Tormenta del Address Resolution Protocol (ARP) del Troubleshooting del nexo 7000 sin la captura Inband

Contenido

Introducción

Este documento describe cómo resolver problemas la tormenta ARP, sin ningún tráfico ARP inband.

Antecedente

La tormenta ARP es un ataque de Negación de servicio (DoS) común que usted vería en el entorno del centro de datos.

La lógica común del Switch para manejar el paquete ARP es ésa:

- Paquete ARP con el Destination Media Access Control del broadcast (MAC)
- Paquete ARP con el MAC de destino del unicast, que pertenece al Switch

será procesado por el proceso ARP en el software si la interfaz virtual del Switch (SVI) está para arriba en el Vlan de recepción.

Por esta lógica, si hay uno o más host malicous mantienen el enviar del pedido ARP un Vlan, donde está el gateway un Switch de ese Vlan. El pedido ARP será procesado en el software por lo tanto causa el Switch que es abrumado. En cierto más viejos modelo y versión del switch Cisco, usted verá que el proceso ARP toma el USO de la CPU hasta el nivel elevado y el sistema está demasiado ocupado manejar el otro tráfico del plano del control. La manera común de localizar tal ataque es ejecutar la captura inband para identificar el MAC de origen de la tormenta ARP.

En el centro de datos en donde el nexo 7000 está actuando como el gateway de la agregación, tal impacto es reducido por CoPP en los 7000 Series Switch del nexo. Usted podría todavía ejecutar la captura inband Ethanalyzer en el guía de Troubleshooting del nexo 7000 para identificar el MAC de origen de la tormenta ARP puesto que las Políticas del plano de control (CoPP) son apenas bandido que retrasa pero elminating la tormenta ARP que acomete al CPU.

Cómo sobre este escenario donde:

- El SVI está abajo
- Ningún paquete ARP excesivo que es batea al CPU

- Ningún CPU elevada debido al proceso ARP

El Switch sin embargo todavía considera el problema relacionado ARP, e.g el host conectado directo tiene ARP incompleto. ¿Es causado posiblemente por la tormenta ARP?

La respuesta está sí en el nexo 7000.

Causa raíz

En el diseño del linecard del nexo 7000, soportar el proceso del paquete ARP en CoPP, el pedido ARP conducirá una interfaz lógica especial (LIF) entonces sea tarifa limitada por CoPP en motor de reenvío (FE). Esto sucede ninguna materia que usted tiene un SVI para arriba para el Vlan o no.

Por lo tanto, mientras que la decisión de reenvío final tomada por el FE es no enviar el pedido ARP al CPU inband (en el caso ningún SVI para arriba para el vlan), el contador de CoPP todavía se pone al día. Lleva a CoPP saturó con el pedido ARP excesivo y el pedido ARP/la contestación legítimos de caída. En este escenario, usted no verá ninguna paquetes ARP inband excesiva pero todavía siendo afectado por la tormenta ARP.

Tenemos un bug aumentado CSCub47533 clasifiados para este comportamiento del día uno de CoPP.

Solución

Podía haber algunas opciones para identificar la fuente de tormenta ARP en este escenario. Una opción eficaz es:

- Primero identifique de que el módulo la tormenta ARP viene

```
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
...
```

- Utilice en segundo lugar el procedimiento ELAM para capturar todo el paquete ARP que golpea el módulo. Usted puede ser que necesite hacerlo varias veces. Pero si hay una tormenta que continúa, la ocasión que usted captura el paquete ARP de la violación es mucho mejor que el paquete ARP del legetimate. Identifique el MAC de origen y el Vlan de la captura ELAM.