Solución de problemas de saturación del protocolo de resolución de direcciones (ARP) de Nexus 7000 sin captura dentro de la banda

Contenido

Introducción

Este documento describe cómo resolver el problema de la tormenta ARP, sin tráfico ARP dentro de la banda.

Background

La tormenta ARP es un ataque de denegación de servicio (DoS) común que se vería en el entorno del Data Center.

La lógica común del switch para manejar el paquete ARP es que:

- Paquete ARP con control de acceso a medios (MAC) de destino de difusión
- Paquete ARP con MAC de destino de unidifusión, que pertenece al switch

será procesada por el proceso ARP en el software si la interfaz virtual del switch (SVI) está activa en la VLAN receptora.

Según esta lógica, si hay uno o más hosts malintencionados siguen enviando la solicitud ARP en una VLAN, donde un switch es el gateway de esa VLAN. La solicitud ARP se procesará en el software, por lo tanto, el switch se verá saturado. En algunas versiones y modelos de switch de Cisco anteriores, verá que el proceso ARP lleva el uso de la CPU a un nivel alto y el sistema está demasiado ocupado para manejar otro tráfico del plano de control. La manera común de rastrear tal ataque es ejecutar la captura dentro de la banda para identificar la MAC de origen de la tormenta ARP.

En el Data Center en el que Nexus 7000 actúa como gateway de agregación, este impacto se reduce mediante CoPP en los switches Nexus serie 7000. Aún podría ejecutar Ethanalyzer de captura dentro de la banda en la guía de solución de problemas de Nexus 7000 para identificar el MAC de origen de la tormenta ARP, ya que Control Plane Policing (CoPP) es sólo un bandolero que se ralentiza pero no elimina la tormenta ARP que se apresura hacia la CPU.

¿Qué hay de este escenario en el que:

- SVI está inactivo
- No se envía un paquete ARP excesivo a la CPU

- No hay CPU alta debido al proceso ARP

Sin embargo, el switch aún ve el problema relacionado con ARP, por ejemplo, el host conectado directamente tiene ARP incompleto. ¿Es posible que se deba a una tormenta ARP?

La respuesta es sí en Nexus 7000.

Causa raíz

En el diseño de la tarjeta de línea Nexus 7000, para admitir el proceso de paquetes ARP en CoPP, la solicitud ARP impulsará una interfaz lógica especial (LIF) y, a continuación, la velocidad será limitada por CoPP en el motor de reenvío (FE). Esto sucede independientemente de que tenga una SVI para la Vlan o no.

Por lo tanto, mientras que la decisión de reenvío final tomada por FE es no enviar la solicitud ARP a la CPU dentro de la banda (en el caso de que no haya SVI para la vlan), el contador CoPP todavía se actualiza. Esto lleva a CoPP saturado con una solicitud ARP excesiva y a descartar una solicitud/respuesta ARP legítima. En esta situación, no verá ningún paquete ARP dentro de banda excesivo, pero aún se verá afectado por la tormenta ARP.

Tenemos un error mejorado CSCub47533 registrado para este comportamiento del primer día de CoPP.

Solución

Podría haber algunas opciones para identificar el origen de la tormenta ARP en este escenario. Una opción eficaz es:

- Primero, identifique de qué módulo proviene la tormenta 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
...
```

- Segundo, use ELAM Process para capturar todo el paquete ARP que golpea el módulo. Es posible que deba hacerlo varias veces. Pero si hay una tormenta en curso, la posibilidad de capturar el paquete ARP violado es mucho mejor que el paquete ARP legítimo. Identifique la MAC de origen y la Vlan de la captura ELAM.