tous les VLAN sur l'un ou l'autre de ces deux arborescences. Cette technique permet à STP de mesurer des milliers de VLAN tandis que l'équilibrage de charge est activé.

Formats de BPDU

Afin de prendre en charge la norme IEEE 802.1Q, la mise en place existante de Cisco STP a été étendue pour devenir PVST+ en ajoutant la prise en charge de la tunnellisation à travers une région de spanning tree mono IEEE 802.1Q. PVST+ est donc compatible avec IEEE 802.1Q MST et les protocoles PVST de Cisco et n'exige pas de commandes ou de configuration supplémentaires. 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.

Voici quelques points opérationnels importants du protocole PVST+ :

- PVST+ interopère avec le spanning tree mono 802.1Q par le soi-disant Common Spanning Tree (CST) via une jonction 802.1Q. Le CST est toujours sur le VLAN 1, ainsi ce VLAN doit être activé sur la jonction pour interopérer avec d'autres constructeurs. Les BPDU CST sont transmis, toujours non-marqués, au groupe de pontage de la norme IEEE (adresse MAC 01-80-c2-00-00-00, DSAP 42, SSAP 42). Pour l'exhaustivité de la description, un ensemble parallèle de BPDU est également transmis à l'adresse MAC du spanning tree Cisco partagé pour le VLAN 1.
- PVST+ tunnellise les BPDU PVST à travers les régions VLAN 802.1Q sous forme de données multicast. Les BPDU de spanning tree cisco partagé sont transmis à l'adresse MAC 01-00-0c-cc-cc-cd (protocole SNAP HDLC 0x010b) pour chaque VLAN sur une jonction. Les BPDU ne sont pas marqués sur le VLAN natif et sont marqués pour tous les autres VLAN.
- PVST+ contrôle les incohérences de port et de VLAN. PVST+ bloque les ports qui reçoivent des BPDU contradictoires afin d'empêcher des boucles de réacheminement. Il informe également les utilisateurs via les messages syslog au sujet de n'importe quelle disparité de configuration.
- PVST+ est rétrocompatible avec les commutateurs Cisco existants exécutant PVST sur des jonctions ISL. Les BPDU à encapsulation ISL sont encore transmis ou reçus à l'aide de l'adresse MAC IEEE. En d'autres termes, chaque type de BPDU est local à sa liaison ; il n'y a aucun problème de traduction.

Recommandation

Tous les commutateurs Catalyst ont STP activé par défaut. Ceci est recommandé même si une conception est choisie qui n'inclut pas les boucles L2 de sorte que STP ne soit pas activé dans le sens qu'il maintient activement un port bloqué.

```
set spantree enable all
!--- This is the default.
```

Cisco recommande de laisser STP activé pour ces raisons :

- S'il y a une boucle (induite par un mauvais câblage, un câble défectueux, etc.), STP empêche des effets néfastes au réseau provoqués par des données multicast et de diffusion.
- Protection contre une décomposition d'EtherChannel.
- La plupart des réseaux sont configurés avec STP, ce qui lui donne une exposition maximale. Plus d'exposition égale généralement un code stable.
- Protection contre les défaillances des NIC à double connexion (ou pontage activé sur les serveurs).

- Le logiciel pour beaucoup de protocoles (tels que PAgP, IGMP Snooping et jonction) est étroitement lié à STP. L'exécution sans STP peut mener à des résultats indésirables.

Ne changez pas les timers, car ceci peut compromettre la stabilité. La majorité des réseaux déployés ne sont pas accordés. Les timers STP simples accessibles par ligne de commande, comme l'hello-interval et le Maxage, sont eux-mêmes composés d'un ensemble complexe d'autres timers assumés et intrinsèques, ainsi il est difficile d'accorder les timers et de considérer toutes les ramifications. D'ailleurs, il y a le danger de miner la protection UDLD .

Dans le meilleur des cas, gardez le trafic utilisateur du VLAN de gestion. Particulièrement avec les processeurs de commutation Catalyst plus anciens, il vaut mieux éviter des problèmes avec STP en gardant le VLAN 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 qu'il 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. Voyez la section Gestion intrabande de ce document pour plus de détails.

Ne forcez pas trop sur la redondance. Ceci peut mener à un cauchemar de dépannage - trop de ports de blocage compromettent la stabilité à long terme. Maintenez le diamètre SPT total inférieur à sept sauts. Essayez de vous inspirer du modèle Cisco multicouche, avec ses plus petits domaines commutés, ses triangles STP et ses ports bloqués déterministes (comme expliqué dans Conception d'un réseau Gigabit Campus - Principes et architecture) dans la mesure du possible.

Influencez et sachez où la fonctionnalité racine et les ports bloqués résident, et ajoutez cet élément au diagramme de topologie. Les ports bloqués sont la clé du dépannage STP - ce qui les a fait passer du blocage à la 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 celles-ci sont considérées comme les parties les plus stables du réseau. Vérifiez que le recouvrement L3 et HSRP est optimal, avec des chemins de transmission des données L2. Cette commande est une macro qui configure la priorité de pont ; la racine la définit bien en dessous que la valeur par défaut (32768), alors que la racine secondaire la définit raisonnablement en dessous de la valeur par défaut :

```
set spantree root secondary vlan range
```

Remarque: Cette macro fixe la priorité racine soit sur 8192 (par défaut), soit sur la priorité racine actuelle moins 1 (si un autre pont racine est connu), soit sur la priorité racine actuelle (si son adresse MAC est inférieure à la racine actuelle).

Élaguez les VLAN inutiles des ports de liaison (un exercice bidirectionnel). Ceci 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. Référez-vous à la section VTP de ce document pour plus d'informations. Le VLAN 1 par défaut peut également être retiré des jonctions utilisant CatOS 5.4 et ultérieurs.

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

Autres options

Cisco a un autre STP connu sous le nom de pont VLAN. Ce protocole fonctionne avec une adresse MAC de destination de **01-00-0c-cd-cd-ce** et un protocole de type 0x010c.

C'est le plus utile s'il y a un besoin de jeter un pont sur des protocoles non-routable ou existants entre les VLAN sans gêner l'exécution d'exemples d'IEEE Spanning Tree sur ces VLAN. Si les interfaces VLAN pour le trafic non-ponté deviennent bloquées pour le trafic L2 (et ceci pourrait facilement se produire s'ils participaient au même STP que les VLAN IP), le trafic de recouvrement L3 est accidentellement élagué lui aussi - un effet secondaire non désiré. Le pont VLAN est donc une instance de STP séparée pour des protocoles pontés, ce qui fournit une topologie distincte qui peut être manipulée sans affecter le trafic IP.

Cisco recommande d'exécuter un pont VLAN si un pontage est requis entre les VLAN sur des routeurs Cisco tels que le MSFC.

PortFast

Portfast est utilisé pour contourner le fonctionnement normal du Spanning Tree sur les ports d'accès et pour accélérer la connectivité entre les stations d'extrémité et les services auxquels ils doivent se connecter après l'initialisation de la liaison. Sur quelques protocoles, tels qu'IPX/SPX, il est important de voir le port d'accès en mode transmission dès que la liaison est établie afin d'éviter des problèmes GNS.

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 saute les états d'écoute et d'apprentissage normaux de STP en faisant passer un port directement du mode blocking au mode forwarding une fois la liaison établie. 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. Ceci peut prendre deux fois plus de temps que le ForwardDelay (un total de 30 secondes par défaut).

Le mode Portfast empêche également un TCN STP d'être généré à chaque fois que l'état du port passe de learning à forwarding. Les TCN ne sont pas un problème seuls, mais si une vague de TCN frappe le pont racine (typiquement pendant le matin où les gens mettent en marche leurs PC), cela peut étendre le temps de convergence inutilement.

STP Portfast est particulièrement important sur les réseaux CGMP multicast et Catalyst 5500/5000 MLS. Les TCN dans ces environnements peuvent causer le vieillissement des entrées statiques de table CAM CGMP, ce qui a comme conséquence la perte de paquets de multidiffusion jusqu'au rapport IGMP suivant, et/ou le vidage des entrées de cache MLS qui doivent alors être reconstruites, ce qui peut avoir comme conséquence un pic du CPU de routeur, selon la taille du cache. (les installations Catalyst 6500/6000 MLS et entrées de multidiffusion apprises de l'IGMP Snooping ne sont pas affectées.)

Recommandation

Cisco recommande d'activer STP Portfast pour tous les ports hôtes actifs et de le désactiver pour les liaisons commutateur à commutateur et les ports non utilisés.

L'agrégation de liens et l'acheminement doivent également être désactivés sur tous les ports hôtes. 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 ces

protocoles sont laissés pour négocier, le retard suivant dans l'activation du port peut mener à des situations indésirables dans lesquelles des paquets initiaux des postes de travail, tels que des requêtes DHCP, ne sont pas expédiés.

CatOS 5.2 a introduit une commande macro, set port host port range qui met en application cette configuration pour les ports d'accès et aide les performances d'autonégociation et de connexion de manière significative :

```
set port host port range
!--- Macro command for these commands: set spantree portfast port range enable set trunk port
range off set port channel port range mode off
```

Remarque: Portfast ne signifie pas que le spanning tree ne s'exécute pas sur tous ces ports. Les BPDU sont encore envoyés, reçus et traités.

Autres options

La fonctionnalité de protection des BPDU fournit une manière d'empêcher les boucles en faisant passer un port de non-jonction en état errdisable quand un BPDU est reçu sur ce port.

Un paquet de BPDU ne doit jamais être reçu sur un port d'accès configuré pour Portfast, puisque des ports hôtes ne doivent pas être attachés aux commutateurs. Si un BPDU est observé, il indique une configuration non valide et potentiellement dangereuse qui nécessite une action administrative. Quand la fonctionnalité de protection des BPDU est activée, le spanning tree arrête les interfaces configurées qui reçoivent des BPDU au lieu de les mettre en état STP blocking.

La commande fonctionne sur une base par commutateur, pas par port, comme montré :

```
set spantree portfast bpdu-guard enable
```

L'administrateur réseau est notifié par une interruption SNMP ou un message Syslog si le port devient inactif. Il est également possible de configurer un temps de reprise automatique time pour les ports errdisabled. Référez-vous à la section UDLD de ce document pour plus de détails. Pour plus d'informations, reportez-vous à Amélioration de Spanning Tree PortFast BPDU Guard.

Remarque: Portfast pour des ports de liaison a été introduit dans CatOS 7.x et n'exerce aucun effet sur les ports de jonction des versions antérieures. Portfast pour les ports de jonction est conçu pour augmenter les temps de convergence pour les réseaux L3. Pour compléter cette fonctionnalité, CatOS 7.x a également introduit la possibilité de configurer la protection des BPODU PortFast sur une base par port.

UplinkFast

Uplinkfast fournit une convergence STP rapide après une défaillance de liaison directe dans la couche d'accès au réseau. Elle ne modifie pas STP, et son but est d'accélérer le temps de convergence dans des circonstances spécifiques à moins de trois secondes, plutôt que le retard typique de 30 secondes. Référez-vous à Comprendre et configurer la fonctionnalité Cisco Uplink Fast pour plus d'informations.

Aperçu opérationnel

Utilisant le modèle de projet Cisco multicouche au niveau de la couche d'accès, si la liaison

ascendante d'expédition est perdue, la liaison ascendante de blocage passe immédiatement en état forwarding sans attendre les états listening et learning.

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, le port racine assure 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.

Puisque ceci contourne effectivement le procédé normal de modification-manipulation de la topologie STP (listening et learning), un autre mécanisme de correction de la topologie est nécessaire pour mettre à jour les commutateurs du domaine que les stations d'extrémité locale sont accessibles par une voie de déroutement. Le commutateur de la couche d'accès exécutant UplinkFast génère également des trames pour chaque adresse MAC dans son CAM vers une adresse MAC multicast (01-00-0c-cd-cd-cd, protocole HDLC 0x200a) afin de mettre à jour la table CAM dans tous les commutateurs du domaine avec la nouvelle topologie.

Recommandation

Cisco recommande d'activer UplinkFast sur les commutateurs avec des ports bloqués, en général au niveau de la couche d'accès. 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. Elle peut être ajoutée sans interruption à un réseau de production. Émettez cette commande afin d'activer UplinkFast :

```
set spantree uplinkfast enable
```

Cette commande définit également la **priorité de pont** sur une valeur élevée afin de réduire au minimum le risque qu'il devienne un pont racine et la **priorité de port** sur une valeur élevée pour éviter qu'il devienne un port désigné, ce qui casse la fonctionnalité. Quand vous restaurez un commutateur qui avait UplinkFast activé, la fonctionnalité doit être désactivée, la base de données de la liaison ascendante nettoyée avec « clear uplink » et les priorités de pont restaurées manuellement.

Remarque: Le mot clé **all protocols** pour la commande UplinkFast est requis lorsque la fonctionnalité de filtrage du 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 de **débit** indique les paquets par seconde des trames de mise à jour de topologie d'uplinkfast. La valeur par défaut est recommandée. Vous n'avez pas besoin de configurer BackboneFast avec Rapid STP (RSTP) ou IEEE 802.1w parce que le mécanisme est inclus de manière native et automatiquement activé dans RSTP.

BackboneFast

BackboneFast fournit une convergence rapide des défaillances de liaison indirecte. Avec la fonctionnalité ajoutée à STP, les temps de convergence peuvent typiquement être réduits de la valeur par défaut de 50 secondes à 30 secondes.

Aperçu opérationnel

Le mécanisme est lancé quand un port racine ou un port bloqué sur un commutateur reçoit des BPDU inférieurs de son pont désigné. Ceci peut se produire quand un commutateur en aval a perdu sa connexion à la racine et commence à envoyer ses propres BPDU afin d'élire une nouvelle racine. Une **BPDU inférieure** identifie un commutateur comme pont racine et pont désigné.

Selon les règles normales de spanning tree, le commutateur récepteur ignore les BPDU inférieurs pour le délai d'expiration maximal configuré, 20 secondes par défaut. Cependant, avec BackboneFast, le commutateur voit le BPDU inférieur en tant que signal que la topologie pourrait avoir changé, et essaie de déterminer s'il a une voie de déroutement vers le pont racine utilisant les BPDU de requête de liaison racine (RLQ). Cet ajout au protocole permet à un commutateur de contrôler si la racine est encore disponible, fait passer un port blocked en mode forwarding plus rapidement et informe le commutateur isolé qui a envoyé les BPDU inférieurs que la racine est toujours là.

Voici quelques points opérationnels importants du fonctionnement du protocole :

- Un commutateur transmet le paquet RLQ par le port racine seulement (c'est-à-dire vers le pont racine).
- Un commutateur qui reçoit un RLQ peut répondre l'un ou l'autre s'il est le commutateur racine, ou s'il sait qu'il a perdu la connexion à la racine. S'il ne connaît pas ces faits, il doit expédier la requête à son port racine.
- Si un commutateur a perdu sa connexion à la racine, il 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, elle est ignorée.

Les temps de convergence STP peuvent donc être réduits de jusqu'à 20 secondes, car le 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 recommande d'activer BackboneFast sur tous les commutateurs exécutant STP. Elle peut être ajoutée sans interruption à un réseau de production. Émettez cette commande afin d'activer BackboneFast :

```
set spantree backbonefast enable
```

Remarque: Cette commande de niveau global doit être configurée sur tous les commutateurs d'un domaine car il ajoute de la fonctionnalité au protocole STP que tous les commutateurs doivent comprendre.

Autres options

BackboneFast n'est pas pris en charge sur 2900XLs et 3500s. Il ne doit pas être activé si le domaine de commutation contient ces commutateurs en plus des commutateurs Catalyst 4500/4000, 5500/5000 et 6500/6000.

Vous n'avez pas besoin de configurer BackboneFast avec RSTP ou IEEE 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. La fonctionnalité de protection contre les boucles protège les réseaux L2 des boucles provoquées par :

- les interfaces réseau qui fonctionnent mal
- les CPU occupés
- Tout ce qui empêche l'expédition normale des BPDU

Une boucle STP se produit quand un port bloquant dans une topologie incorrectement redondante passe en état de transmission. Cette transition se produit habituellement parce qu'un des ports dans une topologie physiquement redondante (pas nécessairement le port bloquant) cesse de recevoir des BPDU.

La fonctionnalité de protection contre les boucles est seulement utile dans les réseaux où les Commutateurs sont connectés par des liaisons point par point. La plupart des campus modernes et des réseaux de centres de données sont ces types de réseaux. Sur une liaison point à point, un pont désigné ne peut pas disparaître à moins qu'il n'envoie un BPDU inférieur ou désactive la liaison. La fonctionnalité de protection contre les boucles STP a été introduite dans CatOS Version 6.2.1 pour les plates-formes Catalyst 4000 et Catalyst 5000 et dans la version 6.2.2 pour la plate-forme Catalyst 6000.

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

La fonctionnalité de protection contre les boucles vérifie si un port racine ou un port racine alternatif/de secours 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. L'état de boucle incohérente est retiré du port, et STP détermine l'état du port parce qu'une telle 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. La fonctionnalité de protection contre les boucles évite les boucles STP avec la vitesse de la version STP en service. Il n'y a aucune dépendance sur STP lui-même (802.1d ou 802.1w) ou quand les timers STP sont accordés. Pour ces raisons, vous devez mettre en oeuvre la fonctionnalité 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 :

```
set spantree backbonefast enable
```

Lorsque les BPDU sont reçus sur un port dans un état de boucle incohérente, le port passe à un

autre état STP. En accord avec le BPDU reçu, la reprise est automatique et aucune intervention n'est nécessaire. Après la reprise, ce message est enregistré :

```
set spantree backbonefast enable
```

Interaction avec les autres fonctions STP

- **Protection de la racine**La protection de la racine force un port à être constamment désigné. La fonctionnalité de protection contre les boucles est pertinent seulement si le port est le port racine ou un port alternatif. Ces fonctions s'excluent mutuellement. La fonctionnalité de protection contre les boucles et la protection de la racine ne peuvent pas être activées sur un port en même temps.
- **UplinkFast**La fonctionnalité de protection contre les boucles est compatible avec UplinkFast. Si la fonctionnalité+F39805 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 port racine.
- **BackboneFast**La fonctionnalité de protection contre les boucles est compatible avec BackboneFast. La réception d'un BPDU inférieur qui vient d'un pont désigné déclenche BackboneFast. Puisque les BPDU sont reçus à partir de cette liaison, le dispositif de protection contre les boucles n'est pas activé, ainsi le dispositif de protection contre les boucles et BackboneFast sont compatibles.
- **PortFast**Portfast fait passer un port en mode désigné de transmission à l'activation de la liaison. Puisqu'un port en Portfast ne peut pas être une racine ou un accès alternatif, 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. Cependant, afin de former un canal, tous les ports physiques qui sont groupés dans le canal doivent avoir des configurations compatibles. PAgP impose la configuration uniforme de la fonctionnalité de protection contre les boucles sur tous les ports physiques pour former un canal.**Remarque:** Ce sont des obstacles quand vous configurez la fonctionnalité de protection contre les boucles sur un EtherChannel :STP sélectionne toujours le premier port opérationnel dans le canal afin d'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 des ports, qui sont déjà bloqués par la fonctionnalité de protection contre les boucles, sont groupés ensemble afin de former un canal, STP perd toutes les informations d'état pour ces ports. Le nouveau port de canal peut atteindre l'état de transmission avec un rôle indiqué.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 le rôle indiqué, même si une ou plusieurs des liaisons qui ont formé le canal sont unidirectionnelles.Dans les deux derniers cas de cette liste, il est possible qu'une boucle se forme jusqu'à ce qu'UDLD détecte la panne. Mais la fonctionnalité de protection contre les boucles ne peut pas détecter la boucle.

Comparaison des fonctionnalités de protection contre les boucles et UDLD

La fonctionnalité de protection contre les boucles et la fonctionnalité UDLD se recoupent partiellement. Chacune des deux fournit une protection contre les pannes STP que les liens

unidirectionnels entraînent. Mais ces deux fonctions sont différentes dans l'approche du problème et également dans la fonctionnalité. Spécifiquement, il y a certaines défaillances unidirectionnelles qu'UDLD ne peut pas détecter, comme les pannes qui sont provoquées par un 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.

La fonctionnalité 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 la fonctionnalité de protection contre les boucles ne couvre pas ce cas particulier. UDLD fournit une protection contre un tel scénario.

Activez UDLD et la protection contre les boucles afin de fournir le de plus haut niveau de protection. Référez-vous au *Loop Guard contre la* section *unidirectionnelle de détection de lien d'*améliorations de protocole spanning-tree utilisant le fonctionnalités de protection contre les boucles et de détection des différences de temps de propagation des BPDU pour une comparaison de protection de boucle et de caractéristique UDLD.

Recommandation

Cisco recommande d'activer le dispositif de protection contre les boucles globalement sur un réseau de commutation avec des boucles physiques. Dans la version 7.1(1) du logiciel Catalyst et dans les versions ultérieures, vous pouvez activer la protection contre les boucles 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 bidirectionnel de la liaison. Si le mode duplex est bidirectionnel simultané, la liaison est considérée point à point. Émettez cette commande afin d'activer globalement la fonctionnalité de protection contre les boucles :

```
set spantree global-default loopguard enable
```

Autres options

Pour les commutateurs qui ne supportent pas la configuration avec la protection contre les boucles, activez la fonctionnalité sur tous les ports individuels, ce qui inclut les ports de canal de port. Bien qu'il n'y ait aucun avantage à activer le dispositif de protection contre les boucles sur un port désigné, cette activation n'est pas 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. Émettez cette commande afin d'activer la fonctionnalité de protection contre les boucles :

```
set spantree guard loop mod/port
```

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. Cependant, l'activation de la fonctionnalité de protection contre les boucles dans ce type de topologie peut mener à des problèmes d'isolement du réseau. Afin d'établir des topologies sans boucles et d'éviter des problèmes d'isolement du réseau, émettez ces commandes pour désactiver la fonctionnalité de protection contre les boucles globalement ou individuellement. N'activez pas la fonctionnalité de protection contre les boucles sur des liaisons partagées.

- ```
  set spantree global-default loopguard disable
  ```
  ```

```
!--- This is the global default.
```

ou

- ```
  set spantree guard none mod/port
  !--- This is the default port 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, la protection de la racine impose la position du pont racine. La protection de la racine est disponible dans CatOS pour Catalyst 29xx, 4500/4000, 5500/5000 et 6500/6000 Version 6.1.1 et 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 la protection de la racine est appliquée à un port, elle ne permet pas à un port de devenir un port racine. Si la réception d'un 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 montre l'action :

```
set spantree guard none mod/port
!--- This is the default port configuration.
```

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. La reprise est automatique, et aucune intervention humaine n'est nécessaire. Ce message Syslog fournit un exemple :

```
set spantree guard none mod/port
!--- This is the default port configuration.
```

La protection de la racine force un port à être désigné et la protection contre les boucles est pertinente seulement si le port est le port racine ou un port alternatif. Par conséquent, les deux fonctions s'excluent mutuellement. La fonctionnalité de protection contre les boucles et la protection de la racine ne peuvent pas être activées 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 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, émettez cette commande :
```

`set spantree guard root mod/port`

EtherChannel

Les technologies EtherChannel permettent le multiplexage inverse de plusieurs canaux (jusqu'à huit sur Catalyst 6500/6000) dans une liaison logique simple. Bien que chaque plate-forme diffère de la suivante en ce qui concerne la mise en œuvre, il est important de comprendre leurs exigences communes :

- Un algorithme pour multiplexer statistiquement les trames sur plusieurs canaux
- La création d'un port logique de sorte qu'une instance unique de STP puisse être exécutée
- Un protocole de gestion de canal tel que PAgP ou le Link Aggregation Control Protocol (LACP)

Multiplexage d'une trame

EtherChannel comprend un algorithme de distribution de trames qui multiplexe efficacement des trames à travers le composant 10/100 ou des liaisons 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 de charge 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.

Remarque: Il faut considérer les informations suivantes :

- Catalyst 6500/6000 a un matériel de commutation plus récent que Catalyst 5500/5000 et peut lire les informations IP de la couche 4 (L4) à un débit câble afin de prendre une décision de multiplexage plus intelligente que de simples informations MAC L2.
- Les capacités de Catalyst 5500/5000 dépendent de la présence d'une puce Ethernet intégrée (EBC) sur le module. La commande de capacités show port mod/port confirme ce qui est possible pour chaque port.

Référez-vous à cette table, qui illustre l'algorithme de distribution de trames en détail pour chaque plate-forme énumérée :

Plate-forme	Algorithme d'équilibrage de charge du canal
Gamme Catalyst 5500/5000	Un Catalyst 5500/5000 avec les modules nécessaires permet deux à quatre liens à être présents par FEC[1], bien qu'ils doivent être sur le même module. Les adresses MAC source et de destination déterminent la liaison choisie pour la transmission de trames. Une opération X-OR est exécutée sur les deux bits les moins significatifs des adresses MAC source et de destination. Cette opération donne l'un de ces quatre résultats

	suivants : (0 0), (0 1), (1 0) ou (1 1). Chacune de ces valeurs pointe vers une liaison dans le lot FEC. Dans le cas d'un Fast EtherChannel à deux ports, seul un bit est utilisé dans l'opération X-OR. Il arrive qu'une adresse de la paire source/destination soit une constante. Par exemple, la destination peut être un serveur ou, bien plus probable, un routeur. Dans ce cas, l'équilibrage de charge statistique se produit toujours puisque l'adresse source est toujours différente.
Gamme Catalyst 4500/4000	Catalyst 4500/4000 EtherChannel distribue des trames à travers les liaisons dans un canal (sur un module simple) basé sur les bits d'ordre bas des adresses MAC source et de destination de chaque trame. En comparaison avec Catalyst 5500/5000, l'algorithme est plus impliqué et utilise un hachage déterministe de ces champs du DA MAC (octets 3, 5, 6), du SA (octets 3, 5, 6), du port d'entrée et de l'ID VLAN. La méthode de distribution de trames n'est pas configurable.
Gamme Catalyst 6500/6000	Il y a deux possibles algorithmes de hachage, selon le matériel Supervisor Engine. Les informations parasites sont un dix-septième polynôme de degré mis en application dans le matériel qui, dans des tous les cas, prend l'adresse MAC, l'adresse IP, ou le numéro de port IP TCP/UDP2 et applique l'algorithme pour générer une valeur du bit trois. Ceci est fait séparément pour les deux adresses source et de destination. Les résultats sont alors passés au X-OR pour produire une autre valeur de trois bits qui est utilisée pour déterminer quel port dans le canal est utilisé pour expédier le paquet. Des canaux sur Catalyst le 6500/6000 peuvent être formés entre les ports sur n'importe quel module et peuvent être jusqu'à 8 ports.

[1] FEC = Fast EtherChannel

UDP [2] = User Datagram Protocol

Cette table indique les méthodes de distribution prises en charge sur les divers modèles de Supervisor Engine Catalyst 6500/6000 et leur comportement par défaut.

Matériel	Description	Méthodes de distribution
WS-F6020 (L2 Engine)	Early Supervisor Engine 1	L2 MAC : SA ; LE DA ; SA & DA
WS-F6020A	Supervisor Engine 1 plus récent et Supervisor	L2 MAC : SA ; LE DA ; IP SA ET DU

(L2 engine) WS-F6K-PFC (moteur L3)	Engine 1A/PFC1	DA L3 : SA ; LE DA ; SA et DA (valeur par défaut)
WS-F6K-PFC2	Supervisor Engine 2/PFC2 (nécessite CatOS 6.x)	L2 MAC : SA ; LE DA ; IP SA ET DU DA L3 : SA ; LE DA ; Session SA et du DA L4 (par défaut) : Port S ; port D ; port S & D port (défaut)
WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A	Engine 720/PFC3BXL (les besoins CatOS 8.3.x) de superviseur de l'engine 32/PFC3B (les besoins CatOS 8.4.x) de l'engine 720/Supervisor de superviseur de l'engine 720/PFC3A (les besoins CatOS 8.1.x) de superviseur	L2 MAC : SA ; LE DA ; IP SA ET DU DA L3 : SA ; LE DA ; Session SA et du DA L4 (par défaut) : Port S ; port D ; Session du port IP-VLAN-L4 S et D : port SA & VLAN & S ; port DA & VLAN & D ; port SA & DA & VLAN & S & port D

Remarque: Avec la distribution L4, le premier paquet fragmenté utilise la distribution L4. Tous les paquets suivants utilisent la distribution L3.

Pour plus de détails sur la prise en charge d'EtherChannel sur les autres plates-formes, sur leur configuration et leur dépannage, consultez ces documents :

- Présentation de l'équilibrage de charge et de la redondance EtherChannel sur les commutateurs Catalyst
- Configuration d'EtherChannel entre des commutateurs Catalyst 4500/4000, 5500/5000 et des commutateurs 6500/6000 qui exécutent le logiciel système CatOS
- Configuration de LACP (802.3ad) entre un Catalyst 6500/6000 et un Catalyst 4500/4000
- Configuration d'EtherChannel couche 3 et couche 2

Recommandation

Les commutateurs de la gamme Catalyst 6500/6000 exécutent l'équilibrage de charge par adresse IP par défaut. Ceci est recommandé dans CatOS 5.5, supposant que l'IP est le protocole dominant. Émettez cette commande pour définir l'équilibrage de charge :

```
set port channel all distribution ip both
!--- This is the default.
```

La distribution de trames par adresse MAC L2 de la gamme Catalyst 4500/4000 et 5500/5000 est acceptable dans la plupart des réseaux. Cependant, la même liaison est utilisée pour tout le trafic s'il y a seulement deux périphériques principaux qui conversent sur un canal (car SMAC et DMAC sont constants). Ceci peut typiquement être un problème pour la copie de sauvegarde de serveur et d'autres grands transferts de fichiers ou pour un segment de transit entre deux routeurs.

Bien que le port agrégé logique (agport) puisse être contrôlé par SNMP en tant qu'instance distincte et les statistiques de débit cumulé recueillies, Cisco recommande de gérer chacune des interfaces physiques séparément afin de contrôler comment les mécanismes de distribution de trames fonctionnent et si l'équilibrage de charge statistique est réalisé.

Une nouvelle commande CatOS 6.x, show channel traffic, peut afficher les statistiques de distribution en pourcentage plus facilement qu'en contrôlant les compteurs de ports individuels à l'aide des commandes show counters mod/port ou show mac mod/port dans CatOS 5.x. Une autre nouvelle commande CatOS 6.x, show channel hash , permet de contrôler, en fonction du mode de distribution, quel port serait sélectionné comme port de sortie pour certaines adresses et/ou numéros de port. Les commandes équivalentes pour les canaux LACP sont show lacp-channel traffic et show lacp-channel hash .

Autres options

Certaines mesures peuvent s'avérer nécessaires si les limitations relatives des algorithmes de type MAC de Catalyst 4500/4000 ou Catalyst 5500/5000 posent des problèmes, et si le bon équilibrage de charge statistique n'est pas réalisé :

- Commutateurs Catalyst 6500/6000 à déploiement par point
- Augmentez la bande passante sans canaliser en alternant, par exemple, entre plusieurs ports FE et un port GE, ou entre plusieurs ports GE et un port 10 GE.
- Réadressez les paires de stations d'extrémité avec de larges flux de volume
- Liaisons dédiées/VLAN pour les périphériques à forte bande passante

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. Suivez les directives afin d'éviter des 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. Dans le logiciel Cisco IOS, vous pouvez désactiver le contrôle d'attribut de port QoS sur le groupement EtherChannel avec la commande d'interface port-canal no mls qos channel-consistency . Une commande équivalente afin de désactiver le contrôle d'attribut de port QoS n'est pas disponible dans CatOS. Vous pouvez émettre la commande de capacités show port mod/port pour afficher la capacité de port QoS et déterminer si les ports sont compatibles.

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

- La section *Directives de configuration d'EtherChannel* de Configuration d'EtherChannel (Catalyst 6500/6000)
- La section *Directives de configuration et restrictions d'EtherChannel* de Configuration de Fast EtherChannel et Gigabit EtherChannel (Catalyst 4500/4000)
- La section *Directives de configuration et restrictions d'EtherChannel* de Configuration de Fast

EtherChannel et de Gigabit EtherChannel (Catalyst 5000)

Remarque: Le nombre maximal de canaux de port que prend en charge Catalyst 4000 est 126. Avec les versions logicielles 6.2(1) et antérieures, les commutateurs de la gamme Catalyst 6500 à six et à neuf emplacements prennent en charge un maximum de 128 modules EtherChannel. Dans les versions logicielles 6.2(2) et ultérieures, la fonctionnalité de spanning tree gère l'ID de port. Par conséquent, le nombre maximal de modules EtherChannel avec prise en charge est de 126 pour un châssis à six ou neuf emplacements et de 63 pour un châssis à 13 emplacements.

Protocole d'agrégation de ports

PAgP est un protocole de gestion qui contrôle la cohérence des paramètres à chaque extrémité de la liaison et aide le canal dans l'adaptation à la défaillance ou à l'ajout d'une liaison. Notez ces faits sur 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 un groupement existe déjà et que la configuration d'un port est modifiée (comme la modification d'un VLAN ou le mode d'agrégation), tous les ports du groupement sont modifiés pour correspondre à cette configuration.
- 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 paquets PAgP sont envoyés en utilisant la même adresse MAC de groupe multicast qui est utilisée pour les paquets CDP, **01-00-0c-cc-cc-cc**. La valeur du protocole est 0x0104. Voici un résumé du fonctionnement du protocole :

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

Traitement normal

Ces concepts doivent être définis pour faciliter la compréhension du 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. Par conséquent, un agport ne contient pas de

ports non-opérationnels.
- **Canal** - une agrégation répondant aux critères de formation ; il peut donc contenir des ports non-opérationnels (les agports sont un sous-ensemble de canaux). Des protocoles comprenant STP et VTP, mais excluant CDP et DTP, s'exécutent par-dessus PAgP sur les agports. Aucun de ces protocoles ne peut envoyer ou recevoir de paquets jusqu'à ce que PAgP attache leurs agports à un ou plusieurs ports physiques.
- **Capacité de groupe** - chaque port physique et agport possède un paramètre de configuration appelé la capacité de groupe. Un port physique peut être agrégé avec un autre port physique si et seulement s'il a la même capacité de groupe.
- **Procédure d'agrégation** - quand un port physique atteint les états d' UpData ou d' UpPAgP , il est attaché à un agport approprié. Quand il laisse l'un ou l'autre de ces états pour un autre état, il est détaché de l'agport.

Des définitions des états et des procédures de création sont données dans cette table :

État	Signification
`UpData`	Aucun paquet PAgP n'a été reçu. Des paquets PAgP sont envoyés. Le port physique est le seul connecté à son 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.
`UpPAgP`	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 ce que va être le groupement, défini en tant que plus grand groupe de ports dans l'agport qui est permis par les deux extrémités de la connexion.

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 d'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 a expiré est enlevé 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 dans un canal existant échoue, (par exemple, port débranché, convertisseur

d'interface Gigabit [GBIC] retiré, ou fibre cassée), l'agport est mis à jour et le trafic est haché via les liaisons restantes en une 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.

Remarque: Le comportement quand une liaison échoue dans un canal en raison d'une mise hors tension ou du retrait d'un module peut être différent. Par définition, il faut deux ports physiques dans un canal. 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. Ceci signifie que le trafic peut être ignoré jusqu'à ce que STP permette au port de devenir disponible aux données de nouveau.

Il y a une exception à cette règle sur Catalyst 6500/6000. Dans les versions antérieures à CatOS 6.3, un agport ne passe pas en état down pendant la suppression de module si le canal est composé de ports sur les modules 1 et 2 seulement.

Cette différence entre les deux modes de défaillance est importante quand la maintenance d'un réseau est prévue, car il peut y avoir un TCN STP à considérer lorsque vous exécutez une suppression à chaud ou une mise en place d'un module. Comme indiqué, il est important de gérer chaque liaison physique dans le canal avec NMS puisque l'agport n'est pas affecté par une panne.

Voici quelques mesures à prendre afin d'atténuer un changement de topologie non désiré sur Catalyst 6500/6000 :

- Si un seul port est utilisé par module pour former un canal, trois modules ou plus doivent être utilisés (trois ports ou plus au total).
- Si le canal enjambe deux modules, deux ports sur chaque module doivent être utilisés (quatre ports au total).
- Si un canal à deux ports est nécessaire sur deux cartes, utilisez seulement les ports de Supervisor Engine.
- Passez à CatOS 6.3, qui gère la suppression de module sans recalcul STP pour des canaux répartis sur plusieurs modules.

Options de configuration

Des EtherChannels peuvent être configurés dans différents modes, comme récapitulé dans cette table :

Mode	Options configurables
`Sur`	PAgP non en fonction. Le port canalise indépendamment de la façon dont le port voisin est configuré. Si le mode du port voisin est on, un canal est formé.
`Outre de`	Le port ne canalise pas, indépendamment de la façon dont le port voisin est configuré.
`Auto (defa ult)`	L'agrégation est sous le contrôle du protocole PAgP. Place un port en état negotiating passif, et aucun paquet PAgP n'est envoyé sur l'interface jusqu'à ce qu'au moins un paquet PAgP soit reçu et indique que l'expéditeur fonctionne en mode

	desirable .
`Desirable`	L'agrégation est sous le contrôle du protocole PAgP. Place un port en état negotiating actif, dans lequel le port entame des négociations avec d'autres ports en envoyant des paquets PAgP. Un canal est formé avec un autre groupe de ports en mode desirable ou auto.
Non-silent (par défaut sur les ports fibres GE et FE Catalyst 5500/5000)	Un mot clé en mode auto ou desirable. Si aucun paquet de données n'est reçu sur l'interface, alors l'interface n'est jamais attachée à un agport et ne peut pas être utilisée pour des données. Ce contrôle de bidirectionnalité a été créé spécialement pour le matériel Catalyst 5500/5000 car certaines défaillances de liaison ont comme conséquence la dislocation du canal. Puisque le mode non-silent est activé, 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 (par défaut sur tous les ports cuivre Catalyst 6500/6000, 4500/4000 et 5500/5000)	Un mot clé en mode auto ou desirable. Si aucun paquet de données n'est reçu sur l'interface après une période d'expiration de 15 secondes, l'interface est attachée par elle-même à un agport et peut être utilisée ainsi 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.

La configuration silent/non-silent affecte la manière dont les ports réagissent aux situations qui entraînent un trafic unidirectionnel ou la façon dont ils réalisent un basculement. Quand un port ne peut pas transmettre (en raison d'une sous-couche physique en échec [PHY] ou d'une fibre ou d'un câble cassé, par exemple), le port voisin peut tout de même rester en état opérationnel. Le partenaire continue à transmettre des données, mais des données sont perdues, car 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.

Quelques ports fibre ont la capacité désirée de faire passer le port en état non-opérationnel quand il perd son signal de réception (FEFI). Cela force le port partenaire 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 (telles que des BPDU) et qui ne peuvent pas détecter des conditions unidirectionnelles, le mode non-silent doit être utilisé afin de permettre aux ports de rester non-opérationnels jusqu'à ce que les données de réception soit présentes et que la liaison soit confirmée comme étant bidirectionnelle. PAgP met environ 3,5 * 30 secondes = 105 secondes à détecter une liaison unidirectionnelle, où 30 secondes représente le temps entre deux messages PAgP successifs. L'UDLD est recommandé comme détecteur plus rapide des liens unidirectionnels.

Quand vous utilisez des périphériques qui ne transmettent aucune donnée, le mode silent doit être utilisé. Ceci force le port à se connecter et à rester opérationnel, que les données reçues soient présentes ou pas. En outre, pour les ports qui peuvent détecter la présence d'une condition unidirectionnelle, telle que de plus récentes plates-formes utilisant L1 FEFI et UDLD, le mode silent est utilisé par défaut.

Vérification

la table présente un résumé de tous les possible scénarios de modes de canalisation 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 (c'est-à-dire, certaines des combinaisons arrêtent les ports du côté canalisation).

Mode canal du commutateur A	Mode canal du commutateur B	État du canal
Sur	Sur	Channel (non-PAgP)
Sur	Outre de	Not Channel (errdisable)
Sur	Automatique	Not Channel (errdisable)
Sur	Desirable	Not Channel (errdisable)
Outre de	Sur	Not Channel (errdisable)
Outre de	Outre de	Not Channel
Outre de	Automatique	Not Channel
Outre de	Desirable	Not Channel
Automatique	Sur	Not Channel (errdisable)
Automatique	Outre de	Not Channel

Automatique	Automatique	Not Channel
Automatique	Desirable	Canal PAgP
Desirable	Sur	Not Channel (errdisable)
Desirable	Outre de	Not Channel
Desirable	Automatique	Canal PAgP
Desirable	Desirable	Canal PAgP

Recommandation

Cisco recommande d'activer PAgP sur toutes les connexions de canal commutateur à commutateur et d'éviter le mode on . La méthode idéale consiste à définir le mode desirable aux deux extrémités de la liaison. La recommandation supplémentaire est de laisser le mot clé silent/non-silent sur la valeur par défaut - silent sur les commutateurs Catalyst 6500/6000 et 4500/4000, et non-silent sur les ports fibre Catalyst 5500/5000.

Comme évoqué dans ce document, l'explicite configuration de la canalisation sur tous les autres ports est utile pour la transmission rapide de données. Il faut éviter d'attendre l'expiration de PAgP pendant 15 secondes sur un port qui n'est pas utilisé pour la canalisation, d'autant plus que le port est alors remis à STP, qui lui-même peut prendre 30 secondes pour permettre la transmission de données, plus potentiellement 5 secondes pour le DTP, ce qui fait un total de 50 secondes. La commande **set port host** est traitée plus en détails dans la section STP de ce document.

```
set port channel port range mode desirable

set port channel port range mode off
!--- Ports not channeled; part of the set port hostcommand.
```

Cette commande assigne des canaux à un numéro de groupe admin, vu avec une commande show channel group. L'ajout et le retrait de ports de canalisation sur le même agport peuvent alors être gérés par le numéro d'admin si désiré.

Autres options

Une autre configuration commune pour les clients qui ont une administration minimale de la couche d'accès consiste à définir le mode sur desirable au niveau des couches de distribution et centrales, et de laisser les commutateurs de la couche d'accès sur leur configuration automobile par défaut.

Quand vous canalisez vers des périphériques qui ne prennent pas en charge PAgP, le canal doit être encodé sur on. Ceci s'applique aux périphériques tels que les serveurs, Local Director, les commutateurs de contenu, les routeurs, les commutateurs avec un logiciel plus ancien, les commutateurs Catalyst XL, et Catalyst 8540s. Émettez la commande suivante :

```
set port channel port range mode on
```

La nouvelle norme IEEE LACP 802.3ad, disponible dans CatOS 7.x, remplacera vraisemblablement PAgP à long terme parce qu'elle apporte l'avantage de l'interopérabilité entre plate-formes et constructeurs.

Protocole de contrôle d'agrégation de lien

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 qui peut être exécuté seulement sur les commutateurs Cisco et 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. Les versions du logiciel CatOS 7.x ont introduit la prise en charge de LACP.

Il y a très peu de différence entre le LACP et le PAgP d'un point de vue fonctionnel. Les deux protocoles prennent en charge 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
- 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 le LACP ne prend pas en charge les ports bidirectionnels en alternat.
- Le LACP prend en charge les ports de veille. 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, tous les ports qui ne peuvent pas être activement inclus dans le canal sont mis en état de veille et utilisés seulement si un des ports utilisés échoue. Un exemple d'une situation dans laquelle le LACP ne peut pas agréger tous les ports compatibles est si le système distant a des limitations matérielles plus restrictives.

Remarque: Dans CatOS, le nombre maximal de ports auxquels la même clé administrative peut être assignée est de huit. Dans le logiciel Cisco IOS, LACP essaye de configurer le nombre maximal de ports compatibles dans un EtherChannel, jusqu'au nombre maximal que le matériel autorise (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 multicast, **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 associés sur 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 à l'associé. 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, la capacité d'établir ces paramètres est nécessaire :

- un identifiant global unique pour chaque système participant à l'agrégation de liaisonsChaque système qui exécute LACP doit se voir assigner une priorité qui peut être choisie automatiquement ou par l'administrateur. La priorité système par défaut est 32768. 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 comprendChaque port du système doit se voir assigner une priorité automatiquement ou par l'administrateur. 128 est établi par défaut. La priorité est utilisée en conjonction avec le numéro de port afin de former l'identifiant de port.
- Un moyen d'identifier un groupe d'agrégation de liaisons et son agrégateur associéLa capacité d'un port à s'agréger avec un autre est récapitulée par un paramètre de 16 bits simple de nombre entier qui est strictement plus grand que zéro. Ce paramètre s'appelle « la clé ». Différents facteurs déterminent chaque clé, comme :Les caractéristiques physiques de port, qui incluent :Débit de donnéesDuplexityPoint à point ou médium partagéContraintes de configuration que l'administrateur réseau établitDeux clés sont associées à chaque port :Une clé administrative - elle permet au responsable de manipuler les valeurs clé. Un utilisateur peut choisir cette clé.Une clé opérationnelle - le système utilise cette clé afin de former des agrégations. Un utilisateur ne peut pas choisir ou directement changer cette clé.L'ensemble de ports d'un système qui partagent la même valeur de clé opérationnelle sont considérés comme des membres du même groupe de clés.

Si vous avez deux systèmes et un ensemble de ports avec la même clé administrative, chaque système essaie d'agréger les ports. Chaque système commence à partir du port à la priorité la plus élevée dans le système à la priorité la plus élevée. Ce comportement est possible parce que chaque système connaît sa propre priorité, que l'utilisateur ou le système a assignée, et la priorité de son partenaire, qui a été découverte par les paquets LACP.

Comportement en cas de panne

Le comportement en cas de panne pour LACP est identique au comportement pour PAgP. Si une liaison dans un canal existant est en échec, l'agport est mis à jour et le trafic est haché via les liaisons restantes en une seconde. Une liaison peut échouer pour ces raisons et d'autres encore :

- Un port est débranché

- Un GBIC est retiré
- Une fibre est cassée
- Défaillance matérielle (interface ou module)

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

Des EtherChannels LACP peuvent être configurés dans différents modes, comme récapitulé dans cette table :

Mode	Options configurables
Sur	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.
Outre de	Le port ne canalise pas, indépendamment de la façon dont le port voisin est configuré.
Passif (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 active) lance une négociation en envoyant un paquet LACP. Le commutateur reçoit et répond au paquet, et forme 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 afin de former un aglink. L'agrégat de liaisons est formé si l'autre extrémité s'exécute en mode LACP active ou passive .

Vérification (LACP et LACP)

La table 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 mener STP à mettre les ports du côté canalisation en état errdisable. Ceci signifie que certaines des combinaisons arrêtent les ports canalisation.

Mode canal du commutateur A	Mode canal du commutateur B	État du canal du commutateur A	État du canal du commutateur B

Sur	Sur	Canal (non LACP)	Canal (non LACP)
Sur	Outre de	Not Channel (errdisable)	Not Channel
Sur	Passif	Not Channel (errdisable)	Not Channel
Sur	Actif	Not Channel (errdisable)	Not Channel
Outre de	Outre de	Not Channel	Not Channel
Outre de	Passif	Not Channel	Not Channel
Outre de	Actif	Not Channel	Not Channel
Passif	Passif	Not Channel	Not Channel
Passif	Actif	Canal LACP	Canal LACP
Actif	Actif	Canal LACP	Canal LACP

Vérification (LACP et PAgP)

La table 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. Ceci signifie que certaines des combinaisons arrêtent les ports canalisation.

Mode canal du commutateur A	Mode canal du commutateur B	État du canal du commutateur A	État du canal du commutateur B
Sur	Sur	Canal (non LACP)	Channel (non-PAgP)
Sur	Outre de	Not Channel (errdisable)	Not Channel
Sur	Automatique	Not Channel (errdisable)	Not Channel
Sur	Desirable	Not Channel (errdisable)	Not Channel
Outre de	Sur	Not Channel	Not Channel (errdisable)
Outre de	Outre de	Not Channel	Not Channel
Outre de	Automatique	Not Channel	Not Channel
Outre de	Desirable	Not Channel	Not Channel
Passif	Sur	Not Channel	Not Channel (errdisable)
Passif	Outre de	Not Channel	Not Channel
Passif	Automatique	Not Channel	Not Channel
Passif	Desirable	Not Channel	Not Channel
Actif	Sur	Not Channel	Not Channel (errdisable)
Actif	Outre de	Not Channel	Not Channel
Actif	Automatique	Not Channel	Not Channel
Actif	Desirable	Not Channel	Not Channel

Recommandation

Cisco recommande d'activer PAgP sur des connexions de canal entre les commutateurs Cisco. Quand vous canalisez vers des périphériques qui ne supportent pas PAgP mais supportent LACP, activez LACP via la configuration de LACP active sur les deux extrémités des périphériques. Si l'extrémité des périphériques ne supporte pas LACP ou PAgP, vous devez encoder le canal sur on.

- **set channelprotocol lacp** *module*

  Sur les commutateurs qui exécutent CatOS, tous les ports sur Catalyst 4500/4000 et Catalyst 6500/6000 utilisent le protocole de canal PAgP par défaut et n'exécutent donc pas LACP. Afin de configurer des ports pour utiliser LACP, vous avez besoin de 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.
- **set port lacp-channel** *port_range admin-key*
  Un paramètre **admin key** (clé administrative) est échangé dans le paquet LACP. Un canal se forme seulement entre les ports qui ont la même clé admin. La commande set port lacp-channel port_range admin-key assigne aux canaux un numéro de clé admin. La commande show lacp-channel group affiche le numéro. La commande **set port lacp-channel port_range admin-key** assigne la même clé admin à tous les ports de la même plage. La clé admin est assignée aléatoirement si aucune clé spécifique n'est configurée. Puis, vous pouvez vous référer à la clé admin, si désiré, pour gérer l'ajout et le retrait de ports de canalisation au même agport.
- **set port lacp-channel** *port_range* **mode active**
  La commande **set port lacp-channel port_range mode active** fait passer le mode de canal en active pour une série de ports qui étaient auparavant assignés à la même clé admin.

En outre, 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 des informations LACPDU reçues est de 90 quand vous utilisez des délais d'expiration longs (3 x Slow_Periodic_Time). Utilisez UDLD, qui est un détecteur plus rapide de liens unidirectionnels. Vous ne pouvez pas ajuster les timers LACP, et aujourd'hui vous ne pouvez pas configurer les commutateurs pour employer la transmission rapide PDU (chaque seconde) afin de maintenir le canal après que le canal soit formé.

Autres options

Si vous avez un modèle de gestion minimal au niveau de la couche d'accès, une configuration commune consiste à définir le mode sur active au niveau de la couche de distribution et des couches centrales. Laissez les commutateurs de la couche d'accès sur leur configuration passive par défaut.

Unidirectional Link Detection

L'UDLD est un protocole propriétaire Cisco et léger qui a été développé pour détecter des instances de transmissions unidirectionnelles entre les périphériques. Bien qu'il y ait d'autres méthodes pour détecter l'état bidirectionnel de média de transmission, comme FEFI, il y a certaines instances dans lesquelles les mécanismes de détection L1 ne sont pas suffisants. Ces

scénarios peuvent avoir comme conséquence l'une de ces occurrences :

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

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

- Surveillez les configurations de câblage physiques et arrêtez les ports mal câbles en tant que errdisable.
- Protégez-vous des liens unidirectionnels. 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 errdisable, et un message Syslog correspondant est produit.
- En outre, le mode UDLD agressif vérifie qu'une liaison précédemment considérée comme bidirectionnelle ne perd pas la connectivité en cas de congestion, devenant ainsi inutilisable. UDLD effectue des tests de connectivité permanents sur la liaison. L'objectif principal du mode UDLD agressif est d'éviter la formation de trous noirs dans le trafic dans certaines conditions d'échec.

Spanning-tree, avec du son flux BPDU équilibré et unidirectionnel, était une victime grave de ces pannes. Il est facile de voir comment un port peut soudainement ne pouvoir pas transmettre de BPDU, entraînant chez STP une modification d'état de blocking à forwarding sur le voisin. Cette modification crée une boucle, puisque le port peut encore recevoir.

Aperçu opérationnel

UDLD est un protocole L2 qui fonctionne sur la couche LLC (adresse MAC de destination 01-00-0c-cc-cc-cc, protocole SNAP HDLC 0x0111). En exécutant UDLD en combinaison avec FEFI et des mécanismes d'autonégociation L1, il est possible de valider l'intégrité physique (L1) et logique (L2) d'une liaison.

UDLD prévoit des fonctionnalités et une protection que FEFI et l'autonégociation ne peuvent pas exécuter, à savoir la détection et la mise en cache des informations sur les voisins, la capacité d'arrêter tous les ports mal connectés, et détecte les dysfonctionnements de l'interface logique/port ou les défauts sur les liaisons qui ne sont pas point par point (ceux traversant les convertisseurs de supports ou les concentrateurs).

UDLD emploie deux mécanismes de base ; il se renseigne sur les voisins, maintient l'information à jour dans un cache local et envoie une série de messages sonde/écho UDLD toutes les fois qu'il détecte un nouveau voisin ou toutes les fois qu'un voisin demande une resynchronisation du cache.

UDLD envoie constamment des messages sondes sur tous les ports sur lesquels UDLD est activé. Toutes les fois qu'un message « déclenchant » UDLD est reçu sur un port, une phase de détection et un processus de validation débute. Si toutes les conditions valides sont satisfaites à la fin de ce processus, l'état du port n'est pas modifié. Afin de remplir les conditions, le port doit être bidirectionnel et correctement câblé. Autrement, le port est errdisable, et un message syslog s'affiche. Le message syslog est semblable à ces messages :

- `UDLD-3-DISABLE : Unidirectional link detected on port [dec]/[dec]. Port disabled`
- `UDLD-4-ONEWAYPATH : A unidirectional link from port [dec]/[dec] to port[[dec]/[dec] of device [chars] was detected`

Référez-vous à Messages et procédures de récupération (commutateurs de la gamme Catalyst 7.6) pour une liste complète de messages système par installation, ce qui inclut les événements UDLD.

Une fois une liaison établie et classée comme bidirectionnel, UDLD continue à envoyer des messages sonde/écho à un intervalle de 15 secondes par défaut. Cette table représente les états valides de liaisons UDLD comme signalé dans la sortie de la commande **show udld port** :

État du port	Commentaire
Indéterminé	Détection en cours, ou une entité UDLD voisine a été désactivée ou sa transmission a été bloquée.
Sans objet	UDLD a été désactivé.
Arrêt	Une liaison unidirectionnelle a été détectée et le port a été désactivé.
Bidirectionnel	Une liaison bidirectionnelle a été détectée.

- **Entretien du cache 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 sonde 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 timer time-to-live correspondant est réinitialisé.
- Afin de maintenir l'intégrité du cache UDLD, toutes les fois qu'une interface avec UDLD est désactivée ou un périphérique réinitialisé, toutes les entrées de cache existante pour les interfaces affectées par le changement de configuration sont effacées et UDLD transmet au moins un message pour informer les voisins respectives qu'il faut vider les entrées de cache correspondantes.
- **Mécanisme de détection d'écho** - le mécanisme faisant 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 se ferme et qu'aucune réponse valide n'a été reçue, la liaison est considérée comme unidirectionnelle, et un processus de rétablissement de la liaison ou de fermeture du port peut être déclenché.

Temps de convergence

Afin d'éviter des boucles STP, CatOS 5.4(3) a ramené l'intervalle des messages par défaut d'UDLD de 60 secondes à 15 secondes afin d'arrêter une liaison unidirectionnelle avant qu'un port bloqué n'arrive à passer en état de transmission.

Remarque: 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 les voisins UDLD sont établis, l'intervalle des messages configuré est envoyé

et le délai d'expiration pour cet homologue est calculé pour être (3 * message_interval). Par conséquent, un rapport de partenariat expire après trois sondes consécutives manquées. Avec les intervalles des messages différents de chaque côté, cette valeur d'expiration est différente de chaque côté.

Le temps approximatif qui est nécessaire pour qu'UDLD détecte une défaillance unidirectionnelle est approximativement (2,5 * message_interval + 4 secondes), ou environ 41 secondes avec l'utilisation de l'intervalle des messages par défaut de 15 secondes. Ce chiffre est largement inférieur aux 50 secondes qui sont habituellement nécessaires pour que STP reconverge. Si le CPU NMP a quelques cycles disponibles et si vous surveillez soigneusement son niveau d'utilisation, vous pouvez ramener l'intervalle des messages (même) au minimum de 7 secondes. Cet intervalle des messages aide à accélérer la détection de manière significative.

Par conséquent, UDLD une dépendance assumée aux timers de spanning tree par défaut. Si vous accordez STP pour converger plus rapidement qu'UDLD, considérez un mécanisme alternatif, tel que la fonctionnalité de protection contre les boucles de CatOS 6.2. Considérez également un mécanisme alternatif quand vous mettez en application RSTP (IEEE 802.1w) parce que RSTP a des caractéristiques de convergence en millisecondes, ce qui dépend de 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 empêche la formation de boucles STP avec la vitesse du STP en service, et UDLD détecte les connexions unidirectionnelles sur différentes liaisons Etherchannel ou dans les cas dans lesquels les BPDU ne circulent pas dans la direction cassée.

Remarque: 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 * FwdDelay + Maxage). Pour cette raison, Cisco recommande d'installer UDLD en conjonction avec le dispositif de protection contre les boucles (qui a été présenté dans CatOS 6.2) dans les topologies qui s'appuient sur STP.

Attention : Prenez garde des versions antérieures d'UDLD qui utilisent un intervalle des messages par défaut non configurable de 60 secondes. Ces versions sont sensibles aux boucles de spanning tree.

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 de PDU UDLD est symétrique et les deux extrémités expirent, aucun des deux ports n'est errdisabled.
- Un côté d'une liaison a un port coincé (les deux transmettent [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 L1, est désactivé.
- Une réduction de la confiance dans les mécanismes L1 FEFI est désirable.
- La 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 L1 est désactivé ou inutilisable. C'est particulièrement vrai avec les connexions EtherChannel parce que PAgP/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 ajouté de prévenir de potentielles boucles de spanning tree.

Il est plus difficile de caractériser les circonstances qui contribuent à la perte symétrique de sondes d'analyse d'UDLD. Vous devez comprendre qu'UDLD en mode normal vérifie l'existence d'une liaison unidirectionnelle, même après que la liaison a atteint un état bidirectionnel. L'intention d'UDLD est de détecter les problèmes L2 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 normal en même temps que l'autonégociation et le protection contre les boucles (pour les réseaux qui s'appuient sur STP) est presque toujours suffisante. Cependant, le mode UDLD agressif est salutaire dans les situations dans lesquelles la congestion est égale dans les deux directions, cd qui entraîne la perte de sondes UDLD dans les deux directions. Par exemple, cette perte de sondes UDLD peut se produire si l'utilisation du CPU sur chaque extrémité de la liaison est élevée. D'autres exemples de la perte de connectivité bidirectionnelle incluent la défaillance d'un de ces périphériques :

- Un transpondeur de multiplexage en longueur d'onde dense (DWDM)
- Un convertisseur de supports
- Un concentrateur
- Un autre périphérique L1**Remarque:** La défaillance ne peut pas être détectée par l'autonégociation.

L'erreur d'UDLD agressif désactive le port dans ces situations de panne. Considérez les ramifications soigneusement quand vous activez le mode UDLD agressif sur les liaisons qui ne sont pas point à point. Les liens avec des convertisseurs de supports, des concentrateurs, ou des périphériques semblables ne sont pas point à point. Des équipements intermédiaires peuvent empêcher l'expédition de paquets UDLD et forcer une liaison à être arrêtée inutilement.

Une fois que tous les voisins d'un port ont vieilli, le mode UDLD agressif (s'il est activé) relance la séquence de liaison pour tenter de resynchroniser avec les voisins potentiellement hors-synchronisation. Cet effort a lieu pendant l'annonce ou la phase de détection. 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: Quelques commutateurs ne sont pas compatibles avec le mode UDLD agressif. Actuellement, les commutateurs Catalyst 2900XL et Catalyst 3500XL ont des intervalles de messages encodés de 60 secondes. Cet intervalle n'est pas considéré comme suffisamment rapide protéger contre de potentielles boucles STP (avec l'utilisation des paramètres STP par défaut).

UDLD sur des liaisons routées

Dans le cadre de cette discussion, une liaison routée est l'un de ces deux types de connexion :

- Point à point entre deux noeuds de routeurCette liaison est configurée avec un masque de sous-réseau 30 bits.
- UN VLAN avec plusieurs ports mais qui supporte seulement les connexions routéesUn exemple est une topologie de noyau L2 fractionné.

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. Les caractéristiques dont traite cette section 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).

D'abord, notez qu'une panne L1 ou L2 sur n'importe quel réseau routé point à point résulte dans le démontage presque immédiat de la connexion L3. Puisque le seul port de commutation dans ce VLAN passe à un état non-connect en cas de panne L1/L2, la fonctionnalité d'auto-état MSFC synchronise les états du port L2 et L3 en approximativement deux secondes. Cette synchronisation place l'interface L3 VLAN dans un état actif/inactif (avec le protocole de ligne inactif).

Assumez les valeurs de timer par défaut. OSPF envoie des messages de sonde 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. Ce basculement est le cas même si la panne L1/L2 n'est pas pure sur une connexion point-à-point, qui laisse un scénario à demi opérationnel auquel le protocole L3 doit faire face. 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 L3 point-à-point sont limités.

Dans de nombreux cas, EIGRP converge plus rapidement qu'OSPF. Cependant, vous devez noter que la transmission bidirectionnelle n'est pas nécessaire pour que les voisins échangent 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 mode normal peut alléger les circonstances dont parle cette section. UDLD mode normal détecte la défaillance de liaison unidirectionnelle et l'erreur désactive le port.

Pour les connexions routées L3 qui utilisent n'importe quel protocole de routage, UDLD mode normal assure toujours la protection contre les problèmes qui peuvent se produire au lancement de liaison initial. Ces problèmes incluent un mauvais câblage ou un matériel défectueux. En outre, le mode UDLD agressif fournit ces avantages sur les connexions routées L3 :

- Empêche la formation de trous noirs dans le trafic**Remarque:** Des timers minimaux sont requis dans certains cas.
- Place une liaison oscillante en état errdisable
- Protège contre les boucles qui résultent des configurations de l'EtherChannel L3

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, UDLD est désactivé par défaut sur les ports cuivre. Les ports cuivre tendent à être utilisés pour l'accès à l'hôte.

Remarque: UDLD doit être activé globalement et au niveau de l'interface avant que les voisins ne puissent atteindre le état bidirectionnel. Dans CatOS 5.4(3) et versions ultérieures, l'intervalle de messages par défaut est de 15 secondes et est configurable entre 7 et 90 secondes.

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. Vous pouvez manuellement empêcher une réactivation de port en définissant le délai d'expiration errdisable de ce port sur disable. **Émettez la commande set port errdisable-timeout mod/port disable .**

Remarque: L'utilisation de cette commande dépend de la version de votre logiciel.

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 Configuration de la commutation Ethernet, Fast Ethernet, Gigabit Ethernet et 10-Gigabit Ethernet pour plus de détails sur la façon dont configurer un délai d'expiration pour les ports qui sont en état errdisable.

Recommandation

Le mode normal d'UDLD est suffisant dans la vaste majorité des cas si vous l'utilisez correctement et en même temps que les fonctionnalités et les protocoles appropriés. Ces fonctionnalités/protocoles incluent :

- FEFI
- Négociation automatique
- Protection de boucle

Quand vous vous déployez UDLD, considérez si un test continu de la connectivité bidirectionnelle (mode agressif) est nécessaire. Typiquement, si l'autonégociation est activée, le mode agressif n'est pas nécessaire parce que l'autonégociation compense la détection de panne sur L1.

Cisco recommande d'activer le mode normal d'UDLD sur toutes les liaisons point à point FE/GE entre les commutateurs Cisco sur lesquels l'intervalle de messages d'UDLD est défini sur la valeur par défaut de 15 secondes. Cette configuration assume les timers de spanning 802.1d par défaut. En outre, utilisez UDLD en même temps que le dispositif de protection contre les boucles dans les réseaux qui s'appuient sur STP pour la redondance et la convergence. Cette recommandation s'applique aux réseaux dans lesquels il y a un ou plusieurs ports en état de blocage STP dans la topologie.

Émettez ces commandes afin d'activer UDLD :

```
set udld enable
!--- After global enablement, all FE and GE fiber !--- ports have UDLD enabled by default. set udld enable port range
!--- This is for additional specific ports and copper media, if needed.
```

Vous devez manuellement activer les ports qui sont désactivés pour erreur en raison de symptômes de liaisons unidirectionnels. Émettez la commande **set port enable** .

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

Autres options

Pour une protection maximale contre les symptômes qui résultent des liens unidirectionnels, configurez la détection UDLD en mode agressif :

set udld aggressive-mode enable *port_range*

En outre, vous pouvez accorder la valeur d'intervalle des messages UDLD entre 7 et 90 secondes à chaque extrémité, si supporté, pour une convergence plus rapide :

set udld interval *time*

Considérez l'utilisation de la fonctionnalité d'expiration errdisable sur n'importe quel périphérique qui peut devenir isolé du réseau en cas d'une situation errdisable. Cette situation est en général vraie dans la couche d'accès et quand vous mettez en application le mode UDLD agressif sans capacités d'administration de réseau hors bande.

Si un port est placé en état errdisable, le port reste inactif par défaut. Vous pouvez émettre cette commande qui permet de réactiver des ports après un délai d'expiration :

Remarque: Le délai d'expiration est de 300 secondes par défaut.

```
>set errdisable-timeout enable ?
bpdu-guard
!--- This is BPDU port-guard. channel-misconfig !--- This is a channel misconfiguration. duplex-
mismatch udld other !--- These are other reasons. all !--- Apply errdisable timeout to all
reasons.
```

Si le périphérique associé n'est pas compatible UDLD, comme un hôte d'extrémité ou un routeur, n'exécutez pas le protocole. Émettez la commande suivante :

set udld disable *port_range*

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 et débranchez un brin d'une fibre afin de voir l'état errdisable désiré, vous devez avoir arrêté l'autonégociation L1. Autrement, le port physique se désactive, ce qui réinitialise la communication de messages UDLD. L'extrémité distante passe en état indéterminé en mode UDLD normal. Si vous utilisez le mode UDLD agressif, l'extrémité distante passe en état errdisable.

Il existe une autre méthode de test pour simuler la perte de PDU voisin pour UDLD. Utilisez des filtres par adresse MAC afin de bloquer l'adresse matérielle UDLD/CDP mais de laisser passer d'autres adresses.

Émettez ces commandes afin de surveiller UDLD :

```
>show udld

UDLD              : enabled
Message Interval  : 15 seconds
```

```
>show udld port 3/1

UDLD              : enabled
Message Interval  : 15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
3/1      enabled       disabled         bidirectional
```

À partir du mode enable, vous pouvez aussi émettre la commande masquée show udld neighbor afin de contrôler le contenu de cache d'UDLD (de la même manière que CDP). Une comparaison du cache d'UDLD avec le cache CDP afin de vérifier s'il y a une anomalie spécifique au protocole est souvent utile. Toutes les fois que CDP est également affecté, tous les PDUs/BPDUs sont en général affectés. Contrôlez par conséquent STP également. Par exemple, vérifiez les modifications récentes d'identité de racine ou de placement de racine/port désigné.

```
>show udld neighbor 3/1

Port  Device Name            Device ID    Port-ID OperState
----- --------------------  ------------ ------- ----------
3/1   TSC07117119M(Switch)   000c86a50433 3/1     bidirectional
```

En outre, vous pouvez surveiller l'état UDLD et la cohérence de configuration grâce aux variables Cisco UDLD SNMP MIB.

Trame étendue

La taille d'une unité de transmission maximale (MTU) est de 1518 octets par défaut pour tous les ports Ethernet, ce qui inclut GE et 10 GE. La fonctionnalité de trame étendue permet aux interfaces de commuter des trames qui sont plus grandes que la taille de trame Ethernet standard. Cette fonctionnalité est utile afin d'optimiser la performance de serveur à serveur et de soutenir les applications telles que la commutation multiprotocole par étiquette (MPLS), la tunnellisation 802.1Q, le protocole de tunnellisation L2 version 3 (L2TPv3), qui augmentent la taille des trames initiales.

Aperçu opérationnel

La spécification standard IEEE 802.3 définit une taille de trame Ethernet maximale de 1518 octets pour les trames normales et de 1522 octets pour les trames encapsulées 802.1Q. Les trames encapsulées 802.1Q sont désignées parfois sous le nom de « baby giants ». Généralement, les paquets sont classifiés en tant que trames géantes quand ils dépassent la longueur maximale spécifique Ethernets pour une connexion Ethernet spécifique. Les paquets géants sont également connus en tant que trames étendues.

Il existe diverses raisons pour lesquelles la taille du MTU de certaines trames peut dépasser 1518 octets. En voici quelques exemples :

- Conditions spécifiques au constructeur - Les applications et certains NIC peuvent spécifier une taille de MTU en dehors de la norme de 1500 octets. La tendance à spécifier de telles tailles de MTU est due à des études qui ont été entreprises et 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 de liaison agrégée sont l'encapsulation propriétaire Cisco ISL et IEEE 802.1Q.

- MPLS — Après que le MPLS soit activé sur une interface, il a le potentiel d'augmenter la taille de trame d'un paquet. Cette augmentation dépend du nombre d'étiquettes dans la pile d'étiquettes pour un paquet MPLS. La taille totale d'une étiquette est de 4 octets. La taille totale d'une pile d'étiquettes est de *n* x 4 octets. Si une pile d'étiquettes est formée, les trames peuvent dépasser le MTU.
- Tunnellisation 802.1Q - les paquets de tunnellisation 802.1Q contiennent deux étiquettes 802.1Q, dont seulement une à la fois est habituellement visible au matériel. Par conséquent, l'étiquette interne ajoute 4 octets à la valeur de MTU (taille de charge utile).
- Universal Transport Interface (UTI)/L2TPv3 - UTI/L2TPv3 encapsule les données L2 qui doivent être expédiées sur le réseau IP. L'encapsulation peut augmenter la taille de la trame initiale de jusqu'à 50 octets. La nouvelle trame inclut une nouvelle en-tête d'IP (20 octets), une en-tête L2TPv3 (12 octets), et une nouvelle en-tête L2. La charge utile L2TPv3 comprend la trame L2 entière, ce qui inclut l'en-tête L2.

La capacité des différents commutateurs Catalyst à supporter diverses tailles de trames dépend de beaucoup de facteurs, qui incluent le matériel et le logiciel. Certains modules peuvent prendre en charge de plus grandes tailles de trame que d'autres, même dans la même plate-forme.

- Les commutateurs Catalyst 5500/5000 prennent en charge les trames étendues dans CatOS 6.1. Quand la fonctionnalité de trames étendues est activée sur un port, la taille du MTU grimpe jusqu'à 9216 octets. Sur les cartes de ligne (UTP) torsadées et non blindées 10/100-Mbps, la taille de trame maximale qui est supportée est seulement 8092 octets. Cette limitation est une limitation d'ASIC. Il n'y a généralement aucune restriction dans l'activation de la fonction de taille de trame étendue. Vous pouvez utiliser cette fonctionnalité avec ou sans agrégation et avec ou sans canalisation.
- Les commutateurs Catalyst 4000 (supervisor engine 1 [WS-X4012] et supervisor engine 2 [WS-X4013]) ne supportent pas les trames étendues en raison d'une limitation ASIC. Cependant, l'exception est l'agrégation 802.1Q.
- La plate-forme de la gamme Catalyst 6500 peut supporter des trames étendues dans CatOS 6.1(1) et versions ultérieures. Cependant, cela dépend du type de cartes de ligne que vous utilisez. Il n'y a généralement aucune restriction dans l'activation de la fonction de taille de trame étendue. Vous pouvez utiliser cette fonctionnalité avec ou sans agrégation et avec ou sans canalisation. 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. La valeur de MTU par défaut n'est pas configurable avec l'utilisation de CatOS. **Cependant, le logiciel Cisco IOS Version 12.1(13)E a introduit la commande system jumbomtu afin de remplacer la valeur de MTU par défaut.**

Référez-vous à Exemple de configuration pour la prise en charge des trames étendues/géantes sur les commutateurs Catalyst pour plus d'informations.

Cette table décrit les tailles de MTU qui sont supportées par différentes cartes de ligne pour les commutateurs de la gamme Catalyst 6500/6000 :

Remarque: La taille de MTU ou de paquet se réfère seulement à la charge utile Ethernet.

Linecard	Taille de MTU
Par défaut	9216 octets
WS-X6248-RJ-45, WS-X6248A-RJ-45 WS-	8092

X6248-TEL, WS-X6248A-TEL WS-X6348-RJ-45(V), WS-X6348-RJ-21(V)	octets (limités par la puce PHY)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V) WS-X6148-45AF, WS-X6148-21AF	9100 octets (@ 100 Mbits/s) 9216 octets (@ 10 Mbits/s)
WS-X6148A-RJ-45, WS-X6148A-45AF, WS-X6148-FE-SFP	9216 octets
WS-X6324-100FX-MM, -SM, WS-X6024-10FL-MT	9216 octets
WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-MM WS-X6148X2-RJ-45, WS-X6148X2-45AF WS-X6196-RJ-21, WS-X6196-21AF WS-X6408-GBIC, WS-X6316-GE-TX , WS-X6416-GBIC WS-X6516-GBIC, WS-X6516A-GBIC, WS-X6816-GBIC Uplinks of Supervisor Engine 1, 2, 32 and 720	9216 octets
WS-X6516-GE-TX	8092 octets (@ 100 Mbits/s) 9216 octets (@ 10 ou 1000 Mbits/s)
WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF, WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF	1500 octets (trames étendues non supportées)
WS-X6148A-GE-TX, WS-X6148A-GE-45AF, WS-X6502-10GE, WS-X67xx Series	9216 octets
OSM ATM (OC12c)	9180 octets
OSM CHOC3, CHOC12, CHOC48, CT3	9216 octets (OCx et DS3) 7673 octets (T1/E1)
Flex WAN	7673

	octets (CT3 T1/DS0) 9216 octets (POS OC3c) 7673 octets (t1)
CSM (WS-X6066-SLB-APC)	9216 octets (à partir de CSM 3.1(5) et 3.2(1))
OSM POS OC3c, OC12c, OC48c; OSM DPT OC48c, OSM GE WAN	9216 octets

Prise en charge des trames étendues de couche 3

Avec CatOS qui s'exécute sur Supervisor Engine et le logiciel Cisco IOS qui s'exécute sur le MSFC, les commutateurs 6500/6000 fournissent également une prise en charge des trames étendues L3 dans Cisco IOS® 12.1(2) et versions ultérieures avec l'utilisation de PFC/MSFC2, de PFC2/MSFC2, ou de matériel postérieur. Si les VLAN d'entrée et de sortie sont configurés pour supporter les trames étendues, tous les paquets sont commutés au niveau matériel par PFC à la vitesse de câble maximale. Si l'entrée VLAN est configurée pour supporter les trames étendues mais pas la sortie, il y a deux scénarios :

- Une trame étendue envoyée par l'hôte d'extrémité avec l'ensemble de bits Don't Fragment (DF) (pour la détection de chemins MTU) - le paquet est relâché et un Internet Control Message Protocol (ICMP) inaccessible est envoyé à l'hôte d'extrémité avec le message codé fragment needed and DF set.
- Une trame étendue qui est envoyée par l'hôte d'extrémité avec un ensemble de bits DF non défini - les paquets sont pontés à MSFC2/MSFC3 afin d'être fragmentés et commutés dans le logiciel.

Cette table récapitule le support des trames étendues L3 pour diverses plates-formes :

Commutateur ou module L3	**Taille maximale du MTU L3**
Gamme Catalyst 2948G-L3/4908G-L3	Les trames étendues ne sont pas prises en charge.
Catalyst 5000 RSM[1]/RSFC2	Les trames étendues ne sont pas prises en charge.
Catalyst 6500 MSFC1	Les trames étendues ne sont pas prises en charge.
Catalyst 6500 MSFC2 et versions ultérieures	Logiciel Cisco IOS Version 12.1(2)E : 9216 octets

[1] RSM = module de route switch

[2] RSFC = carte fonctionnelle de route switch

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. Avec un RTT constant et la perte de paquets, vous pouvez doubler le débit TCP si vous doublez la taille du 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.

Deuxièmement, les exigences toujours croissantes de performance des parcs de serveurs exigent des moyens plus efficaces pour assurer des débits de données supérieurs avec des datagrammes de système de fichiers en réseau (NFS) UDP. Le NFS est le mécanisme de stockage de données le plus largement déployé pour transférer des fichiers entre les serveurs basés sur Unix, et il comporte des datagrammes 8400 octets. Etant donné le MTU étendu 9 Ko d'Ethernet, une seule trame étendue est assez grande pour porter un datagramme d'application de 8 Ko (par exemple, NFS) plus l'en-tête de paquet supplémentaire. Cette capacité permet également des transferts plus efficaces de l'accès direct à la mémoire sur les serveurs parce que le logiciel n'a pas besoin de davantage de capacités pour fragmenter les blocs NFS en datagrammes UDP distincts.

Recommandation

Quand vous voulez prendre en charge les trames étendues, contraignez l'utilisation des trames étendues sur les zones du réseau où tous les modules de commutation (L2) et les interfaces (L3) supportent les trames étendues. Cette configuration évite la fragmentation n'importe où sur le chemin. La configuration des trames étendues qui sont plus grandes que la longueur maximale supportée dans le chemin élimine tous les gains qui sont réalisés en employant cette fonctionnalité parce que la fragmentation est requise. Comme l'indiquent les tables dans cette section Trame étendue , différentes plate-formes et cartes de ligne peuvent varier en ce qui concerne la taille maximale de paquet supportée.

Configurez les périphériques sensibles aux trames étendues avec une taille de MTU qui est le dénominateur commun minimum supporté par le matériel réseau pour tout le VLAN L2 où réside le périphérique hôte. Afin d'activer le support des trames étendues sur les modules avec cette capacité de support, émettez cette commande :

```
set port jumbo mod/port enable
```

En outre, si vous désirez supporter les trames étendues au-delà des limites de L3, configurez la plus grande valeur disponible de MTU de 9216 octets sur toutes les interfaces VLAN applicables. Émettez la commande **mtu** sous les interfaces VLAN :

```
interface vlan vlan# mtu 9216
```

Cette configuration garantit que le MTU de trame étendue L2 qui est supporté par les modules est toujours inférieur ou égal à la valeur qui est configurée pour les interfaces L3 que traverse le trafic. Ceci empêche la fragmentation quand le trafic est routé du VLAN à travers l'interface L3.

Configuration de la gestion

Des considérations sur le contrôle, la provision et le dépannage d'un réseau Catalyst sont traitées dans cette section.

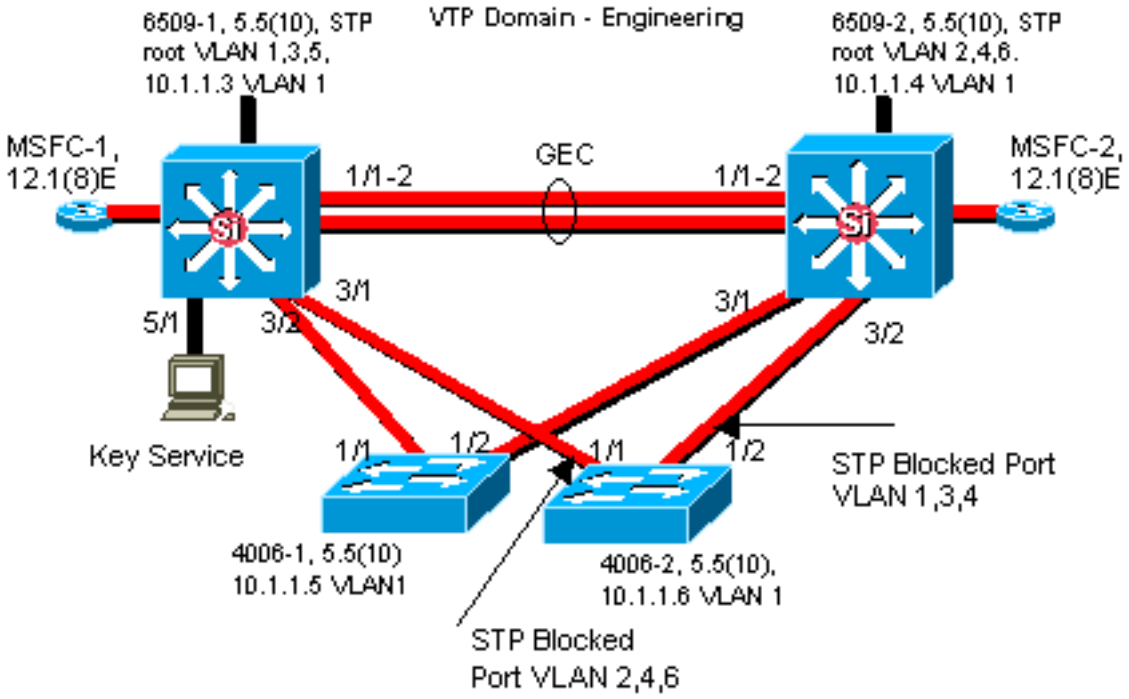
Diagrammes du réseau

Des diagrammes de réseau clairs sont une partie fondamentale du fonctionnement du réseau. Ils deviennent critiques pendant le dépannage et sont le véhicule le plus important simple pour la transmission d'informations une fois remontés aux constructeurs et aux associés pendant une panne. Leur préparation, promptitude et accessibilité ne doivent pas être sous-estimées.

Recommandation

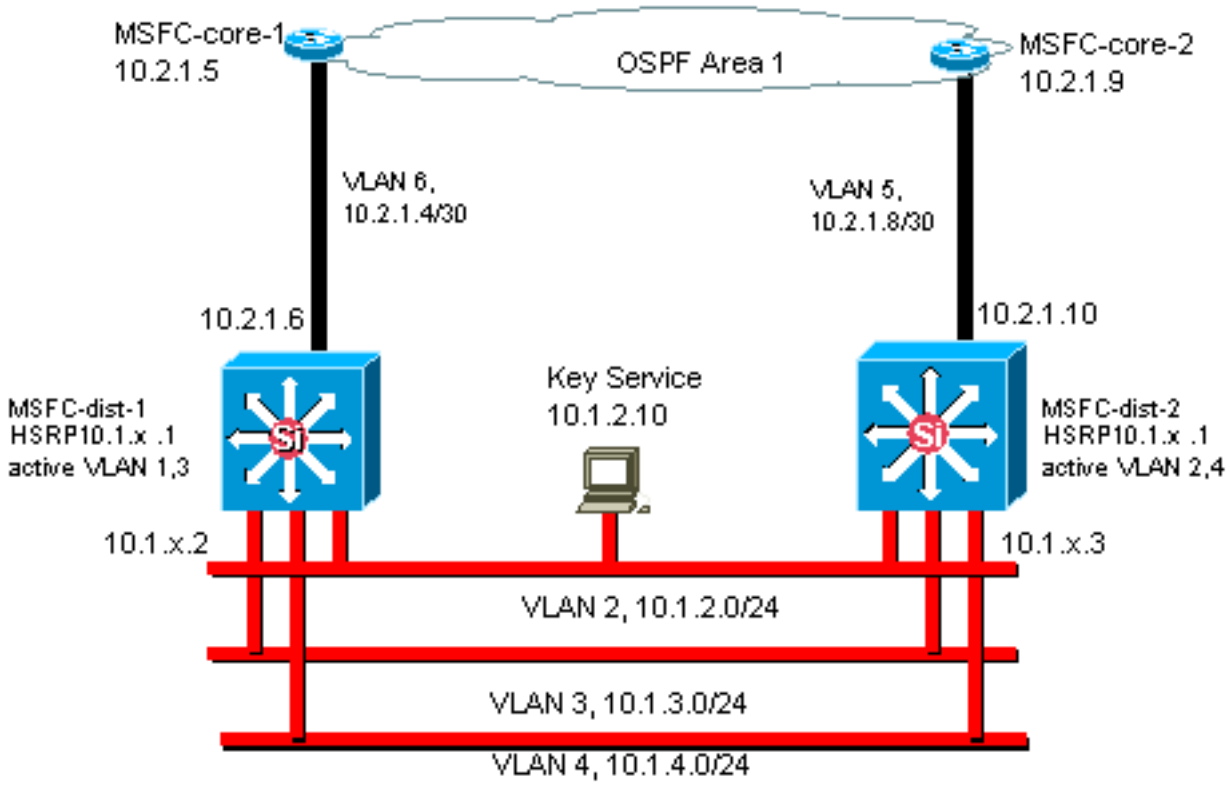
Cisco recommande de créer ces trois diagrammes :

- **Diagramme global** - même pour les plus grands réseaux, un diagramme qui montre la connectivité physique et logique de bout en bout est important. Il peut être commun pour les entreprises qui ont mis en application une conception hiérarchique pour documenter chaque couche séparément. Pendant la résolution des problèmes de planification, cependant, c'est souvent une bonne connaissance de la façon dont les domaines sont reliés qui importe.
- **Diagramme physique** - montre tout le matériel de commutation et de routage et le câblage. Les liaisons agrégées, les liaisons, les vitesses, les groupes de canaux, les numéros de port, les logements, les types de châssis, les logiciels, les domaines VTP, le pont racine, la priorité de pont racine de secours, l'adresse MAC et les ports bloqués par VLAN doivent être étiquetés. Il est souvent plus clair de dépeindre des équipements internes, tels que Catalyst 6500/6000 MSFC, comme un routeur sur une barrette connectée par une liaison



agrégée.

- **Diagramme logique** - n'affiche que la fonctionnalité L3 (routeurs comme objets, VLAN comme segments Ethernet). Les adresses IP, les sous-réseaux, l'adressage secondaire, le HSRP actif et en veille, les couches accès-centre-distribution et les informations de routage doivent être
étiquetés.



Gestion intrabande

Selon la configuration, l'interface de gestion (interne) de commutation intrabande (connue sous le nom de sc0) peut avoir à traiter ces données :

- Des protocoles de gestion de la commutation tels que SNMP, Telnet, Secure Shell Protocol

(SSH) et Syslog
- Des données utilisateur comme des diffusions et des multicasts
- Des protocoles de contrôle de la commutation tels que STP BPDUs, VTP, DTP, CDP, etc

Il est commun dans la conception Cisco multicouche de configurer un VLAN de gestion qui englobe un domaine commuté et contient toutes les interfaces sc0. Ceci aide à séparer le trafic d'administration du trafic utilisateur et augmente la sécurité des interfaces de gestion de la commutation. Cette section décrit l'importance et les problèmes potentiels d'utiliser le VLAN 1 par défaut et d'exécuter le trafic d'administration du commutateur dans le même VLAN que le trafic utilisateur.

Aperçu opérationnel

Le souci principal en ce qui concerne l'utilisation du VLAN 1 pour des données utilisateur est que Supervisor Engine NMP en général n'a pas besoin d'être interrompu par une grande partie du multicast et du trafic de diffusion qui est produit par les stations d'extrémité. Le matériel Catalyst 5500/5000 plus ancien, Supervisor Engine I et Supervisor Engine II en particulier, a des ressources limitées pour traiter ce trafic, bien que le principe s'applique à tous les Supervisor Engines. Si le CPU du Supervisor Engine, la mémoire tampon, ou le canal intrabande du fond de panier est entièrement occupé à écouter un trafic inutile, il est possible que des trames de contrôle soient manquées. Dans un pire scénario, ceci peut mener à une boucle de spanning tree ou une défaillance d'EtherChannel.

Si les commandes show interface et show ip stats sont émises sur Catalyst, elles peuvent donner une indication de la proportion de la diffusion vs trafic monodiffusion et du trafic IP vs non-IP (généralement non vu dans les VLAN de gestion).

Une autre vérification de l'intégrité pour un matériel Catalyst 5500/5000 plus ancien est d'examiner la sortie de **show inband** / **biga** (commande cachée) pour des erreurs de ressource (RscrcErrors), semblable aux abandons de mémoire tampon dans un routeur. Si ces erreurs de ressource se produisent continuellement, la mémoire n'est pas disponible pour recevoir des paquets système, peut-être en raison d'une importante quantité de trafic de diffusion dans le VLAN de gestion. Une erreur simple de ressource peut signifier que Supervisor Engine ne peut pas traiter un paquet tel que des BPDU, ce qui pourrait rapidement devenir un problème parce que les protocoles tels que le spanning tree ne renvoient pas les BPDU manqués.

Recommandation

Comme mis en valeur dans la section Cat Control de ce document, VLAN 1 est un VLAN spécial qui marque et gère la majeure partie du trafic du plan de contrôle. VLAN 1 est activé sur toutes les liaisons agrégées par défaut Avec de plus grands réseaux de campus, le soin doit être pris au sujet du diamètre du **domaine STP** du VLAN 1; l'instabilité dans une partie du réseau pourrait affecter VLAN 1, influençant de ce fait la stabilité du plan de contrôle et donc la stabilité STP pour tous les autres VLAN. Dans CatOS 5.4 et versions ultérieures, il est possible de limiter le transport par VLAN 1 de données utilisateur et l'exécution STP avec cette commande :

```
clear trunk mod/port vlan 1
```

Cela n'empêche pas les paquets de contrôle d'être envoyés de commutateur à commutateur dans le VLAN 1, comme vu 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: Il n'est pas actuellement possible de supprimer les liaisons agrégées VLAN 1 sur 3500s et 2900XLs.

Même si le soin a été pris avec le modèle campus pour contraindre les VLAN utilisateur à des domaines relativement petits et également à des petites limites de panne/L3, quelques clients sont encore tentés de traiter le VLAN de gestion différemment et d'essayer de couvrir tout le réseau avec un sous-réseau de gestion simple. Il n'y a aucune raison technique pour qu'une application NMS centrale soit adjacente L2 aux périphériques qu'elle contrôle, et il ne s'agit pas d'un argument de sécurité acceptable. Cisco recommande de limiter le diamètre des VLAN de gestion à la même structure de domaine routée que les VLAN utilisateur et de considérer l'administration hors bande et/ou la prise en charge de CatOS 6.x SSH comme une façon d'augmenter la sécurité du réseau.

Autres options

Cependant, 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. Ceci exige que vous contraigniez chaque sous-réseau IP/VLAN à un commutateur de couche d'accès simple, ou une grappe de commutateurs. Dans ces conceptions, il ne peut y avoir aucune agrégation de lien configurée au niveau de la couche d'accès.

Il n'est pas facile de savoir si un VLAN de gestion séparé doit être créé et l'agrégation de lien activée afin de la porter entre la couche d'accès L2 et les couches de distribution L3. 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. Cela 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. (Notez que si VLAN 1 est effacé des liaisons agrégées il y a une étape de configuration supplémentaire.) 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 : STP PortFast pour les liaisons agrégées (CatOS 7.x et versions ultérieures) ou synchronisation VLAN Autostate avec transmission STP (versions ultérieures à CatOS 5.5[9]).
- **Option 2 :** un VLAN unique pour les données et la gestion peut être acceptable. Avec un matériel de commutation plus récent, tel que des CPU plus puissants et des limitations de débit du plan de contrôle, plus une conception avec des domaines de diffusion relativement petits comme préconisé par la conception multicouche, la réalité pour beaucoup de clients est que garder l'interface sc0 séparée des données utilisateur est un problème moindre que par le passé. La décision finale est idéalement prise après examen du profil de trafic de diffusion pour ce VLAN et une discussion sur les capacités du matériel de commutation avec votre ingénieur Cisco. Si le VLAN de gestion contient en effet tous les utilisateurs sur ce commutateur de la couche d'accès, l'utilisation de filtres d'entrée d'IP est fortement recommandée pour protéger le commutateur des utilisateurs, comme évoqué dans la section Configuration de la sécurité de ce document.

Gestion extrabande

En poussant les arguments de la section précédente encore plus loin, l'administration de réseau peut être rendue plus fortement disponible avec la construction d'une infrastructure de gestion

distincte autour du réseau de production, de sorte que les périphériques soient toujours accessibles à distance, qu'importent les événements dus au trafic ou au plan de contrôle qui se produisent. Ces deux approches sont typiques :

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

Aperçu opérationnel

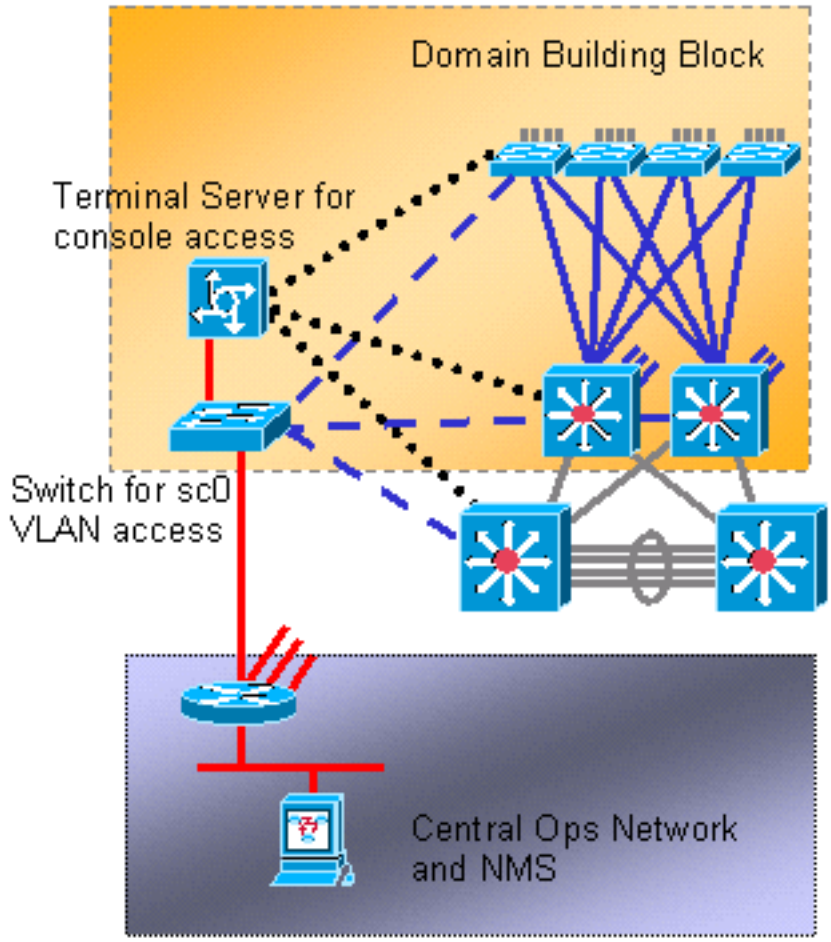
Chaque routeur et commutateur du réseau peut être équipé d'une interface de gestion Ethernet hors bande sur un VLAN de gestion. Un port Ethernet sur chaque périphérique est configuré dans le VLAN de gestion et câblé en dehors du réseau de production à un réseau de gestion commuté séparé via l'interface sc0. Notez que les commutateurs Catalyst 4500/4000 ont une interface me1 spéciale sur Supervisor Engine qui doit être utilisée pour la gestion hors bande seulement, pas comme port de commutation.

En outre, la connectivité du serveur de terminal peut être réalisée par configuration d'un 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. 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 également configurer un modem simple sur le port auxiliaire du serveur de terminaux afin de fournir un service à accès commuté aux autres périphériques quand la connectivité réseau échoue.

Recommandation

Avec cet agencement, deux chemins hors bande au chaque vers chaque commutateur et routeur sont possibles en plus de nombreux chemins de intrabande, de ce fait activant la gestion de réseau à haute disponibilité. Le hors bande est responsable de :

- Le hors bande sépare le trafic d'administration des données utilisateur.
- Le hors bande a l'adresse IP de gestion dans un sous-réseau, VLAN, et commutateur distincts pour une sécurité plus élevée.
- Le hors bande fournit une assurance plus élevée pour la remise des données de gestion pendant les pannes de réseau.
- Le hors bande n'a aucun spanning tree actif dans le VLAN de gestion. La redondance n'est pas critique.



Tests système

Diagnostics au démarrage

Pendant le démarrage système, un certain nombre de processus sont exécutés afin de s'assurer qu'une plate-forme fiable et opérationnelle est disponible de sorte que le matériel défectueux ne perturbe pas le réseau. Les diagnostics de démarrage Catalyst sont répartis entre des diagnostics d'autotest de mise sous tension (POST) et des diagnostics en ligne.

Aperçu opérationnel

Selon la plate-forme et la configuration matérielle, différents diagnostics sont effectués au démarrage et quand une carte est remplacée à chaud dans le châssis. Un plus haut niveau de diagnostic a pour conséquence un plus grand nombre de problèmes détectés mais un plus long cycle de démarrage. Ces trois niveaux de diagnostic POST peuvent être sélectionnés (tous les essais contrôlent la DRAM, la RAM, et la présence et la taille du cache et les initialisent) :

Aperçu opérationnel			
Contournement	S/O	3	Non disponible sur la gamme 4500/4000 utilisant CatOS 5.5 ou versions antérieures.
Minimal	Tests d'écriture de séquence sur le premier Mo de	30	Par défaut sur la gamme 5500/5000 et 6500/6000 ; non

	DRAM seulement.		disponible sur la gamme 4500/4000.
Complet	Tests d'écriture de séquence pour toute la mémoire.	60	Par défaut sur la gamme 4500/4000.

Diagnostics en ligne

Ces tests vérifient l'itinéraire du paquet à l'intérieur du commutateur. Il est important de noter que les diagnostics en ligne s'appliquent à tout le système, pas seulement aux ports. Sur les commutateurs Catalyst 5500/5000 et 6500/6000, des essais sont réalisés d'abord à partir du Supervisor Engine de veille, puis de nouveau à partir du Supervisor Engine principal. La durée des diagnostics dépend de la configuration système (nombre de logements, de modules, de ports). Il y a trois catégories de tests :

- Test de boucle locale - les paquets du NMP de Supervisor Engine sont envoyés à chaque port, puis retournés au NMP et examinés pour y trouver des erreurs.
- Test de groupage - des canaux de jusqu'à huit ports sont créés et des tests de boucle locale sont réalisés à l'agport pour vérifier le hachage vers des liaisons spécifiques (référez-vous à la section EtherChannel de ce document pour de plus amples informations).
- Test de logique de reconnaissance des adresses encodées (EARL) - le Supervisor Engine central et les moteurs de réécriture L3 du module Ethernet en ligne sont testés. Des entrées de transmission de matériel et des ports routés sont créés avant que l'échantillon de paquets soit envoyé (pour chaque type d'encapsulation de protocole) du NMP via le matériel de commutation sur chaque module et de nouveau au NMP. Cela s'applique aux modules Catalyst 6500/6000 PFC et plus récents.

Les diagnostics en ligne complets peuvent prendre approximativement deux minutes. Les diagnostics minimaux n'exécutent pas de tests de groupage ou de réécriture sur les modules autre que Supervisor Engine, et peuvent prendre approximativement 90 secondes.

Pendant un test mémoire, quand une différence est découverte entre le schéma et le schéma écrit, l'état du port est changé en faulty. Les résultats de ces tests peuvent être vus si la commande **show test** est émise, suivie du numéro de module à examiner :

```
>show test 9

Diagnostic mode: complete (mode at next reset: complete)
!--- Configuration setting. Module 9 : 4-port Multilayer Switch Line Card Status for Module 9 :
PASS Port Status : Ports 1 2 3 4 ---------------- . . . . Line Card Diag Status for Module 9 (.
= Pass, F = Fail, N = N/A) Loopback Status [Reported by Module 1] : Ports 1 2 3 4 -------------
--- . . F . !--- Faulty. Channel Status : Ports 1 2 3 4 ---------------- . . . .
```

Recommandation

Cisco recommande de paramétrer tous les commutateurs de façon à ce qu'ils utilisent des diagnostics complets pour fournir une détection de panne maximale et pour empêcher des pannes pendant le fonctionnement normal.

Remarque: Cette modification n'entre pas en vigueur jusqu'à ce que la prochaine fois que le périphérique est démarré. Émettez cette commande pour sélectionner le diagnostic complet :

```
set test diaglevel complete
```

Autres options

Dans quelques situations, un temps de démarrage peut être préférable au fait d'attendre que le diagnostic complet soit exécuté. Il y a d'autres facteurs et temporisations impliqués dans la création d'un système, mais dans l'ensemble, les diagnostics POST et en ligne rallongent cette durée d'environ un tiers. Lors d'un test avec un châssis à neuf logements d'un Supervisor Engine entièrement rempli et un Catalyst 6509, la durée de démarrage totale était d'environ 380 secondes avec des diagnostics complets, d'environ 300 secondes avec des diagnostics minimaux, et de seulement 250 secondes avec aucun diagnostic. Émettez cette commande pour configurer l'évitement du diagnostic :

```
set test diaglevel bypass
```

Remarque: Catalyst 4500/4000 accepte d'être configuré pour des diagnostics minimaux, cependant cela a toujours comme conséquence la réalisation d'un test complet. Le mode minimal pourrait être supporté à l'avenir sur cette plate-forme.

Diagnostics d'exécution

Une fois est le système opérationnel, le commutateur Supervisor Engine exécute diverses opérations de surveillance des autres modules. Si un module n'est pas accessible par les messages de gestion (Serial control protocol [SCP] fonctionnant sur le bus de gestion hors bande), Supervisor Engine tente de redémarrer la carte ou de prendre d'autres mesures appropriées.

Aperçu opérationnel

Le Supervisor Engine effectue diverses opérations de surveillance automatiquement ; ceci n'exige pas de configuration. Pour Catalyst 5500/5000 et 6500/6000, ces composants de commutateur sont surveillés :

- NMP par une horloge de surveillance
- Erreurs de puce EARL avancé
- Canal intrabande du Supervisor Engine au fond de panier
- Modules par des keepalives sur le canal hors bande (Catalyst 6500/6000)
- L'état du Supervisor Engine actif est surveillé par le Supervisor Engine de veille (Catalyst 6500/6000)

Détection d'erreurs système et matérielles

Aperçu opérationnel

Dans CatOS 6.2 et versions ultérieures, d'autres fonctionnalités ont été ajoutées pour surveiller les composants essentiels du système et du matériel. Ces trois composants matériels sont supportés :

- Intrabande
- Compteur de ports
- Mémoire

Quand la fonctionnalité est activée et une condition d'erreur est détectée, le commutateur génère un message syslog. Le message informe l'administrateur qu'un problème existe avant qu'une dégradation des performances apparente se produise. Dans CatOS versions 6.4(16), 7.6(12), 8.4(2) et ultérieures, le mode par défaut pour chacun des trois composants est passé de désactivé à activé.

Intrabande

Si une erreur intrabande est détectée, un message syslog vous informe qu'un problème existe avant que la dégradation des performances apparente ne se produise. L'erreur affiche le type de panne intrabande. Exemples :

- Intrabande coincée
- Erreurs de ressource
- Échec de l'intrabande au démarrage

Lors de la détection d'une panne de ping intrabande, la fonctionnalité enregistre également un message syslog supplémentaire avec un instantané du débit Tx et Rx actuels sur la connexion intrabande, ainsi que la charge de fond de panier du commutateur. Ce message vous permet de déterminer correctement si l'intrabande est coincée (aucun Tx/Rx) ou surchargée (Tx/Rx excessif). Ces informations supplémentaires peuvent vous aider à déterminer la cause des pannes de ping intrabande.

Compteur de ports

Quand vous activez cette fonctionnalité, elle crée et commence un processus pour déboguer les compteurs de port. Le compteur de ports surveille périodiquement certains compteurs d'erreurs de port internes. L'architecture de la carte de ligne, et plus spécifiquement les ASIC sur le module, détermine quels compteurs la fonctionnalité questionne. L'assistance technique Cisco ou l'ingénierie de développement peuvent alors employer cette information afin de dépanner des problèmes. Cette fonctionnalité n'interroge pas les compteurs d'erreur tels que FCS, CRC, le cadrage et les trames incomplètes directement associées avec la connectivité de partenaire de liaison. Voyez la section Gestion des erreurs EtherChannel/liaison de ce document afin d'incorporer cette capacité.

L'interrogation est exécutée toutes les 30 minutes et s'exécute à l'arrière-plan des compteurs d'erreur sélectionnés. Si le nombre augmente entre deux interrogations successives sur le même port, un message syslog rapporte l'incident et donne les détails du module/port et du compteur d'erreurs.

L'option de compteur de ports n'est pas supportée sur la plate-forme Catalyst 4500/4000.

Mémoire

L'activation de cette fonctionnalité exécute la surveillance de fond et la détection des états de corruption de la DRAM. De tels états de corruption mémoire incluent :

- Allocation
- Libération
- Hors de portée
- le mauvais cadrage

Recommandation

Activez toutes les fonctionnalités de détection d'erreurs, ce qui inclut l'intrabande, les compteurs de port, et la mémoire, lorsqu'ils sont supportés. L'activation de ces fonctionnalités permet d'obtenir un système plus proactif et des diagnostics d'avertissement de matériel pour la plate-forme de commutation Catalyst. Émettez ces commandes afin d'activer chacune des trois fonctionnalités de détection d'erreurs :

```
set errordetection inband enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection
portcounters enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection memory
enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later.
```

Émettez cette commande afin de confirmer que la détection d'erreurs est activée :

```
>show errordetection

Inband error detection:                 enabled
Memory error detection:                 enabled
Packet buffer error detection:          errdisable
Port counter error detection:           enabled
Port link-errors detection:             disabled
Port link-errors action:                port-failover
Port link-errors interval:              30 seconds
```

Gestion d'erreurs EtherChannel/de liaisons

Aperçu opérationnel

Dans CatOS 8.4 et versions ultérieures, une nouvelle fonctionnalités a été introduite afin de fournir un basculement automatique du trafic d'un port dans un EtherChannel à un autre port dans le même EtherChannel. Le basculement de port se produit quand un des ports du canal dépasse un certain seuil d'erreurs configurables dans l'intervalle spécifique. Le basculement de port se produit seulement s'il reste un port opérationnel dans l'EtherChannel. Si le port en échec est le dernier port dans l'EtherChannel, le port n'entre pas dans l'état port-failover . Ce port continue à passer du trafic, indépendamment du type d'erreurs qui sont reçues. Les ports simples et non-canalisants n'entrent pas dans l'état port-failover . Ces ports entrent en état errdisable quand le seuil d'erreur est dépassé dans l'intervalle spécifique.

Cette fonctionnalité est seulement pertinente quand vous activez **set errordetection portcounters**. Les erreurs de liaison à surveiller sont basées sur trois compteurs :

- InErrors
- RxCRCs (CRCAlignErrors)
- TxCRCs

Émettez la commande show counters sur un commutateur afin d'afficher le nombre de compteurs d'erreur. Voici un exemple :

```
>show counters 4/48

.......

32 bit counters
```

```
0  rxCRCAlignErrors           =          0
.......

6  ifInErrors                 =          0
.......

12 txCRC                      =          0
```

Cette table répertorie les paramètres de configuration possibles et la configuration respective par défaut :

Paramètres	Par défaut
Global	Handicapé
Surveillance du port pour RxCRC	Handicapé
Surveillance du port pour InErrors	Handicapé
Surveillance du port pour TxCRC	Handicapé
Action	Basculement du port
Intervalle	30 secondes
Nombre d'échantillonnage	3 consécutifs
Seuil bas	1000
Seuil élevé	1001

Si la fonction est activée et que le nombre d'erreurs d'un port atteint la valeur élevée du seuil configurable au cours de la période spécifique de nombre d'échantillonnage, l'action configurable est soit la désactivation des erreurs soit le basculement de port. L'action de désactivation des erreurs place le port en état errdisable. Si vous configurez l'action de basculement de port, l'état de canal de port est considéré. Le port est en désactivation d'erreurs seulement s'il se trouve dans un canal mais qu'il n'est pas le dernier port opérationnel dans ce canal. En outre, si l'action configurée est le basculement de port et le port est un port unique ou non-canalisé, le port est placé en état errdisable quand le nombre d'erreurs de port atteint la valeur élevée du seuil.

L'intervalle est un timer constant pour lire les compteurs d'erreurs de ports. La valeur par défaut de l'intervalle d'erreurs de liaison est de 30 secondes. La plage autorisée est entre 30 et 1800 secondes.

Il y a un risque de désactivation d'erreur accidentelle d'un port en raison d'un événement occasionnel inattendu. Afin de réduire au minimum ce risque, des mesures sont prises sur un port seulement quand le problème persiste dans tous les échantillons consécutifs. La valeur d'échantillonnage par défaut est de 3 et la plage autorisée est de 1 à 255.

Le seuil est un nombre absolu à vérifier selon l'intervalle liaison-erreurs. Le seuil inférieur de liaison-erreurs par défaut est de 1000 et la plage autorisée est de 1 à 65 535. Le seuil supérieur de liaison-erreurs par défaut est de 1001. Quand le nombre consécutif d'opérations d'échantillonnage atteint le seuil inférieur, un syslog est envoyé. Si le nombre consécutif d'opérations d'échantillonnage atteint le seuil supérieur, un syslog est envoyé et une action de désactivation des erreurs ou de basculement de port est déclenchée.

Remarque: Utilisez la même configuration détection d'erreurs pour tous les ports dans un canal. Référez-vous à ces sections du guide de configuration logicielle de la gamme Catalyst 6500 pour

plus d'informations :

- La section Configuration de la gestion d'erreurs EtherChannel/Liaisons de Contrôle de l'état et de la connectivité
- La section *Configuration de la détection d'erreurs de port* de Configuration de la commutation Ethernet, Fast Ethernet, Gigabit Ethernet et 10-Gigabit Ethernet

Recommandations

Puisque la fonctionnalité emploie des messages SCP afin d'enregistrer et comparer les données, le nombre élevé de ports actifs peut fortement solliciter le CPU. Cette sollicitation devient encore plus forte quand l'intervalle de seuil est défini sur une valeur très petite. Activez cette fonctionnalité avec précaution sur les ports qui sont indiqués en tant que liaisons critiques et transportent du trafic pour des applications sensibles. Émettez cette commande afin d'activer la détection d'erreurs de liaison globalement :

```
set errordetection link-errors enable
```

En outre, commencez par le seuil par défaut, l'intervalle, et les paramètres d'échantillonnage. Utilisez l'action par défaut, le basculement de port.

Émettez ces commandes afin d'appliquer les paramètres globaux de liaison-erreurs aux ports individuels :

```
set port errordetection mod/port inerrors enable

set port errordetection mod/port rxcrc enable

set port errordetection mod/port txcrc enable
```

Vous pouvez émettre ces commandes afin de vérifier la configuration liaison-erreurs :

```
show errordetection

show port errordetection {mod | mod/port}
```

Diagnostics de temporisation des paquets Catalyst 6500/6000

Dans CatOS versions 6.4(7), 7.6(5), et 8.2(1), les diagnostics de mise en tampon des paquets Catalyst 6500/6000 ont été introduits. Les diagnostics de mise en tampon des paquets, qui sont activés par défaut, détectent les pannes de mise en tampon de paquets qui sont provoquées par des pannes temporaires de la RAM statique (SRAM). La détection se fait sur ces modules 48 ports à ligne 10/100-Mbps :

- WS-X6248-RJ45
- WS-X6248-RJ21
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45
- WS-X6148-RJ21

Quand la condition de panne se produit, 12 ports sur les 48 ports 10/100-Mbps continuent à rester connectés et peuvent rencontrer des problèmes aléatoires de connectivité. La seule manière de

se remettre de ce problème est d'éteindre et de rallumer le module de ligne.

Aperçu opérationnel

Les diagnostics de mise en tampon des paquets contrôlent les données qui sont enregistrées dans une section spécifique de la mémoire tampon afin de déterminer si elle est altérée par des pannes passagères SRAM. Si le processus lit quelque chose de différent de ce qu'il a écrit, il a le choix entre deux options de récupération :

1. L'action par défaut consiste à désactiver les erreurs des ports de carte de ligne qui sont affectés par la défaillance du tampon.
2. La seconde option consiste à éteindre et rallumer la carte de ligne.

Deux messages syslog ont été ajoutés. Les messages avertissent que les erreurs ont été désactivés ou le module éteint et rallumé en raison des erreurs de la mémoire tampon :

```
show errordetection

show port errordetection {mod | mod/port}
```

Dans les versions de CatOS antérieures à 8.3 et 8.4, le temps nécessaire pour éteindre et rallumer la carte de ligne est entre 30 et 40 secondes. Une fonctionnalité de démarrage rapide a été introduite dans CatOS versions 8.3 et 8.4. La fonctionnalité télécharge automatiquement le microprogramme sur les cartes de ligne installées pendant le processus de démarrage initial afin de réduire au minimum le temps de démarrage. La fonctionnalité de démarrage rapide ramène le temps de mise hors tension et redémarrage à approximativement 10 secondes.

Recommandation

Cisco recommande l'option errdisable par défaut. Cette action a moins d'incidence sur le service réseau pendant les heures de production. Si possible, déplacez la connexion qui est affectée par les ports en désactivation des erreurs vers d'autres ports de commutation disponibles afin de restaurer le service. Programmez une mise hors tension et un redémarrage manuel de la carte de ligne pendant la fenêtre de maintenance. Emettez la commande reset module mod afin de récupérer entièrement de l'état corrompu du tampon de paquets.

Remarque: Si les erreurs continuent après que le module soit remis à l'état initial, essayez de réinsérer le module.

Émettez cette commande afin d'activer l'option errdisable :

```
set errordetection packet-buffer errdisable
!--- This is the default.
```

Autre option

Puisqu'il est nécessaire d'éteindre et de rallumer la carte de ligne afin de récupérer entièrement tous les ports qui ont rencontré une panne SRAM, une action alternative de reprise est de configurer l'option de mise hors tension et de redémarrage. Cette option est utile dans les circonstances dans lesquelles une panne des services réseau qui peuvent durer entre 30 et 40 secondes est acceptable. Cette durée est le temps nécessaire pour qu'un module de ligne s'éteigne, se rallume et soit à nouveau en service sans la fonctionnalité de démarrage rapide. La fonctionnalité de démarrage rapide peut ramener la durée de la panne dans les services réseau à

10 secondes avec l'option de mise hors tension et de redémarrage. Émettez cette commande afin d'activer l'option de mise hors tension et redémarrage :

```
set errordetection packet-buffer power-cycle
```

Diagnostics du tampon des paquets

Ce test s'applique uniquement aux commutateurs Catalyst 5500/5000. Ce test est conçu pour rechercher le matériel défaillant sur les commutateurs Catalyst 5500/5000 qui utilisent des modules Ethernet avec un matériel spécifique qui fournit une connectivité 10/100-Mbps entre les ports utilisateurs et le fond de panier du commutateur. Puisqu'ils ne peuvent pas exécuter de vérification CRC pour les trames agrégées, si un tampon mémoire de port devient défectueux pendant le délai d'exécution, des paquets peuvent se retrouver corrompus et entraîner des erreurs CRC. Malheureusement, ceci pourrait mener à la propagation de mauvaises trames plus loin dans le réseau ISL Catalyst 5500/5000, ce qui entraînerait potentiellement une perturbation du plan de contrôle et des tempêtes de diffusion dans les pires scénarios.

Les modules Catalyst 5500/5000 autres plates-formes plus récentes ont mis à jour le contrôle d'erreurs de matériel incorporées et n'ont pas besoin de tests de tampon mémoire ; il n'existe donc aucune option pour les configurer.

Les modules de ligne qui ont besoin de diagnostics de mise en tampon des paquets sont WS-X5010, WS-X5011, WS-X5013, WS-X5020, WS-X5111, WS-X5113, WS-X5114, WS-X5201, WS-X5203, WS-X5213/a, WS-X5223, WS-X5224, WS-X5506, WS-X5509, WS-U5531, WS-U5533, and WS-U5535.

Aperçu opérationnel

Ce diagnostic vérifie que les données enregistrées dans une section spécifique de la mémoire tampon ne sont pas accidentellement corrompues par le matériel défectueux. Si le processus lit quelque chose de différent de ce qu'il a écrit, il arrête le port en mode failed , puisque ce port pourrait altérer des données. Il n'y a aucun seuil d'erreurs requis. Des ports en échec ne peuvent pas être activés de nouveau jusqu'à ce que le module ait été réinitialisé (ou substitué).

Il y a deux modes pour des tests de tampon mémoire : programmé et à la demande. Quand un test débute, des messages syslog sont produits afin d'indiquer la durée prévue du test (arrondi jusqu'à la minute la plus proche) et le fait que le test a commencé. La longueur exacte du test varie selon le type de port, la taille de la mémoire tampon, et le type de test exécuté

Les tests à la demande sont agressifs afin de se finir en quelques minutes. Puisque ces tests gênent activement la mémoire de paquets, des ports doivent être administrativement arrêtés avant le test. Émettez cette commande afin d'arrêter les ports :

```
> (enable) test packetbuffer 4/1
Warning: only disabled ports may be tested on demand - 4/1 will be skipped.
> (enable) set port disable 4/1
> (enable) test packetbuffer 4/1
Packet buffer test started. Estimated test time: 1 minute.
%SYS-5-PKTTESTSTART:Packet buffer test started
%SYS-5-PKTTESTDONE:Packet buffer test done. Use 'show test' to see test results
```

Les tests programmés sont beaucoup moins agressifs que les tests à la demande, et ils s'exécutent à l'arrière-plan. Les tests sont réalisés en parallèle à travers plusieurs modules mais sur un port par module à la fois. Le test préserve, écrit et lit de petites sections de mémoire

tampon de paquets avant de restaurer les données tampon des paquets utilisateur, et ne produit ainsi aucune erreur. Cependant, puisque le test écrit sur la mémoire tampon, il bloque des paquets entrants pendant quelques millisecondes et entraîne une certaine perte sur les liaisons occupées. Par défaut, il y a une pause de huit secondes entre chaque test d'écriture en tampon pour réduire au maximum n'importe quelle perte de paquets, mais ceci signifie que dans un système plein de modules ayant besoin d'un test de tampon mémoire, le test peut mettre plus de 24 heures pour se terminer. Ce test programmé est activé par défaut pour s'exécuter tous les dimanches à 03:30 pour CatOS version 5.4 et ultérieures, et l'état du test peut être confirmé avec cette commande :

```
>show test packetbuffer status

!--- When test is running, the command returns !--- this information: Current packet buffer test
details Test Type : scheduled Test Started : 03:30:08 Jul 20 2001 Test Status : 26% of ports
tested Ports under test : 10/5,11/2 Estimated time left : 11 minutes !--- When test is not
running, !--- the command returns this information: Last packet buffer test details Test Type :
scheduled Test Started : 03:30:08 Jul 20 2001 Test Finished : 06:48:57 Jul 21 2001
```

Recommandation

Cisco recommande d'utiliser la fonctionnalité de test de tampon mémoire programmé pour les systèmes Catalyst 5500/5000, car l'avantage de découvrir des problèmes sur des modules est supérieur au risque de faible perte de paquets.

Un horaire hebdomadaire normalisé doit alors être programmé sur tout le réseau, permettant au client de changer les liaisons sur ports défectueux ou des modules RMA selon les besoins. Comme ce test peut entraîner une certaine perte de paquets, selon la charge réseau, il doit être planifié pendant des périodes plus calmes, telles que le dimanche matin à 3:30 par défaut. Émettez cette commande pour définir la durée du test :

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

Une fois activé (comme quand CatOS passe en 5.4 et versions ultérieures pour la première fois), il y a un risque pour qu'un problème mémoire/matériel précédemment masqué soit exposé, et un port est arrêté automatiquement en conséquence. Vous pourriez voir ce message :

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

Autres options

S'il n'est pas acceptable de risquer un faible niveau de perte de paquets par port sur une base hebdomadaire, alors il est recommandé d'utiliser la fonctionnalité à la demande pendant les coupures programmées. Émettez cette commande pour lancer cette fonctionnalité manuellement sur une base par plage (bien que le port doive être administrativement désactivé d'abord) :

```
test packetbuffer port range
```

Journalisation système

Les messages Syslog sont spécifiques à Cisco et une partie principale de la gestion de pannes anticipées. Syslog permet de rapporter un plus large éventail de statuts réseau et protocole que le SNMP standardisé. Les plates-formes de gestion, telles que le Resource Manager Essentials de

Cisco (RMEs) et la boîte à outils d'analyse de réseau (NATkit) font l'utilisation puissante de l'information Syslog parce qu'elles effectuent ces tâches :

- Analyse actuelle par gravité, message, périphérique, etc
- Activez le filtrage des messages qui arrivent pour analyse
- Déclenchez les alertes, comme les pageurs, ou la collecte à la demande de l'inventaire et des modifications de la configuration

Recommandation

Un point important est le niveau d'informations enregistrées dans le journal à générer localement et à retenir dans le tampon de commutation qui est envoyé à un serveur Syslog (utilisant la commande set logging server severity value). Quelques organismes enregistrent un haut niveau d'informations centralement, tandis que d'autres vont vers le commutateur lui-même pour regarder les logs plus détaillés d'un événement ou activer un plus haut niveau de la saisie Syslog seulement pendant le dépannage.

Le débogage est différent sur les plates-formes CatOS par rapport au logiciel Cisco IOS, mais une journalisation système détaillée peut être activée sur une base par session avec set logging session enable sans changer ce qui est enregistré par défaut.

Cisco recommande généralement d'amener les installations spantree et système Syslog jusqu'au niveau 6, car ces derniers sont des fonctionnalités de stabilité principale à suivre. En outre, pour des environnements de multidiffusion, il est recommandé d'augmenter le niveau de journalisation de mcast jusqu'à 4, de sorte que des messages Syslog soient produits si des ports du routeur sont supprimés. Malheureusement, avant CatOS 5.5(5), ceci pourrait avoir comme conséquence l'enregistrement de messages syslog pour les entrées et sorties IGMP, ce qui est trop bruyant à surveiller. Enfin, si des listes de saisie IP sont utilisées, il est recommandé de définir le niveau minimal de journalisation sur 4 pour saisir les tentatives de connexion non autorisées. Émettez ces commandes pour définir ces options :

```
set logging buffer 500
!--- This is the default. set logging server syslog server IP address set logging server enable
!--- This is the default. set logging timestamp enable
set logging level spantree 6 default
!--- Increase default STP syslog level. set logging level sys 6 default
!--- Increase default system syslog level. set logging server severity 4
!--- This is the default; !--- it limits messages exported to syslog server. set logging console
disable
```

Arrêtez les messages de console afin de vous protéger contre le risque d'arrêt du commutateur lorsqu'il attend une réponse d'un terminal lent ou non-existant quand le volume de message est élevé. La journalisation sur console est une priorité élevée sous CatOS et est principalement utilisée pour saisir les messages finaux localement en dépannant ou dans un scénario de crash du commutateur.

Cette table fournit les services de journalisation individuelle, les niveaux par défaut, et les changements recommandés pour Catalyst 6500/6000. Chaque plate-forme a des équipements légèrement différents, selon les fonctionnalités supportées.

Installation	Niveau par défaut	Action recommandée

acl	5	Mettre de côté.
cdp	4	Mettre de côté.
cops	3	Mettre de côté.
DTP	8	Mettre de côté.
comte	2	Mettre de côté.
ethc[1]	5	Mettre de côté.
filesys	2	Mettre de côté.
gvrp	2	Mettre de côté.
IP	2	**Passez à 4 si vous utilisez des listes de saisie d'IP**.
noyau	2	Mettre de côté.
1d	3	Mettre de côté.
mcast	2	Passez à 4 si multicast est utilisé (CatOS 5.5[5] et versions ultérieures) .
mgmt	5	Mettre de côté.
mls	5	Mettre de côté.
pagp	5	Mettre de côté.
protfilt	2	Mettre de côté.
élagage	2	Mettre de côté.
Privatevlan	3	Mettre de côté.
qos	3	Mettre de côté.
rayon	2	Mettre de côté.
RSVP	3	Mettre de côté.
Sécurité	2	Mettre de côté.
SNMP	2	Mettre de côté.
spantree	2	**Passez à 6.**
système	5	**Passez à 6.**
tac	2	Mettre de côté.
TCP	2	Mettre de côté.
telnet	2	Mettre de côté.
Tftp	2	Mettre de côté.
UDLD	4	Mettre de côté.
VMPS	2	Mettre de côté.
VTP	2	Mettre de côté.

[1] dans CatOS 7.x et plus tard, le code d'installation d'ethc remplace le code d'installation de pagp afin de refléter le support LACP.

Remarque: Actuellement, les commutateurs Catalyst enregistrent un message syslog de niveau 6 de changement de configuration pour chaque commande **set** ou **clear** exécutée, à la différence du logiciel Cisco IOS, qui déclenche le message seulement après avoir quitté le mode configuration. Si vous avez besoin de RMEs pour sauvegarder des configurations en temps réel lors de ce déclencheur, alors ces messages doivent également être envoyés au serveur syslog de RMEs.

Pour la plupart des clients, des sauvegardes régulières de la configuration pour des commutateurs Catalyst suffisent, et aucune modification de la gravité de journalisation serveur par défaut n'est nécessaire.

Si vous accordez vos alertes NMS, consultez le Guide des messages système.

Protocole SNMP

SNMP est utilisé pour récupérer des statistiques, des compteurs et des tables enregistrées dans les bases d'informations de gestion des périphériques réseau (MIBs). Les informations collectées peuvent être utilisées par les NMS (tel que HP Openview) afin de produire des alertes en temps réel, mesurer la disponibilité, et produire des informations de planification de la capacité, aussi bien qu'exécuter des contrôles de la configuration et de dépannage.

Aperçu opérationnel

Avec quelques mécanismes de sécurité, une station de gestion de réseau est capable de rechercher des informations dans les MIB avec le protocole SNMP, d'obtenir les requêtes suivantes et de changer des paramètres avec la commande **set**. De plus, un périphérique réseau peut être configuré pour produire un message dérouté pour NMS pour l'alerte en temps réel. L'interrogation SNMP utilise IP UDP port 161 et les messages déroutés SNMP utilisent le port 162.

Cisco supporte ces versions de SNMP :

- SNMPv1 : Norme Internet RFC 1157, utilisant une sécurité de chaîne communautaire en texte clair. Une liste de contrôle d'accès d'adresse IP et un mot de passe définissent la communauté de responsables capables d'accéder au MIB de l'agent.
- SNMPv2C : une combinaison de snmpv2, une norme Internet d'ébauche définie dans RFCs 1902 à 1907, et SNMPv2C, une infrastructure administrative basée sur la communauté pour snmpv2 qui est un projet expérimental défini dans RFC 1901. Les avantages incluent un mécanisme de récupération en bloc qui supporte la recherche de tables et de grandes quantités d'information, réduit au minimum le nombre d'allers-retours, et améliore la gestion d'erreurs.
- SNMPv3 : RFC 2570 a proposé que l'ébauche fournisse l'accès sécurisé aux périphériques par la combinaison de l'authentification et du chiffrement de paquets sur le réseau Les fonctionnalités de sécurité fournies dans SNMPv3 sont :Intégrité du message : s'assure qu'un paquet n'a pas été altéré pendant le transitAuthentification : détermine si le message provient d'une source valideCryptage : brouille le contenu d'un paquet pour l'empêcher d'être affiché facilement par une source non autorisée

Cette table identifie les combinaisons de modèles de sécurité :

Niveau modèle	Authentification	Cryptage	Résultat
v1	noAuthNoPriv, Chaîne	Non	Utilise une chaîne de caractères de la communauté

	de caractères de la communauté		correspondante pour l'authentification.
v2c	noAuthNoPriv, Chaîne de caractères de la communauté	Non	Utilise une chaîne de caractères de la communauté correspondante pour l'authentification.
v3	noAuthNoPriv, Nom d'utilisateur	Non	Utilise un nom d'utilisateur correspondant pour l'authentification.
v3	authNoPriv, MD5 ou SHA	Le NP	Fournit une authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA.
v3	authPriv, MD5 ou SHA	DES	Fournit une authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA. Fournit un cryptage DES 56 bits en plus de l'authentification basée sur la norme CBC-DES (DES-56).

Remarque: Maintenez cette information à l'esprit au sujet des objets SNMPv3 :

- Chaque utilisateur appartient à un groupe.
- Un groupe définit la stratégie d'accès pour un ensemble d'utilisateurs.
- Une stratégie d'accès définit quels objets SNMP peuvent être consultés pour lire, écrire, et créer.
- Un groupe détermine la liste des notifications que ses utilisateurs peuvent recevoir.
- Un groupe définit également le modèle de sécurité et le niveau de sécurité pour ses utilisateurs.

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 sur le commutateur doit être paramétré pour utiliser la version SNMP supportée par la station de gestion. Puisqu'un agent peut communiquer avec plusieurs responsables, il est possible de configurer le logiciel pour supporter la transmission avec une station de gestion utilisant le protocole SNMPv1 et une autre utilisant le protocole snmpv2, par exemple.

La plupart des stations NMS utilisent SNMPv2C aujourd'hui sous cette configuration :

```
set snmp community read-only string
!--- Allow viewing of variables only. set snmp community read-write string
!--- Allow setting of variables. set snmp community read-write-all string<string>
!--- Include setting of SNMP strings.
```

Cisco recommande d'activer les messages déroutés SNMP pour toutes les fonctionnalités en service (les fonctionnalités non utilisées peuvent être désactivées si désiré). Une fois un message dérouté activé, il peut être testé avec la commande test snmp et une gestion appropriée définie sur le NMS pour l'erreur (telle qu'une alerte par radiomessagerie ou instantané).

Tous les messages déroutés sont désactivés par défaut et doivent être ajoutés à la configuration, individuellement ou via le paramètre **all** , comme montré :

```
set snmp trap enable all
set snmp trap server address read-only community string
```

Les messages déroutés disponibles dans CatOS 5.5 incluent :

Déroutement	Description
authentique	Authentification
passerelle	Passerelle
châssis	Châssis
config	Configuration
entité	Entité
ippermit	Autorisation IP
module	Module
répéteur	Répéteur
stpx	Extension de Spanning-tree
Syslog	Notification Syslog
vmps	Serveur de stratégie d'appartenance au VLAN
VTP	Protocole VTP

Remarque: Le message dérouté syslog envoie tous les messages syslog générés par le commutateur au NMS comme message dérouté SNMP aussi. Si l'alerte Syslog déjà est exécutée par un analyseur tel que Cisco Works 2000 RMEs, alors il n'est pas nécessairement utile de recevoir cette information deux fois.

Àla différence du logiciel Cisco IOS, les messages déroutés SNMP au niveau des ports sont désactivés par défaut parce que les commutateurs peuvent avoir des centaines d'interfaces actives. Cisco recommande donc que les ports principaux, tels que les liaisons de l'infrastructure aux routeurs, aux commutateurs et aux serveurs principaux, aient les messages déroutés SNMP activés au niveau des ports. D'autres ports, comme des ports hôte d'utilisateur, ne sont pas requis, ce qui aide à simplifier l'administration de réseau.

```
set port trap port range enable
!--- Enable on key ports only.
```

Recommandation concernant l'interrogation SNMP

Un examen d'administration de réseau est recommandé afin de discuter les besoins spécifiques en détail. Cependant, quelques philosophies de base de Cisco pour la gestion de grands réseaux sont énumérées :

- Faites quelque chose de simple, et faites-le bien.
- Réduisez la surcharge de personnel due à l'interrogation de données excessives, à la collecte, aux outils, et à l'analyse manuelle.
- L'administration de réseau est possible avec juste quelques outils, tels que HP Openview en tant que NMS, Cisco RMEs en tant que configuration, Syslog, inventaire et responsable de logiciel, Microsoft Excel comme analyseur de données NMS, et CGI comme méthode de publication sur le Web.
- La publication de rapports sur le Web permet aux utilisateurs, tels que la haute direction et les analystes, de trouver les informations eux-mêmes sans charger le personnel d'opérations avec beaucoup de demandes spéciales.
- Découvrez ce qui fonctionne bien sur le réseau et laissez-le tel quel. Concentrez-vous sur ce qui ne fonctionne pas.

La première phase de la mise en oeuvre NMS doit être la spécification de base du matériel réseau. Beaucoup d'informations peuvent être déduites au sujet de la santé du périphérique et du protocole grâce à l'utilisation du CPU, de la mémoire, du tampon sur les routeurs, et de l'utilisation du CPU NMP, de la mémoire et du fond de panier sur les commutateurs. C'est seulement une fois le matériel spécifié que la charge de trafic L2 et L3, la crête, et les spécifications de base moyennes deviennent entièrement significatives. Les spécifications de base sont habituellement établies sur plusieurs mois pour obtenir une visibilité sur les tendances quotidiennes, hebdomadaires, et trimestrielles - selon le cycle économique de la société.

Beaucoup de réseaux souffrent de problèmes de performance NMS et de capacité provoqués par une sur-interrogation. Il est donc recommandé, une fois que la spécification de base est établie, de définir des seuils RMON d'alarme et d'événement sur les périphériques eux-mêmes afin d'alerter NMS à propos des modifications anormales, et ainsi supprimer le besoin d'interrogation. Ceci permet au réseau d'indiquer aux opérateurs quand quelque chose n'est pas normal plutôt que de continuellement effectuer des interrogations pour voir si tout est normal. Des seuils peuvent être définis basés sur diverses règles, telles que la valeur maximale plus un pourcentage ou l'écart type d'une moyenne, et sont hors de portée de ce document.

La seconde phase de la mise en oeuvre NMS est d'interroger des zones particulières du réseau plus en détail avec SNMP. Ceci inclut des zones incertaines, des zones avant une modification, ou des zones qui sont caractérisées comme fonctionnant bien. Employez les systèmes NMS comme projecteur pour balayer le réseau en détail et pour illuminer les points chauds (n'essayez pas d'allumer tout le réseau).

Le groupe de conseil sur la gestion de réseau Cisco propose ces MIB défectueux principaux à analyser ou à surveiller dans les réseaux de campus. Référez-vous à Surveillance de réseau Cisco et conseils de corrélation d'événement pour plus d'informations (sur les MIB de performance à interroger, par exemple).

Nom d'objet	Description d'objet	OID	Intervalle d'interrogation	Seuil
MIB-II				
sysUpTime	disponibilité système dans 1/100èmes secondes	1.3.6.1.2.1.1.3	5 mn	< 30000

Nom d'objet	Description d'objet	OID	Intervalle d'interrogation	Seuil
CISCO-PROCESS-MIB				
cpmCPUTotal5min	Le pourcentage général de CPU occupé pendant les 5 dernières minutes	1.3.6.1.4.1.9.9.109.1.1.1.1.5	10 mn	Spécification de base

Nom d'objet	Description d'objet	OID	Intervalle d'interrogation	Seuil
CISCO-STACK-MIB				
sysEnableChassisTraps	Indique si des messages déroutés chassisAlarmOn et chassisAlarmOff dans ce MIB doivent être produits.	1.3.6.1.4.1.9.5.1.1.24	24 heures	1
sysEnableModuleTraps	Indique si des messages déroutés moduleUp et moduleDown dans ce MIB doivent être produits.	1.3.6.1.4.1.9.5.1.1.25	24 heures	1
sysEnableBridgeTraps	Indique si des messages déroutés newRoot et topologyChange dans le BRIDGE-MIB (RFC 1493) doivent être produits.	1.3.6.1.4.1.9.5.1.1.26	24 heures	1

sysEnableRepeaterTraps	Indique si des messages déroutés dans le REPEATER-MIB (RFC1516) doivent être produits.	1.3.6.1.4.1.9.5.1.1.29	24 heures	1
sysEnableIpPermitTraps	Indique si des messages déroutés d'autorisation IP dans ce MIB doivent être produits.	1.3.6.1.4.1.9.5.1.1.31	24 heures	1
sysEnableVmpsTraps	Indique si le message dérouté vmVmpsChange défini dans CISCO VLAN-MEMBERSHIP-MIB doit être produit.	1.3.6.1.4.1.9.5.1.1.33	24 heures	1
sysEnableConfigTraps	Indique si un message dérouté sysConfigChange dans ce MIB doit être produit.	1.3.6.1.4.1.9.5.1.1.35	24 heures	1
sysEnableStpxTrap	Indique si un message dérouté stpxInconsistencyUpdate dans le CISCO-STP-EXTENSIONS-MIB doit être produit.	1.3.6.1.4.1.9.5.1.1.40	24 heures	1
chassisPs1status	État de l'alimentation électrique 1.	1.3.6.1.4.1.9.5.1.2.4	10 mn	2
chassisPs1TestResult	Les informations détaillées sur l'état de l'alimentation électrique 1.	1.3.6.1.4.1.9.5.1.2.5	Comme nécessaire.	
chassisPs2Status	État de l'alimentation électrique 2.	1.3.6.1.4.1.9.5.1.2.7	10 mn	2
chassisPs2TestResult	Les informations détaillées sur	1.3.6.1.4.1.9.5.1.2.8	Comme	

	l'état de l'alimentation électrique 2.		nécessaire.	
chassisFanStatus	État du ventilateur du châssis.	1.3.6.1.4.1.9.5.1.2.9	10 mn	2
chassisFanTestResult	Les informations détaillées sur l'état du ventilateur du châssis.	1.3.6.1.4.1.9.5.1.2.10	Comme nécessaire.	
chassisMinorAlarm	État de l'alarme secondaire du châssis.	1.3.6.1.4.1.9.5.1.2.11	10 mn	1
châssis MajorAlarm	État de l'alarme principale du châssis.	1.3.6.1.4.1.9.5.1.2.12	10 mn	1
chassisTempAlarm	État d'alarme de température du châssis.	1.3.6.1.4.1.9.5.1.2.13	10 mn	1
moduleStatus	État opérationnel du module.	1.3.6.1.4.1.9.5.1.3.1.1.10	30 mn	2
moduleTestResult	Les informations détaillées sur l'état des modules.	1.3.6.1.4.1.9.5.7.3.1.1.11	Comme nécessaire.	
moduleStandbyStatus	État d'un module redondant.	1.3.6.1.4.1.9.5.7.3.1.1.21	30 mn	= 1 or = 4

Nom d'objet	Description d'objet	OID	Intervalle d'interrogation	Seuil
CISCO-MEMORY-POOL-MIB				
dot1dStpTimeSinceTopologyChange	La durée écoulée (en 1/100èmes de sec) depuis la dernière fois qu'une modification de la topologie a été	1.3.6.1.2.1.17.2.3	5 mn	< 30000

	détectée par l'entité.			
dot1dStpTopChanges	Le nombre total de modifications de la topologie détectées par ce pont depuis que l'entité de gestion a été pour la dernière fois réinitialisée ou initialisée.	1.3.6.1.2.1.17.2.4	Comme nécessaire.	
dot1dStpPortState [1]	L'état actuel du port comme défini par application du protocole spanning-tree. La valeur de retour peut être l'une des valeurs suivantes : disabled (1), blocking (2), listening (3), learning (4), forwarding (5) ou broken (6).	1.3.6.1.2.1.17.2.15.1.3	Comme nécessaire.	

Nom d'objet	Description d'objet	OID	Intervalle d'interrogation	Seuil
CISCO-MEMORY-POOL-MIB				

ciscoMemoryPoolUsed	Indique le nombre d'octets de la mémoire commune qui sont actuellement en service par des applications sur le périphérique contrôlé.	1.3.6.1.4.1.9.9.48.1.1.1.5	30 mn	Spécification de base
ciscoMemoryPoolFree	Indique le nombre d'octets de la mémoire commune qui sont actuellement inutilisés sur le périphérique contrôlé. **Remarque:** La somme de ciscoMemoryPoolUsed et ciscoMemoryPoolFree est la quantité totale de mémoire dans le pool.	1.3.6.1.4.1.9.9.48.1.1.1.6	30 mn	Spécification de base
ciscoMemoryPoolLargestFree	Indique le plus grand nombre d'octets contigus qui sont actuellement inutilisés sur le périphérique contrôlé.	1.3.6.1.4.1.9.9.48.1.1.1.7	30 mn	Spécification de base

Référez-vous à la Boîte à outils de gestion de réseau Cisco - MIB pour plus d'informations sur la

prise en charge de MIB par Cisco.

Remarque: Certains MIB standards supposent qu'une entité SNMP particulière contient seulement une instance du MIB. Ainsi, le MIB standard n'a aucun index qui permet à des utilisateurs d'accéder directement à une instance particulière du MIB. Dans ces cas, l'indexation de la chaîne de caractères communautaire est fournie afin d'accéder à chaque instance du MIB standard. La syntaxe est [community string] @ [instance number], où l'instance est généralement un numéro de VLAN.

Autres options

Les aspects de sécurité du SNMPv3 signifient que son utilisation va normalement rattraper snmpv2 au bout d'un certain temps. Cisco recommande aux clients de se préparer pour ce nouveau protocole en tant qu'élément de leur stratégie NMS. Les avantages sont que les données peuvent être collectées en toute sécurité à partir des périphériques SNMP sans crainte d'altération ou de corruption. Les informations confidentielles, telles que la commande de définition SNMP pour les paquets qui changent de configuration de commutation, peuvent être chiffrées pour empêcher leur contenu d'être exposé sur le réseau. En outre, les différents groupes d'utilisateurs peuvent avoir différents privilèges.

Remarque: La configuration de SNMPv3 est sensiblement différente de la ligne de commande snmpv2, et il faut s'attendre à une augmentation de la charge CPU sur Supervisor Engine.

Télésurveillance

RMON permet aux données MIB d'être prétraitées par le périphérique réseau lui-même, en vue des utilisations communes ou application de ces informations par l'administrateur réseau, tel qu'exécuter la détermination de base historique et l'analyse de seuil.

Les résultats du traitement RMON sont enregistrés dans les MIB RMON pour la collection suivante par NMS, comme défini dans RFC 1757 .

Aperçu opérationnel

Les commutateurs Catalyst supportent mini-RMON dans le matériel sur chaque port, qui se compose de quatre groupes RMON-1 de base : Statistiques (groupe 1), historique (groupe 2), alarmes (groupe 3), et événements (groupe 9).

La partie la plus importante de RMON-1 est le **mécanisme de seuil** fourni par **les groupes d'alarmes et d'événements**. Comme discuté, la configuration des seuils RMON permet au commutateur d'envoyer un message dérouté SNMP quand un événement anormal se produit. Une fois que les ports principaux ont été identifiés, SNMP peut être utilisé afin d'interroger les compteurs ou les groupes historiques RMON et de créer des spécifications de base enregistrant l'activité de trafic normale pour ces ports. Par la suite, des seuils RMON d'augmentation et de chute peuvent être définis et des alarmes configurées pour quand il y a un écart défini de la spécification de base.

La configuration des seuils est idéalement exécutée avec un module de gestion RMON, puisque la création réussie des lignes des paramètres dans les tables d'alarmes et d'événements est pénible. Des modules commerciaux RMON NMS, tels que Cisco Traffic Director, qui fait partie de Cisco Works 2000, incorporent des GUI qui rendent la configuration des seuils RMON beaucoup

plus simple.

Pour la spécification de base, le groupe etherStats fournit une plage utile de statistiques de trafic L2 Les objets dans cette table peuvent être utilisés pour obtenir des statistiques sur la monodiffusion, la multidiffusion, le trafic de diffusion aussi bien qu'un grand choix d'erreurs L2. L'agent RMON sur le commutateur peut également être configuré pour enregistrer ces valeurs échantillonnées dans le groupe d'historique. Ce mécanisme active la quantité d'interrogation à réduire sans réduire le taux d'échantillonnage. Les historiques RMON peuvent donner des spécifications de base précises sans temps système substantiel d'interrogation. Cependant, plus vous collectez d'historiques, plus de ressources de commutation sont utilisées.

Tandis que les commutateurs fournissent seulement quatre groupes de base de RMON-1, il est important de ne pas oublier le reste de RMON-1 et de RMON-2. Tous les groupes sont définis dans RFC 2021, y compris UsrHistory (groupe 18) et ProbeConfig (groupe 19). Les informations L3 et plus élevées peuvent être récupérées sur les commutateurs grâce aux fonctions de port SPAN ou de redirection VLAN ACL qui vous permettent de copier du trafic vers un RMON SwitchProbe externe ou un module d'analyse de réseau interne (NAM).

Les NAM supportent tous les groupes RMON et peuvent même examiner **les données de la couche application**, y compris les données Netflow exportées des Catalyst quand MLS est activé. L'exécution MLS signifie que le routeur ne commute pas tous les paquets dans un écoulement, ainsi seulement les données d'exportation de Netflow et non les compteurs d'interface fournissent des informations de gestion VLAN fiables.

Vous pouvez employer un port SPAN et une sonde de commutateur pour saisir un flux de paquets pour un port particulier, une liaison agrégée ou un VLAN et pour télécharger les paquets pour décoder avec un module de gestion RMON. Le port SPAN est contrôlable par SNMP via le groupe SPAN dans le CISCO-STACK-MIB, ainsi il est facile d'automatiser ce processus. Le Traffic Director se sert de ces fonctions avec sa fonctionnalité d'agent de surclassement.

Il y a des mises en garde à l'enjambement de tout un VLAN. Même si vous utilisez une sonde 1Gbps, le flux de paquets entier d'un VLAN ou même un port en mode bidirectionnel simultané 1Gbps peut dépasser la bande passante du port SPAN. Si le port SPAN fonctionne constamment à bande passante maximale, des données risquent d'être perdues. Référez-vous à Configuration de la fonctionnalité Catalyst Switched Port Analyzer (SPAN) pour plus de détails.

Recommandation

Cisco recommande de déployer des seuils RMON et un mécanisme d'alerte afin de simplifier la gestion de réseau de manière plus intelligente que l'interrogation SNMP. Ceci réduit le temps système du trafic de gestion du réseau et permet au réseau d'alerter intelligemment quand quelque chose a changé dans la spécification de base. RMON doit être piloté par un agent externe comme Traffic Director ; il n'y a aucun support de CLI. Émettez ces commandes afin d'activer RMON :

```
set snmp rmon enable
set snmp extendedrmon netflow enable mod
!--- For use with NAM module only.
```

Il est important de se rappeler que la fonction principale d'un commutateur est d'expédier des trames, pas d'agir en tant que grande sonde de multi-port RMON. Par conséquent, quand vous définissez des historiques et des seuils sur plusieurs ports pour des conditions multiples, gardez à l'esprit que des ressources sont consommées. Considérez un module NAM si vous agrandissez

RMON. Rappelez-vous également cette règle primordiale de port : n'interrogez et ne définissez des seuils que sur les ports identifiés comme importants dans l'étape de planification.

Configurations requises en matière de mémoire

L'utilisation mémoire de RMON est constante à travers toutes les plates-formes de commutation concernant les statistiques, les historiques, les alarmes, et les événements. RMON utilise un compartiment afin d'enregistrer des historiques et statistiques sur l'agent RMON (le commutateur, dans ce cas). La taille de compartiment est définie sur la sonde RMON (sonde de commutation) ou l'application RMON (Traffic Director), puis envoyée au commutateur afin d'être définie. Typiquement, les contraintes de mémoire sont seulement une considération sur les Supervisor Engine plus anciens à moins de 32Mo de DRAM. Référez-vous à ces directives :

- Approximativement 450K de l'espace de code est ajouté à l'image NMP afin de supporter le mini-RMON (qui est quatre groupes de RMON : statistiques, historique, alarmes, et événements). La configuration requise en mémoire dynamique pour le RMON varie parce qu'elle dépend de la configuration de l'exécution. L'information sur l'utilisation mémoire du RMON d'exécution pour chaque groupe de mini-RMON est expliquée ici :Groupe Ethernet Statistics - Prend 800 octets pour chaque interface Ethernet/FE commutée.Groupe d'historique - Pour l'interface Ethernet, chaque entrée de contrôle d'historique configurée avec 50 compartiments prend approximativement 3.6Ko et 56 octets d'espace mémoire pour chaque compartiment supplémentaire.Groupes d'alarmes et d'événements - Prend 2.6Ko pour chaque alarme configurée et ses entrées d'événement correspondantes.
- La sauvegarde de la configuration RMON prend approximativement 20K NVRAM d'espace si la taille totale du NVRAM est de 256K ou plus et 10K NVRAM d'espace si la taille totale du NVRAM est de 128K.

Network Time Protocol

Le NTP, RFC 1305 , synchronise la mesure du temps entre différents serveur temporels et clients distribués et permet aux événements d'être corrélés quand des entrées de journal sont créées ou que d'autres événements temporels se produisent.

NTP fournit des exactitudes de l'horloge client, typiquement en une milliseconde sur des LAN et jusqu'à quelques dizaines de millisecondes sur des WAN, relativement à un serveur principal synchronisé à l'heure universelle coordonnée (UTC). 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.

Aperçu opérationnel

NTP a été documenté la première fois dans RFC 958 , mais a évolué par RFC 1119 (NTP version 2) et en est maintenant à sa troisième version comme défini dans RFC 1305 . Il s'exécute sur le port UDP 123. Toute la transmission NTP utilise l'UTC, qui est identique à l'heure du méridien de Greenwich.

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 synchronisés aux serveurs principaux qui fournissent une synchronisation à plus de 100 000 clients et serveurs sur Internet. Les listes actuelles sont stockées sur la page de listes de serveurs NTP publics, qui est mise à jour régulièrement. Il y a aussi de nombreux serveurs primaires et secondaires privés pas normalement disponibles au public. Pour une liste de serveurs NTP publics et des informations sur la façon de les utiliser, consultez le site Web de l'université du Delaware Serveur de synchronisation temporelle .

Puisqu'il n'y a aucune garantie que ces serveurs NTP Internet publics seront disponibles, ou qu'ils produisent l'heure correcte, il est fortement recommandé que d'autres options soient considérées. Ceci pourrait inclure l'utilisation de divers périphériques de positionnement globaux autonomes du service (GPS) directement connectés à un certain nombre de routeurs.

Une autre option possible est l'utilisation de divers routeurs configurés comme maîtres de la strate 1, bien que ceci ne soit pas recommandé.

Strate

Chaque server NTP adopte une strate qui indique à quelle distance d'une source temporelle externe le serveur se trouve. Les serveurs de la strate 1 ont accès à un certain genre de source temporelle externe, telle qu'une horloge radio. Les serveurs de la strate 2 obtiennent des détails temporels à partir d'un ensemble nominé de serveurs de la strate 1, alors que les serveurs de la strate 3 obtiennent ces détails à partir des serveurs de la strate 2, etc.

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 est répond aux requêtes client, mais essaye d'utiliser les requêtes client en tant qu'étant un candidat potentiel pour une meilleure source temporelle et pour faciliter la stabilisation de sa fréquence d'horloge.
- Afin d'être un véritable partenaire, les deux côtés de la connexion doivent entrer dans un rapport de partenariat plutôt que d'avoir un utilisateur homologue et un autre utilisateur serveur. Il est également recommandé que les homologues échangent des clés de sorte que seuls les hôtes de confiance parlent entre eux 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 et garde des informations d'état sur le client pour savoir quelle est la qualité de sa mesure du temps et quel serveur de strate il exécute.**Remarque:** CatOS peut seulement agir en tant que client NTP.

Ce n'est aucun problème pour qu'un serveur NTP gère des milliers de clients. Cependant, la gestion de centaines d'homologues a un impact sur la mémoire, et la conservation de l'état consomme plus de ressources CPU et de bande passante sur le cadre.

Vote

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

le NTP est d'abord configuré sur un périphérique Cisco, il envoie huit requêtes consécutifs rapides à des intervalles NTP_MINPOLL (24 = 16 secondes). Le NTP_MAXPOLL est de 214 secondes (qui est 16.384 secondes ou 4 heures, 33 minutes, 4 secondes), le temps maximal qu'il faut avant que NTP ne demande une réponse à nouveau. Actuellement, Cisco n'a pas de méthode pour forcer manuellement la durée POLL à être définie par l'utilisateur.

Le NTP votant des débuts de compteur à 2^6 (64) secondes et est par unités de deux incrémenté (comme sync de deux serveurs les uns avec les autres), à 2^{10}. C'est-à-dire, vous pouvez s'attendre aux messages de sync à envoyer à un intervalle de 64, 128, 256, 512, ou 1024 secondes par serveur ou pair configuré. Cette durée varie entre 64 secondes et 1024 secondes comme unité de deux basée sur la boucle de phase qui envoie et reçoit des paquets. S'il y a beaucoup de gigue dans la durée, elle procède plus souvent à des interrogations. Si l'horloge de référence est précise et la connectivité réseau cohérente, vous voyez les durée d'interrogation converger sur 1024 secondes entre chaque interrogation.

Dans la réalité, ceci signifie que l'intervalle entre deux interrogations NTP change pendant que la connexion entre le client et le serveur change. Plus la connexion est bonne, plus l'intervalle entre deux interrogations est long, signifiant que le client NTP a reçu huit réponses pour ses huit dernières demandes (l'intervalle entre deux interrogations est alors doublé). Une réponse manquée simple cause une division par deux de l'intervalle d'interrogation. L'intervalle entre deux interrogations commence à 64 secondes et va à un maximum de 1024 secondes. Dans les meilleures circonstances, il faut un peu plus de deux heures pour que l'intervalle entre deux interrogations aille de 64 secondes à 1024 secondes.

Émissions

Les diffusions NTP ne sont jamais expédiées. La commande **ntp broadcast** force le routeur à émettre des diffusions NTP sur l'interface où il est configuré. La commande broadcastclient de ntp entraîne le routeur ou le commutateur à écouter le NTP annonce sur l'interface sur laquelle il est configuré.

Niveaux de trafic NTP

La bande passante utilisée par NTP est minimale, puisque l'intervalle entre les messages d'interrogation échangés par les homologues ne dépasse généralement pas un message toutes les 17 minutes (1024 secondes). Avec une planification soigneuse, ceci peut être maintenu dans des réseaux de routeurs sur les liaisons WAN. Les clients NTP doivent établir une relation d'homologue avec les serveurs NTP locaux, pas dans tout le WAN jusqu'aux routeurs principaux du site central, qui seront les serveurs de la strate 2.

Un client NTP en convergence utilise approximativement 0,6 bits/seconde par serveur.

Recommandation

Beaucoup de clients font configurer NTP dans le mode client aujourd'hui sur leurs plates-formes CatOS, synchronisé à partir de plusieurs sources fiables d'Internet ou d'une horloge radio. Cependant, 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 permet à un domaine tout entier de Catalyst de recevoir une horloge à partir d'un seul message 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. Les préoccupations en matière de sécurité peuvent être abordées de ces deux manières :

- Mises à jour de serveur de filtrage
- Authentification

La corrélation temporelle d'événements est extrêmement précieuse dans deux cas : audits de dépannage et de sécurité. Un soin tout particulier doit être apporté pour protéger les sources temporelles et les données, et le chiffrement est recommandé de sorte que les événements clés ne soient pas effacés intentionnellement ou involontairement.

Cisco recommande ces configurations :

Configuration d'un Catalyst

```
set ntp broadcastclient enable
set ntp authentication enable
set ntp key key
!--- This is a Message Digest 5 (MD5) hash. set ntp
timezone <zone name>
set ntp summertime <date change details>
```

Configuration alternative de Catalyst

```
!--- This more traditional configuration creates !---
more configuration work and NTP peerings. set ntp client
enable
set ntp server IP address of time server set timezone
zone name set summertime date change details
```

Configuration de routeur

```
!--- This is a sample router configuration to distribute
!--- NTP broadcast information to the Catalyst broadcast
clients. ntp source loopback0
ntp server IP address of time server ntp update-calendar
clock timezone zone name clock summer-time date change
details ntp authentication key key ntp access-group
access-list
!--- To filter updates to allow only trusted sources of
NTP information. Interface to campus/management VLAN
containing switch sc0 ntp broadcast
```

Cisco Discovery Protocol

CDP échange des informations entre les périphériques contigus sur la couche liaison de données et est extrêmement utile dans la détermination de la topologie du réseau et de la configuration physique en dehors de la couche logique ou IP. Les périphériques supportés sont principalement des commutateurs, des routeurs, et des téléphones IP. Cette section met en valeur certaines des améliorations de la version 2 de CDP par rapport à la version 1.

Aperçu opérationnel

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, protocole HDLC 0x2000** est utilisée. Sur des Token Ring, l'adresse fonctionnelle c000.0800.0000 est utilisée. Des trames CDP sont envoyées

périodiquement, chaque minute par défaut.

Les messages CDP contiennent un ou plusieurs sous-messages qui permettent aux périphériques de destination de recueillir et stocker des informations au sujet de chaque périphérique voisin.

CDP version 1 supporte ces paramètres :

Paramètre	Type	Description
1	Device-ID	Nom d'hôte du périphérique ou numéro de série du matériel dans l'ASCII.
2	Adresse	Adresse L3 de l'interface qui a envoyé la mise à jour.
3	Port-ID	Le port sur lequel la mise à jour de CDP a été envoyée.
4	Capacités	Décrit les capacités fonctionnelles du périphérique : Routeur : Pont TB 0x01 : Pont SR 0x02 : Commutateur 0x04 : Hôte 0x08 (fournit la commutation L2 et/ou L3) : filtrage conditionnel IGMP 0x10 : 0x20 Le pont ou le commutateur n'expédie pas les paquets de rapport IGMP sur des ports non-routeurs. Répéteur : 0x40
5	Version	Une chaîne de caractères contenant la version du logiciel (mêmes que dans **show version**).
6	Plate-forme	Plate-forme matérielle, telle que WS-C5000, WS-C6009, ou Cisco RSP.

Dans la version 2 de CD, des champs de protocole supplémentaires ont été introduits. La version 2 de CDP supporte n'importe quel champ, mais ceux mentionnés peuvent être particulièrement utiles dans les environnements commutés et sont utilisés dans CatOS.

Remarque: Quand un commutateur exécute CDPv1, il abandonne les trames v2. 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, c'est le VLAN non balisé.
11	Mode bidirectionnel simultané/en	Ce champ contient la configuration de bidirectionnalité du port

	alternat	émetteur.

Recommandation

CDP est activé par défaut et est essentiel pour gagner une visibilité des périphériques contigus et pour le dépannage. Il est également utilisé par des applications de gestion de réseau pour construire les cartes topologiques L2. Émettez ces commandes afin d'installer CDP :

```
set cdp enable
!--- This is the default. set cdp version v2
!--- This is the default.
```

Dans les parties du réseau où un haut niveau de sécurité est requis (comme les DMZ confrontés à Internet), CDP doit être arrêté de cette façon :

```
set cdp disable port range
```

La commande show cdp neighbors affiche la table CDP locale. Les entrées identifiées par une étoile (*) indiquent une erreur d'assortiment de VLAN ; les entrées identifiées par a # indiquent une erreur de correspondance de bidirectionnalité. Ceci peut être une aide importante pour le dépannage.

```
>show cdp neighbors

* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port  Device-ID          Port-ID Platform
----- ------------------ ------- ------------
 3/1  TBA04060103(swi-2) 3/1     WS-C6506
 3/8  TBA03300081(swi-3) 1/1     WS-C6506
15/1  rtr-1-msfc         VLAN 1  cisco    Cat6k-MSFC
16/1  MSFC1b             Vlan2   cisco    Cat6k-MSFC
```

Autres options

Quelques commutateurs, comme Catalyst 6500/6000, ont la capacité d'assurer l'alimentation par des câbles UTP aux téléphones IP. L'information reçue par le CDP aide la gestion de l'alimentation sur le commutateur.

Comme les téléphones IP peuvent avoir un PC connecté à eux, et les deux périphériques se connectent au même port sur Catalyst, le commutateur a la capacité de placer le téléphone VoIP dans un VLAN séparé, l'auxiliaire. Ceci permet au commutateur d'appliquer facilement une différente Qualité de service (QoS) pour le trafic VoIP.

En outre, si le VLAN auxiliaire est modifié (par exemple, afin de forcer le téléphone à utiliser un VLAN spécifique ou une méthode d'étiquetage spécifique), cette information est envoyée au téléphone par CDP.

Paramètre	Type	Description
14	ID 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 d'énergie qu'un téléphone VoIP consomme, en milliwatts.

Remarque: Les commutateurs Catalyst 2900 et 3500XL ne supportent pas actuellement CDPv2.

Configuration de la sécurité

Dans le meilleur des cas, le client a déjà établi une stratégie de sécurité pour définir quels outils et technologies Cisco sont qualifiés.

Remarque: Le Logiciel Cisco IOS Security, par opposition à CatOS, est traité dans beaucoup de documents, tels que Cisco ISP Essentials.

Fonctions de sécurité de base

Mots de passe

Configurez un mot de passe de niveau utilisateur (connexion). Les mots de passe distinguent les majuscules et minuscules dans CatOS 5.x et versions ultérieures, et peuvent être de 0 à 30 caractères de longueur, y compris les espaces. Définissez le mot de passe d'activation :

set password *password* **set enablepass** *password*

Tous les mots de passe doivent respecter des normes de longueur minimale (par exemple, six caractères minimum, un mélange de lettres et de chiffres, de majuscules et de minuscules) pour l'identifiant et les mots de passe d'activation. Ces mots de passe sont chiffrés en utilisant l'algorithme de hachage MD5.

Afin de permettre une plus grande flexibilité dans la gestion de la sécurité par mot de passe et de l'accès périphérique, Cisco recommande l'utilisation d'un serveur TACACS+. Référez-vous à la section TACACS+ de ce document pour plus d'informations.

Secure Shell

Utilisez le chiffrement SSH afin de sécuriser les sessions Telnet et d'autres connexions distantes au commutateur. Le chiffrement SSH est supporté seulement pour les connexions distantes au commutateur. Vous ne pouvez pas chiffrer les sessions Telnet qui sont initiées à partir du commutateur. SSH version 1 est supporté dans CatOS 6.1, et la prise en charge de la version 2 a été ajoutée dans CatOS 8.3. SSH version 1 supporte le Data Encryption Standard (DES) et les méthodes de chiffrement du Triple-DES (3-DES), et SSH version 2 supporte le 3-DES et les méthodes de chiffrement d'Advanced Encryption Standard (AES). Vous pouvez utiliser le chiffrement SSH avec l'authentification RADIUS et TACACS+. Cette fonctionnalité est supportée avec des images SSH (k9). Référez-vous à Configuration de SSH sur des commutateurs Catalyst exécutant CatOS pour plus de détails.

set crypto key rsa 1024

Afin de désactiver le retour à la version 1 et accepter les connexions à la version 2, émettez cette commande :

```
set ssh mode v2
```

Filtres d'autorisation IP

Ce sont des filtres pour sauvegarder l'accès à l'interface de gestion sc0 par le telnet et d'autres protocoles. Ils sont particulièrement importants quand le VLAN utilisé pour la gestion contient également des utilisateurs. Émettez ces commandes afin d'activer le filtrage d'adresses IP et de ports :

```
set ip permit enable
set ip permit IP address mask Telnet|ssh|snmp|all
```

Cependant, si l'accès Telnet est limité avec cette commande, l'accès aux périphériques CatOS peut seulement être réalisé par quelques stations d'extrémité de confiance. Cette configuration peut être un obstacle dans le dépannage. Maintenez dans l'esprit qu'il est possible de mystifier des adresses IP et de duper l'accès filtré, ainsi c'est seulement la première couche de protection.

Sécurité de port

Considérez l'utilisation d'une sécurité de port afin de permettre à seulement une ou plusieurs adresses MAC connues de passer des données sur un port particulier (pour empêcher les stations d'extrémité statiques d'être permutées contre de nouvelles stations sans contrôle de modification, par exemple). C'est possible grâce aux adresses MAC statiques.

```
set port security mod/port enable MAC address
```

C'est également possible en apprenant des adresses MAC limitées dynamiquement.

```
set port security port range enable
```

Ces options peuvent être configurées :

- set port security mod/port age time value — spécifie la durée pendant laquelle les adresses du port sont sécurisées avant qu'une nouvelle adresse puisse être apprise. La durée valide en minutes est 10 - 1440. La valeur par défaut est aucun vieillissement.
- set port securitymod/port maximum value — mot clé qui spécifie le nombre maximal d'adresses MAC à sécuriser sur le port. Les valeurs valides sont 1 (défaut) - 1025.
- set port security mod/port violation shutdown — arrête le port (défaut) si une violation se produit et envoie un message syslog (défaut) et ignore le trafic.
- set port security mod/port shutdown time value — durée pendant laquelle un port reste désactivé. Les valeurs valides sont de 10 - 1440 minutes. La valeur par défaut est l'arrêt permanent.

Avec CatOS 6.x et plus tard, Cisco a introduit l'authentification 802.1x qui permet à des clients de s'authentifier sur un serveur central avant que des ports puissent être activés pour des données. Cette fonctionnalité commence à être supportée sur des plates-formes telles que Windows XP, mais peut être considérée comme une direction stratégique par beaucoup d'entreprises. Référez-vous à Configuration de la sécurité du port pour plus d'informations sur la façon de configurer la sécurité de port sur les commutateurs qui exécutent le logiciel Cisco IOS.

Bannières de procédure de connexion

Créez des messages de périphériques appropriés pour énoncer spécifiquement les actions prises pour l'accès non autorisé. N'annoncez pas le nom du site ou les données réseau qui pourraient fournir des informations aux utilisateurs non autorisés. Ces messages fournissent un recours au cas où un périphérique serait compromis et l'auteur est attrapé :.

```
# set banner motd ^C
*** Unauthorized Access Prohibited ***
***  All transactions are logged   ***
------------- Notice Board -------------
----Contact Joe Cisco at 1 800 go cisco for access problems----
^C
```

Sécurité physique

Les périphériques ne doivent pas être accessibles physiquement sans autorisation appropriée, ainsi le matériel doit être dans un espace (verrouillé) contrôlé. afin de s'assurer que le réseau reste opérationnel et inchangé par l'influence malveillante de facteurs environnementaux, tout le matériel doit avoir l'UPS approprié (avec des sources redondantes si possible) et un contrôle de la température (climatisation). Rappelez-vous, si l'accès physique est violé par une personne avec des intentions malveillantes, l'interruption par la récupération de mot de passe ou d'autres méthodes est beaucoup plus probable.

Terminal Access Controller Access Control System

Par défaut, les mots de passe non-privilégiés et en mode favorisé sont globaux et s'appliquent à chaque utilisateur qui accède au commutateur ou au routeur, soit à partir du port de console soit par une session Telnet à travers le réseau. Leur mise en place sur des périphériques réseau est longue et non-centralisée. Il est également difficile de mettre en application des restrictions d'accès utilisant les listes d'accès qui peuvent être enclines aux erreurs de configuration.

Trois systèmes de sécurité sont disponibles pour contrôler et régler l'accès aux périphériques réseau. Ceux-ci utilisent les architectures client/serveur pour placer toutes les informations relatives à la sécurité dans une base de données centrale simple. Ces trois systèmes de sécurité sont :

- TACACS+
- RAYON
- Kerberos

TACACS+ est un déploiement commun dans les réseaux Cisco et est le centre de ce chapitre. Il fournit ces fonctionnalités :

- Authentification - l'identification et le processus de vérification pour un utilisateur. Plusieurs méthodes peuvent être utilisées pour authentifier un utilisateur, mais la plus commune est la combinaison du nom de l'utilisateur et du mot de passe.
- Autorisation - diverses commandes peuvent être accordées une fois qu'un utilisateur est authentifié.
- Comptabilité - l'enregistrement de ce que l'utilisateur fait ou a fait sur le périphérique.

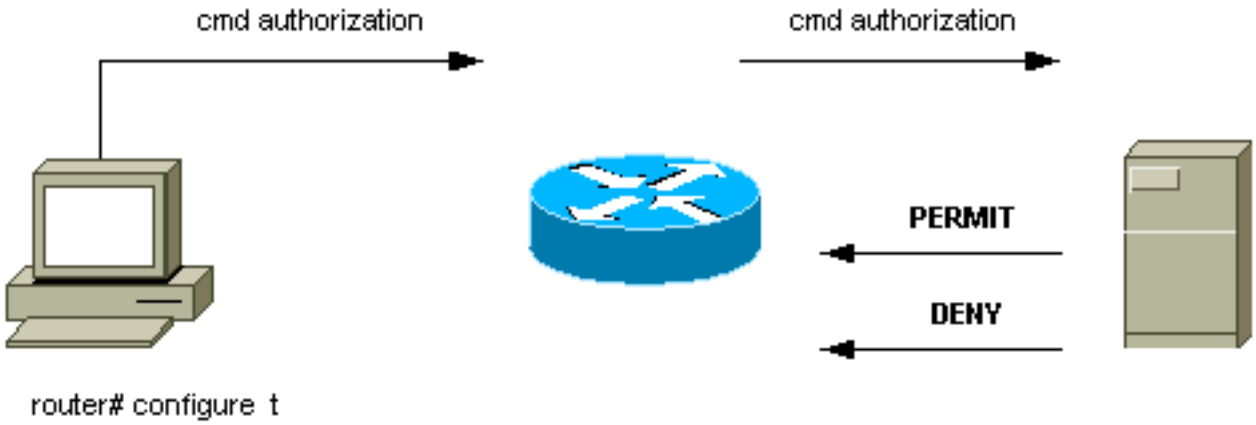
Référez-vous à Configuration de TACACS+, RADIUS, et Kerberos sur les commutateurs Cisco Catalyst pour plus de détails.

Aperçu opérationnel

Le protocole TACACS+ transmet les identifiants et les mots de passe au serveur centralisé, chiffrés sur le réseau à l'aide du **MD5** hachage à sens unique (RFC 1321). Il utilise le port TCP 49 en tant que protocole de transport ; ceci offre ces avantages par rapport à l'UDP (utilisé par RADIUS) :

- Transport orienté connexion
- Séparez l'accusé de réception de la requête (TCP ACK), indépendamment de la charge que subit actuellement le mécanisme d'authentification principal.
- Indication immédiate d'une panne de serveur (paquets 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. Cela offre un plus grand contrôle des commandes pouvant être exécutées sur le commutateur tout en étant découplées du mécanisme d'authentification. Utilisant la commande accounting, il est possible de faire un audit des commandes qu'un utilisateur particulier a émises tandis qu'attaché à un périphérique réseau particulier.



Quand un utilisateur tente une procédure de connexion ASCII par l'authentification à un périphérique réseau avec TACACS+, ce processus se produit typiquement :

- Quand la connexion est établie, le commutateur contacte le daemon TACACS+ pour obtenir une invite de nom d'utilisateur, qui est alors affichée à 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 peut être refusé davantage d'accès ou est invité à réessayer la séquence d'ouverture de connexion selon le daemon TACACS+.ERROR - une erreur s'est produite à un moment donné pendant l'authentification. Ceci 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 invité pour les 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 daemon TACACS+ est de nouveau contacté et renvoie une réponse ACCEPT ou REJECT d'autorisation. Si la réponse ACCEPT est

retournée, la réponse contient des données sous forme d'attributs qui sont utilisés pour diriger l'EXEC ou la session NETWORK pour cet utilisateur, et détermine les commandes auxquelles l'utilisateur peut accéder.

Recommandation

Cisco recommande l'utilisation de TACACS+, car elle peut être facilement mise en application utilisant CiscoSecure ACS pour NT, unix, ou tout autre logiciel tiers. Les fonctionnalités TACACS+ incluent la gestion des comptes détaillée pour fournir des statistiques sur l'utilisation des commandes et l'utilisation du système, l'algorithme de chiffrement MD5, et le contrôle d'administration des processus d'authentification et d'autorisation.

Dans cet exemple, les modes de connexion et d'activation utilisent le serveur TACACS+ pour l'authentification et peuvent revenir à l'authentification locale si le serveur est indisponible. C'est une porte dérobée importante à partir dans la plupart des réseaux. Émettez ces commandes pour installer TACACS+ :

```
set tacacs server server IP primary set tacacs server server IP
!--- Redundant servers are possible. set tacacs attempts 3
!--- This is the default. set tacacs key key
!--- MD5 encryption key. set tacacs timeout 15
!--- Longer server timeout (5 is default). set authentication login tacacs enable
set authentication enable tacacs enable
set authentication login local enable
set authentication enable local enable
!--- The last two commands are the default; they allow fallback !--- to local if no TACACS+
server available.
```

Autres options

Il est possible d'utiliser une autorisation TACACS+ pour contrôler les commandes que chaque utilisateur ou groupe d'utilisateurs peut exécuter sur chaque commutateur, mais il est difficile d'émettre une recommandation parce que tous les clients ont différentes conditions requises dans cette zone. Référez-vous à Contrôle de l'accès au commutateur à l'aide de Authentication, Authorization, and Accounting (AAA) pour plus d'informations.

En conclusion, les commandes de traçabilité fournissent une piste d'audit de ce que chaque utilisateur a tapé et a configuré. Voici un exemple utilisant la pratique courante de recevoir les informations d'audit à la fin de la commande :

```
set accounting connect enable start-stop tacacs+
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
set accounting commands enable all start-stop tacacs+
set accounting update periodic 1
```

Cette configuration a ces caractéristiques :

- La commande **connect** active des traçabilités d'événement de connexion en sortie sur le commutateur comme telnet.
- La commande **exec** active des traçabilités des sessions de connexion sur le commutateur comme le personnel chargé des opérations.
- La commande **system** active la gestion des comptes des événements système sur le

commutateur comme le rechargement ou la réinitialisation.
- La commande **commands** active la gestion des comptes ce qui a été saisi sur le commutateur, pour chacune des deux commandes **show et configuration**.
- Les mises à jour périodique chaque minute sur le serveur sont utiles afin d'enregistrer si des utilisateurs sont encore connectés.

Liste de contrôle de la configuration

Cette section fournit un résumé des configurations recommandées, à l'exclusion des éléments de sécurité.

Il est extrêmement utile d'étiqueter tous les ports. Émettez cette commande afin d'étiqueter les ports :

`set port description` *descriptive name*

Utilisez cette clé en même temps que les tables de commandes répertoriées :

Clé :
Texte en gras - changement recommandé
Texte normal - défaut, configuration recommandée

Commandes de configuration globale

Commande	Commentaire
set vtp domain name passwordx	Protégez-vous contre les mises à jour de VTP non autorisées par les nouveaux commutateurs.
set vtp mode transparent	Mode VTP spécifique favorisé dans ce document. Référez-vous à la section Protocole d'agrégation de liens VLAN de ce document pour plus de détails.
set spantree enable all	Assurez-vous que STP est activé sur tous les vlans.
set spantree root vlan	Recommandé pour placer les ponts racine (et racine secondaire) par VLAN.
set spantree backbonefast enable	Active la convergence STP rapide des pannes indirectes (seulement si tous les commutateurs du domaine supportent cette fonctionnalité).
set spantree uplinkfast enable	Active la convergence STP rapide des pannes directes (pour des commutateurs de la couche d'accès seulement).
set spantree portfast bpdu-guard enable	Permet d'arrêter le port automatiquement s'il y a une

	extension non autorisée de spanning-tree.
set udld enable	Active la détection de lien unidirectionnel (nécessite une configuration au niveau du port).
set test diaglevel complete	Active les diagnostics complets au démarrage (par défaut sur Catalyst 4500/4000).
set test packetbuffer sun 3:30	Active le contrôle d'erreurs du tampon de port (s'applique à catalyst 5500/5000 seulement).
set logging buffer 500	Maintenez au maximum la mémoire tampon interne de Syslog.
set logging server IP address	Configure le serveur syslog cible pour la journalisation de messages système externe.
set logging server enable	Autorise le serveur de journalisation externe.
set logging timestamp enable	Active l'horodatage des messages dans le journal.
set logging level spantree 6 default	Augmente le niveau de Syslog de STP par défaut.
set logging level sys 6 default	Augmente le niveau de Syslog de système par défaut.
set logging server severity 4	Permet l'exportation du Syslog au plus haut niveau de gravité seulement.
set logging console disable	Désactive la console sauf en cas de dépannage
set snmp community read-only string	Configure le mot de passe pour permettre la collecte de données distante.
set snmp community read-write string	Configure le mot de passe pour permettre la configuration distante.
set snmp community read-write-all string	Configure le mot de passe pour autoriser la configuration distante comprenant des mots de passe.
set snmp trap enable all	Active l'envoi de messages déroutés SNMP au serveur pour les alertes de défaillances et d'événements.
set snmp trap server address string	Configure l'adresse du récepteur de message dérouté NMS.
set snmp rmon enable	Active RMON pour la collecte locale de statistiques. Référez-vous à la section Contrôle à distance de ce document pour

	plus de détails.
set ntp broadcastclient enable	Active la réception d'une horloge système précise à partir d'un routeur ascendant.
set ntp timezone zone name	Définit le fuseau horaire local pour le périphérique.
set ntp summertime date change details	Configure l'heure d'été si c'est approprié pour le fuseau horaire.
set ntp authentication enable	Configure des informations horaires chiffrées pour des raisons de sécurité.
set ntp key key	Configure la clé de chiffrement.
set cdp enable	Vérifie que la découverte des voisins est activée (activé sur des ports par défaut).
set tacacs server IP address primary	Configure l'adresse du serveur AAA.
set tacacs server IP address	Des serveurs AAA redondants si possible.
set tacacs attempts 3	Permet 3 tentatives de saisie de mot de passe pour le compte utilisateur d'AAA.
set tacacs key key	Définit la clé de chiffrement MD5 AAA.
set tacacs timeout 15	Permet un plus long délai de temporisation du serveur (cinq secondes est la valeur par défaut).
set authentication login tacacs enable	Utilise AAA pour l'authentification de connexion.
set authentication enable tacacs enable	Utilise AAA pour l'authentification en mode enable.
set authentication login local enable	Par défaut ; permet le retour au local si aucun serveur AAA n'est disponible.
set authentication enable local enable	Par défaut ; permet le retour au local si aucun serveur AAA n'est disponible.

Commandes de configuration des ports hôtes

Commande	Commentaire
set port host port range	Supprime le traitement de port inutile. Cette macro définit le spantree PortFast enable, channel off, trunk off.
set udld disable port range	Supprime le traitement inutile de port (désactivé sur le port cuivre

	par défaut).
set port speed *port range* auto	Utilise la négociation automatique avec les pilotes NIC à jour.
set port trap *port range* disable	Aucun besoin de messages déroutés SNMP pour les utilisateurs généraux ; ne suit que les ports principaux.

Commandes de configuration du serveur

Commande	Commentaire
set port host port range	Supprime le traitement de port inutile. Cette macro définit le spantree PortFast enable, channel off, trunk off.
set udld disable port range	Supprime le traitement inutile de port (désactivé sur le port cuivre par défaut).
set port speed port range 10 / *100*	Configure habituellement les ports statique/serveur ; autrement, utilisez l'autonégociation.
set port duplex port range full / *moitié*	Habituellement ports statique/serveur ; autrement, utilisez l'autonégociation.
set port trap port range enable	Les ports de service principaux doivent envoyer un message dérouté à NMS.

Commandes de configuration de ports non utilisées

Commande	Commentaire
set spantree portfast *port range* disable	Active le traitement et la protection nécessaires de port pour STP.
set port disable port range	Désactive les ports inutilisés.
set vlan unused dummy vlan port range	Redirige le trafic non autorisé au VLAN inutilisé si le port est activé.
set trunk port range off	Désactive le port de la liaison agrégée jusqu'à ce qu'il soit géré.
set port channel port range mode off	Désactive le port de l'acheminement jusqu'à ce qu'il soit géré.

Ports d'infrastructure (commutateur-commutateur, commutateur-routeur)

Commande	Commentaire
set udld enable *port range*	Active la détection de liens unidirectionnels (pas par défaut sur les ports cuivre).
set udld aggressive-mode enable port range	Active le mode agressif (pour les périphériques qui le supportent).
set port negotiation *port rangeenable*	Autorise l'autonégociation GE par défaut des paramètres de liaison.
set port trap port range enable	Autorise les messages déroutés SNMP pour ces ports principaux.
set trunk port range off	Désactive la fonctionnalité si liaisons agrégées non utilisées.
set trunk mod/port desirable ISL / *dot1q* / *négociez*	Si vous utilisez des liaisons agrégées, dot1q est préféré.
clear trunk mod/port vlan range	Limite le diamètre STP en élaguant les VLAN des liaisons agrégées où ils ne sont pas nécessaires.
set port channel port range mode off	Désactive la fonctionnalité si canaux non utilisées.
set port channel port range mode desirable	Si vous utilisez des canaux, ceci active PAgP.
set port channel all distribution ip both	Autorise l'équilibrage de charge source/destination L3 si vous utilisez des canaux (par défaut sur Catalyst 6500/6000).
set trunk mod/port nonegotiate ISL / *dot1q*	Désactive DTP si vous établissez une liaison agrégée vers un routeur, un Catalyst 2900 XL, 3500, ou d'autres constructeurs.
set port negotiation mod/port disable	La négociation peut être incompatible pour quelques vieux périphériques GE.

Informations connexes

- Messages d'erreur CatOS courants sur les commutateurs de la gamme Catalyst 4500/4000
- Messages d'erreur CatOS courants sur les commutateurs de la gamme Catalyst 5000/5500

- Messages d'erreur CatOS courants sur les commutateurs de la gamme Catalyst 6500/6000
- Support pour commutateurs
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems