# Dépannage du protocole ARP (Address Resolution Protocol) du Nexus 7000 sans capture intrabande

## Contenu



## Introduction

Ce document décrit comment dépanner la tempête ARP, sans trafic ARP intrabande.

## Fond

La tempête ARP est une attaque par déni de service (DoS) courante que vous verriez dans l'environnement du data center.

La logique de commutateur la plus courante pour gérer les paquets ARP est la suivante :

- Paquet ARP avec adresse MAC (Media Access Control) de destination de diffusion
- Paquet ARP avec adresse MAC de destination unicast, qui appartient au commutateur

sera traité par le processus ARP dans le logiciel si l'interface virtuelle de commutateur (SVI) est active dans le VLAN de réception.

Par cette logique, s'il y a un ou plusieurs hôtes malveillants continuent à envoyer une requête ARP dans un VLAN, où un commutateur est la passerelle de ce VLAN. La requête ARP sera traitée dans le logiciel, de sorte que le commutateur sera submergé. Dans une version et un modèle de commutateur Cisco plus anciens, vous verrez que le processus ARP augmente l'utilisation du CPU et que le système est trop occupé pour gérer le trafic d'autres plans de contrôle.La façon la plus courante de suivre une telle attaque est d'exécuter la capture intrabande pour identifier l'adresse MAC source de la tempête ARP.

Dans le data center où Nexus 7000 agit comme passerelle d'agrégation, cet impact est réduit par CoPP sur les commutateurs de la gamme Nexus 7000. Vous pouvez toujours exécuter Ethanalyzer de capture intrabande sur le Guide de dépannage Nexus 7000 pour identifier l'adresse MAC source de la tempête ARP, car Control Plane Policing (CoPP) est simplement un bandit qui ralentit mais ne supprime pas la tempête ARP qui se précipite sur le processeur.

Que diriez-vous de ce scénario où :

- SVI désactivé
- Aucun paquet ARP excessif n'est transmis au processeur
- Pas de CPU élevé en raison du processus ARP

Cependant, le commutateur continue de voir un problème lié au protocole ARP, par exemple, l'hôte connecté direct a un protocole ARP incomplet. Est-il peut-être causé par une tempête ARP ?

La réponse est oui sur Nexus 7000.

## Cause première

Dans la conception de la carte de ligne Nexus 7000, pour prendre en charge le processus de paquets ARP dans CoPP, la requête ARP conduira une interface logique spéciale (LIF), puis sera limitée par CoPP dans le moteur de transfert (FE). Cela se produit peu importe que vous ayez une interface SVI activée pour le VLAN ou non.

Par conséquent, alors que la décision finale de transfert prise par FE est de ne pas envoyer la requête ARP au CPU intrabande (dans le cas où aucune SVI n'est activée pour le VLAN), le compteur CoPP est toujours mis à jour. Il entraîne une saturation de CoPP avec une requête ARP excessive et la suppression de la requête/réponse ARP légitime. Dans ce scénario, vous ne verrez aucun paquet ARP intrabande excessif, mais toujours affecté par la tempête ARP.

Nous avons un bogue amélioré CSCub47533 classé pour ce comportement de premier jour CoPP.

## Solution

Dans ce scénario, il peut y avoir quelques options pour identifier la source de la tempête ARP. Une option efficace est la suivante :

- Identifiez d'abord le module d'où provient la tempête ARP.

```
N7K# sh policy-map interface control-plane class copp-system-p-class-normal
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match exception ip multicast directly-connected-sources
match exception ipv6 multicast directly-connected-sources
match protocol arp
set cos 1
police cir 680 kbps bc 250 ms
conform action: transmit
violate action: drop
 module 3:
conformed 4820928 bytes,
5-min offered rate 0 bytes/sec
peak rate 104 bytes/sec at Thu Aug 25 08:12:12 2016
 violated 9730978848 bytes,
       5-min violate rate 6983650 bytes/sec
       peak rate 7632238 bytes/sec at Thu Aug 25 00:43:33 2016
module 4:
conformed 4379136 bytes,
5-min offered rate 0 bytes/sec
peak rate 38 bytes/sec at Wed Aug 24 07:12:09 2016
violated 0 bytes,
```

```
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
...
```

- Utilisez ensuite la procédure ELAM pour capturer tous les paquets ARP qui touchent le module. Il se peut que vous ayez besoin de le faire plusieurs fois. Mais s'il y a une tempête en cours, la probabilité que vous capturiez le paquet ARP violent est bien meilleure que le paquet ARP légitime. Identifiez les adresses MAC et Vlan source à partir de la capture ELAM.