# Propagation monodiffusion dans les réseaux campus commutés

## Contenu



## Introduction

Ce document discute des causes et des implications possibles de la propagation des paquets monodiffusion dans des réseaux commutés.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

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

### Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

## Définition du problème

Les commutateurs LAN utilisent des tables de transfert (tables de couche 2 (L2), tables CAM (Content Addressable Memory)) pour diriger le trafic vers des ports spécifiques selon le numéro de VLAN et l'adresse MAC de destination de la trame. Quand il n'y a aucune entrée correspondant à l'adresse MAC de destination de la trame dans le VLAN entrant, la trame

(monodiffusion) est envoyée à tous les ports de transfert dans le VLAN respectif, ce qui entraîne la propagation.

La propagation limitée fait partie du processus normal de commutation. Il y a des situations, cependant, où la propagation continue peut entraîner une dégradation des performances sur le réseau. Ce document explique les problèmes qui peuvent se poser à cause de la propagation et les raisons les plus communes pour lesquelles un certain trafic peut constamment être propagé.

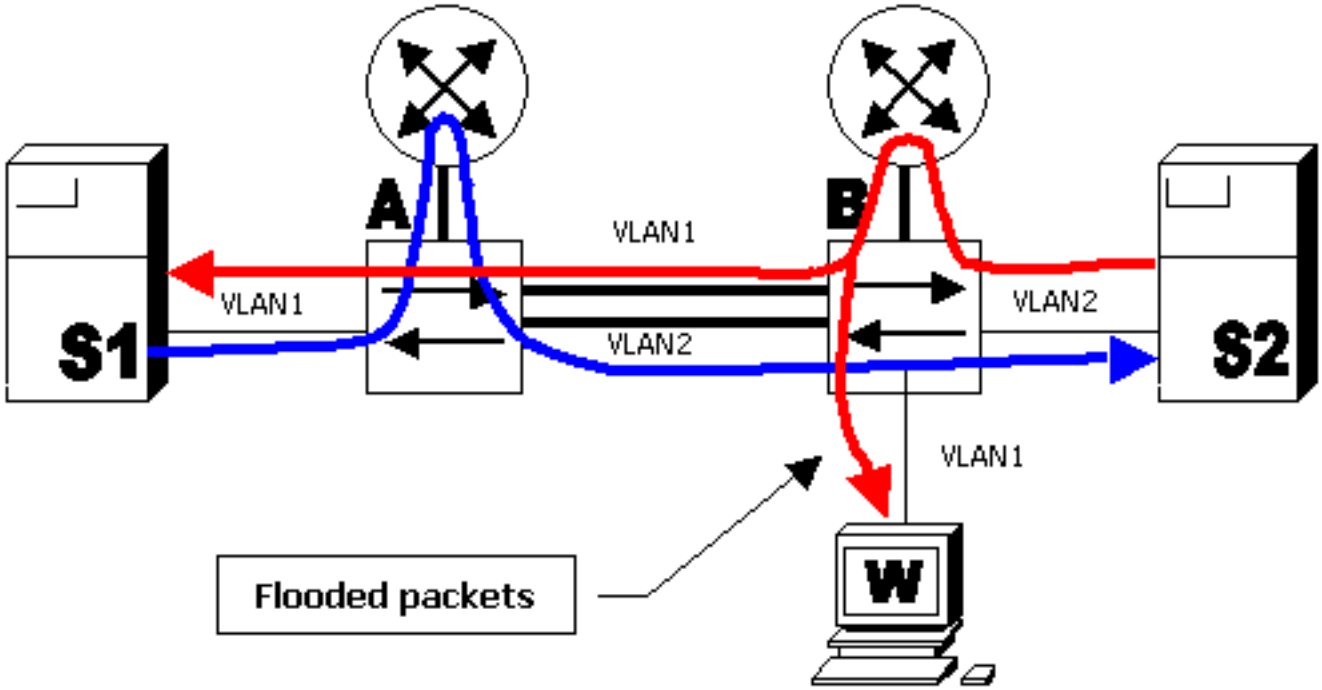
Notez que la plupart des commutateurs modernes comprenant les commutateurs des gammes Catalyst 2900 XL, 3500 XL, 2940, 2950, 2970, 3550, 3750, 4500/4000, 5000 et 6500/6000 gèrent les tables de transfert L2 par VLAN.

# Causes de la propagation

La cause même de la propagation est que l'adresse MAC de destination du paquet n'est pas dans la table de transfert L2 du commutateur. Dans ce cas, le paquet sera évacué de tous les ports de transfert dans son VLAN (sauf le port sur lequel il a été reçu). Les études de cas ci-dessous affichent les raisons les plus communes pour que l'adresse MAC de destination ne soit pas connue du commutateur.

## Cause 1 : Routage asymétrique

De grandes quantités de trafic propagé peuvent saturer les liens de faible bande passante et provoquer des problèmes de performances du réseau ou une panne complète de connectivité pour les périphériques connectés via ces liens de faible bande passante. Considérez le diagramme suivant :




Dans le schéma ci-dessus, le serveur S1 du VLAN 1 exécute la sauvegarde (transfert de données en masse) vers le serveur S2 du VLAN 2. La passerelle par défaut du serveur S1 pointe vers l'interface VLAN 1 du routeur A. Le serveur S2 a sa passerelle par défaut qui pointe vers l'interface VLAN 2 du routeur B. Les paquets de S1 à S2 suivent le chemin suivant :

- Comm1—VLAN 1—Commutateur A—Routeur A—VLAN 2—Commutateur B—VLAN 2—Comm2 (ligne bleue)

Les paquets de S2 à S1 suivent le chemin suivant :

- Comm2—VLAN 2—Commutateur B—Routeur B—VLAN 1—Commutateur A—Diffusé vers VLAN 1—Comm1 (ligne rouge)

Notez qu'avec un tel agencement, le commutateur A ne « voit » pas le trafic de l'adresse MAC S2 dans VLAN 2 (puisque l'adresse MAC source est réécrite par le routeur B et le paquet arrive seulement dans VLAN 1). Ceci signifie que, chaque fois que le commutateur A a besoin d'envoyer le paquet vers l'adresse MAC S2, le paquet est propagé vers VLAN 2. La même situation se produira avec l'adresse MAC S1 sur le commutateur B.

Ce comportement s'appelle routage asymétrique. Les paquets suivent des chemins différents selon la direction. Le routage asymétrique est l'une des deux causes les plus communes de la propagation.

### Impact de la propagation monodiffusion

En retournant à l'exemple qui précède, le résultat est que les paquets du transfert de données entre S1 et S2 seront en grande partie propagés vers VLAN 2 sur le commutateur A et VLAN 1 sur le commutateur B. Ceci signifie que chaque port connecté (station de travail W dans cet exemple) dans VLAN 1 sur le commutateur B recevra tous les paquets de conversation entre S1 et S2. Supposez que la sauvegarde du serveur utilise 50 Mbits/s de bande passante. Ce niveau de trafic saturera les liens de 10 Mbits/s. Ceci entraînera une panne complète de connectivité pour les PC ou les ralentira considérablement.

Cette propagation est due à un routage asymétrique et peut cesser quand le serveur S1 envoie un paquet de diffusion, par exemple le protocole de résolution d'adresse (ARP). Le commutateur A propagera ce paquet à VLAN 1 et le commutateur B recevra et apprendra l'adresse MAC de S1. Puisque le commutateur ne reçoit pas de trafic constamment, cette entrée de transfert expirera finalement et la propagation reprendra. Le même processus s'applique à S2.

Il y a différentes approches pour limiter la propagation provoquée par un routage asymétrique. Référez-vous à ces documents pour plus d'informations :

- Routage asymétrique avec groupes de ponts sur commutateurs Catalyst 2948G-L3 et 4908G-L3
- Routage asymétrique et HSRP (saturation excessive du trafic de monodiffusion dans le réseau avec les routeurs qui exécutent HSRP)

L'approche consiste normalement à rapprocher les délais d'expiration ARP du routeur et de la table de transfert des commutateurs. Les paquets ARP peuvent ainsi être diffusés. Un réapprentissage doit se produire avant que l'entrée de table de transfert L2 n'expire.

Un scénario typique où ce type de problème peut être observé est lorsqu'il y a des commutateurs redondants de couche 3 (L3) (tels qu'un Catalyst 6000 avec carte MSFC (Multillayer Switch Feature Card)) configurés pour équilibrer la charge avec le protocole HSRP (Hot Standby Router Protocol). Dans ce cas, un commutateur sera actif pour les VLAN pairs et l'autre sera actif pour les VLAN impairs.

## Cause 2 : Modifications de la topologie de protocole Spanning Tree

Un autre problème commun causé par la propagation est la notification de modification de topologie (TCN) de protocole Spanning Tree (STP). La notification TCN est conçue pour corriger des tables de transfert après modification de la topologie de transfert. C'est nécessaire pour éviter une panne de connectivité, comme quand après une modification de topologie, quelques destinations précédemment accessibles par l'intermédiaire de ports particuliers pourraient devenir accessibles par l'intermédiaire de différents ports. La notification TCN fonctionne en raccourcissant le délai d'expiration de la table de transfert : si l'adresse n'est pas réapprise, elle expire et la propagation reprend.

Les notifications TCN sont déclenchées par un port qui passe dans ou quitte l'état de transfert. Après la notification TCN, même si l'adresse MAC de destination particulière a expiré, la propagation ne devrait pas se produire longtemps dans la plupart des cas puisque l'adresse sera réapprise. Le problème peut survenir quand les notifications TCN se produisent à plusieurs reprises avec des intervalles courts. Les commutateurs faisant constamment vieillir rapidement leurs tables de transfert, la propagation sera presque constante.

Normalement, une notification TCN est rare dans un réseau bien configuré. Quand le port sur un commutateur monte ou descend, il y a finalement une notification TCN une fois que l'état STP du port passe dans ou quitte l'état de transfert. Quand le port s'agite, des notifications TCN répétitives et la propagation surviennent.

Les ports avec la fonctionnalité portfast STP activée n'entraîneront pas de notifications TCN en passant dans ou en quittant l'état de transfert. La configuration de portfast sur tous les ports de périphérique (tels que des imprimantes, des PC, des serveurs, etc.) devrait limiter les notifications TCN à une basse quantité. Référez-vous à ce document pour plus d'informations sur les notifications TCN :

- Présentation des changements de topologie SPT (Spanning-Tree Protocol)

**Remarque :** Dans MSFC IOS, il y a une optimisation qui déclenchera les interfaces VLAN à remplir à nouveau leurs tables ARP lorsqu'il y a un TCN dans le VLAN respectif. Ceci limite la propagation en cas de notifications TCN, car il y a une diffusion ARP et l'adresse MAC hôte est réapprise quand les hôtes répondent à ARP.

## Cause 3 : Dépassement de la capacité de la table de transfert

Une autre cause possible de la propagation peut être le dépassement de la capacité de la table de transfert du commutateur. Dans ce cas, de nouvelles adresses ne peuvent pas être apprises et les paquets destinés à de telles adresses sont propagés jusqu'à ce qu'un certain espace devienne disponible dans la table de transfert. Les nouvelles adresses seront alors apprises. C'est possible mais rare, puisque la plupart des commutateurs modernes ont des tables de transfert assez grandes pour accueillir les adresses MAC pour la plupart des conceptions.

L'épuisement des tables de transfert peut également être provoqué par une attaque sur le réseau où un hôte commence à générer des trames ayant chacune une adresse MAC différente. Ceci attachera toutes les ressources de la table de transfert. Une fois que les tables de transfert deviennent saturées, un autre trafic sera propagé car aucun nouvel apprentissage ne peut se produire. Ce genre d'attaque peut être détecté en examinant la table de transfert du commutateur. La plupart des adresses MAC indiqueront le même port ou groupe de ports. De telles attaques peuvent être empêchées en limitant le nombre d'adresses MAC apprises sur les ports non fiables à l'aide de la fonctionnalité de sécurité de port.

Les guides de configuration pour des commutateurs Catalyst exécutant le logiciel Cisco IOS® ou

CatOS ont une section appelée Configuration de la sécurité de port ou Configuration du contrôle de trafic de port. Référez-vous à la documentation technique pour votre commutateur dans les pages de produit Commutateurs Cisco pour plus d'informations.

**Remarque :** Si une inondation monodiffusion se produit dans un port de commutateur configuré pour la sécurité des ports avec la condition « Restrict » pour arrêter l'inondation, une violation de sécurité est déclenchée.

```
Router(config-if)#switchport port-security violation restrict
```

**Remarque :** Lorsqu'une telle violation de sécurité se produit, les ports affectés configurés pour le mode « restriction » doivent abandonner les paquets avec des adresses source inconnues jusqu'à ce que vous supprimiez un nombre suffisant d'adresses MAC sécurisées pour descendre en dessous de la valeur maximale. Ceci entraîne une incrémentation du compteur SecurityViolation.

**Remarque :** au lieu de ce comportement, si le port du commutateur passe à l'état Arrêt, vous devez configurer `Router(config-if)#switchport block unicast de` sorte que le port du commutateur particulier soit désactivé pour la diffusion monodiffusion.

# Comment détecter une propagation excessive

La plupart des commutateurs ne mettent en application aucune commande spéciale pour détecter la propagation. Les commutateurs de la gamme Catalyst 6500/6000 Supervisor Engine 2 et versions ultérieures qui exécutent le logiciel système Cisco IOS (natif) versions 12.1(14)E et ultérieures ou le logiciel système Cisco CatOS versions 7.5 ou ultérieures implémentent la fonctionnalité de **protection contre les attaques par propagation monodiffusion**. En bref, cette fonctionnalité permet au commutateur de contrôler la quantité de propagation monodiffusion par VLAN et d'agir en conséquence si la propagation dépasse la quantité spécifiée. Les actions peuvent être Syslog, une limite ou un arrêt de VLAN, Syslog étant la plus utile pour la détection de la propagation. Quand la propagation dépasse le débit configuré et l'action configurée est Syslog, un message semblable au suivant sera imprimé :

```
%UNICAST_FLOOD-4-DETECTED: Host 0000.0000.2100 on vlan 1 is flooding
to an unknown unicast destination at a rate greater than/equal to 1 Kfps
```

L'adresse MAC indiquée est l'adresse MAC d'origine à partir de laquelle les paquets sont propagés sur ce commutateur. Il est souvent nécessaire de connaître les adresses MAC de destination vers lesquelles le commutateur se propage (parce que le commutateur transfère en regardant l'adresse MAC de destination). Les versions Cisco IOS (natif) 12.1(20)E pour Catalyst 6500/6000 Supervisor Engine 2 et ultérieures implémenteront la capacité d'afficher les adresses MAC vers lesquelles la propagation se produit :

```
cat6000#sh mac-address-table unicast-flood
Unicast Flood Protection status: enabled

Configuration:
 vlan      Kfps         action       timeout
------+----------+----------------+----------
   55          1             alert      none

Mac filters:
 No.    vlan    souce mac addr.           installed on           time left (mm:ss)
```

```
-----+------+-----------------+-----------------------------+-----------------

Flood details:
 Vlan    souce mac addr.              destination mac addr.
------+---------------+-------------------------------------------------
   55    0000.2222.0000    0000.1111.0029, 0000.1111.0040, 0000.1111.0063
                           0000.1111.0018, 0000.1111.0090, 0000.1111.0046
                           0000.1111.006d
```

Des recherches plus étendues peuvent alors être effectuées pour voir si l'adresse MAC 0000.2222.0000 est censée envoyer du trafic aux adresses MAC énumérées dans la section des adresses MAC de destination. Si le trafic est légitime, il convient d'établir pourquoi les adresses MAC de destination sont inconnues du commutateur.

Vous pouvez détecter si la propagation se produit en capturant une trace de paquets vus sur une station de travail pendant un ralentissement ou une panne. Normalement, des paquets monodiffusion n'impliquant pas la station de travail ne devraient pas être vus à plusieurs reprises sur le port. Si ceci se produit, il est possible qu'une propagation se produise. Les traces de paquets peuvent sembler différentes quand il y a diverses causes de propagation.

Avec le routage asymétrique, il est probable que des paquets vers une adresse MAC spécifique n'arrêteront pas la propagation même après que la destination répond. Avec les notifications TCN, la propagation inclura beaucoup d'adresses différentes, mais finira par s'arrêter, puis redémarrer.

Avec le dépassement de la capacité de la table de transfert L2, vous êtes susceptible de voir le même genre de propagation qu'avec un routage asymétrique. La différence est qu'il y aura vraisemblablement beaucoup d'étranges paquets, ou des paquets normaux en quantités anormales avec une adresse MAC source différente.

## Informations connexes

- Support pour commutateurs
- Prise en charge de la technologie de commutation LAN
- Support technique - Cisco Systems