# Solução de problemas de tempestade de protocolo de resolução de endereços (ARP) do Nexus 7000 sem captura de banda

## Contents



## Introduction

Este documento descreve como solucionar problemas da tempestade ARP, sem qualquer tráfego ARP inband.

## Background

A tempestade ARP é um ataque comum de negação de serviço (DoS) que você veria no ambiente do data center.

A lógica comum do switch para lidar com o pacote ARP é que:

- Pacote ARP com Media Access Control (MAC) de destino de broadcast
- Pacote ARP com MAC de destino unicast, que pertence ao switch

será processado pelo processo ARP no software se a Interface Virtual do Switch (SVI) estiver ativa na VLAN receptora.

Por essa lógica, se houver um ou mais hosts maliciosos enviando uma solicitação ARP em uma Vlan, onde um switch é o gateway dessa Vlan. A solicitação ARP será processada no software, o que faz com que o switch seja sobrecarregado. Em algum modelo e versão mais antigos do switch Cisco, você verá que o processo ARP leva o uso da CPU para um nível mais alto e o sistema está muito ocupado para lidar com outro tráfego do plano de controle.A maneira comum de rastrear esse ataque é executar a captura inband para identificar o MAC de origem da tempestade ARP.

No data center em que o Nexus 7000 atua como o gateway de agregação, esse impacto é reduzido pelo CoPP nos switches Nexus 7000 Series. Você ainda pode executar a captura Ethanalyzer no Nexus 7000 Troubleshooting Guide para identificar o MAC de origem da tempestade ARP, já que o Control Plane Policing (CoPP) é apenas um bandido abrandando, mas não eliminando a tempestade ARP correndo para a CPU.

Que tal este cenário em que:

- A SVI está inativa
- Nenhum pacote ARP excessivo é direcionado à CPU

- Nenhuma CPU alta devido ao processo ARP

No entanto, o switch ainda vê problemas relacionados ao ARP, por exemplo, o host conectado diretamente tem um ARP incompleto. Isso é possivelmente causado pela tempestade ARP?

A resposta é sim no Nexus 7000.

# Causa raiz

No design da placa de linha do nexus 7000, para suportar o processo de pacote ARP em CoPP, a solicitação ARP conduzirá uma interface lógica especial (LIF) e, em seguida, terá uma taxa limitada pelo CoPP no mecanismo de encaminhamento (FE). Isso acontece independentemente de você ter um SVI ativado para a Vlan ou não.

Assim, embora a decisão final de encaminhamento tomada pelo FE seja não enviar a solicitação ARP para a CPU dentro da banda (no caso de nenhuma SVI ativada para a vlan), o contador do CoPP ainda é atualizado. Isso leva ao CoPP saturado com solicitação ARP excessiva e descartando a solicitação/resposta ARP legítima. Nesse cenário, você não verá nenhum pacote ARP em banda excessiva, mas ainda será afetado pela tempestade ARP.

Temos um bug avançado CSCub47533 arquivado para este comportamento de primeiro dia do CoPP.

# Solução

Pode haver algumas opções para identificar a origem da tempestade ARP neste cenário. Uma opção eficaz é:

- Primeiro identificar de qual módulo a tempestade ARP vem

```
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 o Procedimento ELAM para capturar todo o pacote ARP que atinge o módulo. Você pode precisar fazer isso várias vezes. Mas se houver uma tempestade acontecendo, a chance de capturar o pacote ARP violado é muito melhor do que o pacote ARP legítimo. Identificar o MAC e a VLAN origem da captura ELAM.