Nexus 7000: risoluzione dei problemi relativi alla tempesta ARP (Address Resolution Protocol) senza acquisizione in banda

Sommario

Introduzione

Questo documento descrive come risolvere i problemi relativi alla tempesta ARP, senza traffico ARP in banda.

Sfondo

La tempesta ARP è un attacco DoS (Denial-of-Service) comune che si verifica nell'ambiente del centro dati.

La logica dello switch comune per gestire i pacchetti ARP è che:

- Pacchetto ARP con MAC (Media Access Control) di destinazione di trasmissione
- Pacchetto ARP con MAC di destinazione unicast, che appartiene allo switch

verranno elaborati dal processo ARP nel software se l'interfaccia virtuale dello switch (SVI) è attiva nella VLAN ricevente.

In base a questa logica, se sono presenti uno o più host dannosi, continuare a inviare la richiesta ARP in una VLAN, dove uno switch è il gateway di tale VLAN. La richiesta ARP verrà elaborata nel software, quindi lo switch risulterà sovraccarico. In alcune versioni e modelli di switch Cisco meno recenti, si osserverà che il processo ARP porta l'utilizzo della CPU a livelli elevati e che il sistema è troppo occupato per gestire il traffico di altri control plane. Il modo comune per tracciare tale attacco è eseguire l'acquisizione in banda per identificare l'indirizzo MAC di origine della tempesta ARP.

Nel centro dati in cui Nexus 7000 opera come gateway di aggregazione, tale impatto è ridotto dal CoPP sugli switch Nexus serie 7000. È comunque possibile eseguire Ethanalyzer di acquisizione in banda su Nexus 7000 Troubleshooting Guide (Guida alla risoluzione dei problemi) per identificare l'indirizzo MAC di origine della tempesta ARP, poiché Control Plane Policing (CoPP) è solo un bandit che rallenta ma non elimina la tempesta ARP che precipita sulla CPU.

Informazioni su questo scenario in cui:

- SVI non attivo
- Nessun pacchetto ARP eccessivo reindirizzato alla CPU

- Nessuna CPU elevata a causa del processo ARP

Lo switch continua tuttavia a rilevare un problema relativo all'ARP, ad esempio un host con connessione diretta non ha un ARP completo. È forse causata dalla tempesta ARP?

La risposta è sì su Nexus 7000.

Causa principale

Nel progetto nexus 7000 linecard, per supportare il processo di pacchetti ARP in CoPP, la richiesta ARP guiderà una speciale interfaccia logica (LIF) quindi sarà limitata dalla velocità del CoPP nel motore di inoltro (FE). Ciò accade indipendentemente dal fatto che la VLAN sia o meno collegata a una SVI.

Pertanto, mentre la decisione finale di inoltro presa da FE è di non inviare la richiesta ARP alla CPU in banda (nel caso non vi siano SVI attive per la vlan), il contatore CoPP è ancora aggiornato. Ciò porta il CoPP a diventare saturo di richieste ARP eccessive e a rinunciare a richieste/risposte ARP legittime. In questo scenario, non verranno visualizzati pacchetti ARP in banda in eccesso, ma il pacchetto sarà ancora interessato da una tempesta ARP.

Per questo comportamento del giorno 1 del CoPP, è stato archiviato un bug migliorato CSCub47533.

Soluzione

Ci potrebbero essere alcune opzioni per identificare la fonte della tempesta ARP in questo scenario. Un'opzione efficace è:

- Identificare innanzitutto da quale modulo proviene la tempesta 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
...
```

- Quindi, usare ELAM Procedure per acquisire tutto il pacchetto ARP che colpisce il modulo. Potrebbe essere necessario farlo diverse volte. Ma se c'è una tempesta, la possibilità di catturare il pacchetto ARP violato è molto meglio di un pacchetto ARP legittimo. Identificare l'indirizzo MAC e la VLAN di origine dall'acquisizione ELAM.