Le Nexus 7000 dépannent la tempête de Protocole ARP (Address Resolution Protocol) sans capture intrabande

Contenu

Introduction

Ce document décrit comment dépanner la tempête d'ARP, sans n'importe quel trafic ARP intrabande.

Fond

La tempête d'ARP est une attaque commune du déni de service (DOS) que vous verriez dans l'environnement de centre de traitement des données.

La logique commune de commutateur pour manipuler le paquet d'ARP est celle :

- Paquet d'ARP avec le Contrôle d'accès au support (MAC) de destination d'émission
- Paquet d'ARP avec le MAC de destination d'unicast, qui appartient au commutateur

sera traité par le processus d'ARP en logiciel si Switch Virtual Interface (SVI) est dans le VLAN de réception.

Par cette logique, s'il y a un ou plusieurs hôtes malicous maintiennent envoyer la demande d'ARP dans un VLAN, où un commutateur est la passerelle de ce VLAN. La demande d'ARP sera traitée en logiciel par conséquent entraîne le commutateur étant accablé. Dans un certains modèle de commutateur et version plus anciens de Cisco, vous verrez que le processus d'ARP prend l'utilisation du CPU jusqu'au haut niveau et le système est trop occupé pour traiter l'autre trafic d'avion de contrôle. La manière courante de tracer une telle attaque est d'exécuter la capture intrabande pour identifier le MAC de source de la tempête d'ARP.

Au centre de calculs où le Nexus 7000 agit en tant que passerelle d'agrégation, une telle incidence est réduite par CoPP sur des Commutateurs de gamme de Nexus 7000. Vous pourriez encore exécuter la capture intrabande Ethanalyzer du guide de dépannage de Nexus 7000 pour identifier le MAC de source de la tempête d'ARP puisque la Réglementation du plan de commande (CoPP) est juste un bandit ralentissant mais pas elminating la tempête d'ARP se précipitant à la CPU.

Que diriez-vous de ce scénario où :

- Le SVI est vers le bas

- Aucun paquet excessif d'ARP étant coup de volée à la CPU
- Aucune CPU de haute due au processus d'ARP

Le commutateur cependant voient toujours le problème associé par ARP, par exemple l'hôte connecté direct a l'ARP inachevé. Est-il probablement provoqué par la tempête d'ARP ?

La réponse est oui sur le Nexus 7000.

Cause principale

Dans la conception de linecard du Nexus 7000, pour prendre en charge le processus de paquet d'ARP dans CoPP, la demande d'ARP pilotera une interface logique spéciale (LIF) soit alors débit limité par CoPP dans l'engine d'expédition (technicien). Ceci se produit aucune matière que vous avez un SVI pour le VLAN ou pas.

Par conséquent, alors que la décision de transmission finale prise par le technicien est de ne pas envoyer la demande d'ARP à la CPU intrabande (dans l'affaire no. SVI pour le VLAN), le compteur de CoPP est encore mis à jour. Il mène à CoPP a saturé avec la demande excessive d'ARP et la demande d'ARP/réponse légitimes chutantes. Dans ce scénario, vous ne verrez aucun paquet intrabande excessif d'ARP mais étant affecté toujours par la tempête d'ARP.

Nous avons une bogue améliorée CSCub47533 classés pour ce comportement du jour un de CoPP.

Solution

Il a pu y avoir quelques options d'identifier la source de tempête d'ARP dans ce scénario. Une option efficace est :

- L'identifiez d'abord que le module la tempête d'ARP provient

```
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
...
```

- Employez en second lieu la procédure ELAM pour capturer tout le paquet d'ARP frappant le module. Vous pourriez devoir le faire plusieurs fois. Mais s'il y a une tempête allant en fonction, l'occasion que vous capturez le paquet d'ARP de violer est bien mieux que le paquet d'ARP de legetimate. Identifiez le MAC et le VLAN de source de la capture ELAM.