

Um pacote ARP tem impacto em sessões de BFD na plataforma Nexus 7000?

Contents

[Introduction](#)

[P. Como o Cisco NX-OS pode distribuir a operação de BFD para módulos compatíveis que suportam BFD, uma tempestade de pacotes ARP teria algum impacto nas sessões de BFD na plataforma Nexus 7000?](#)

[Detalhes da configuração do laboratório](#)

[A tempestade ARP começa](#)

[A tempestade ARP começa a impactar o plano de controle](#)

[O que acontece quando um ARP Packet Storm para?](#)

[Conclusão](#)

Introduction

Este documento descreve um impacto de Tempestade de Pacotes ARP em protocolos de plano de controle, como BFD, OSPF e outros, executados em switches Nexus 7000.

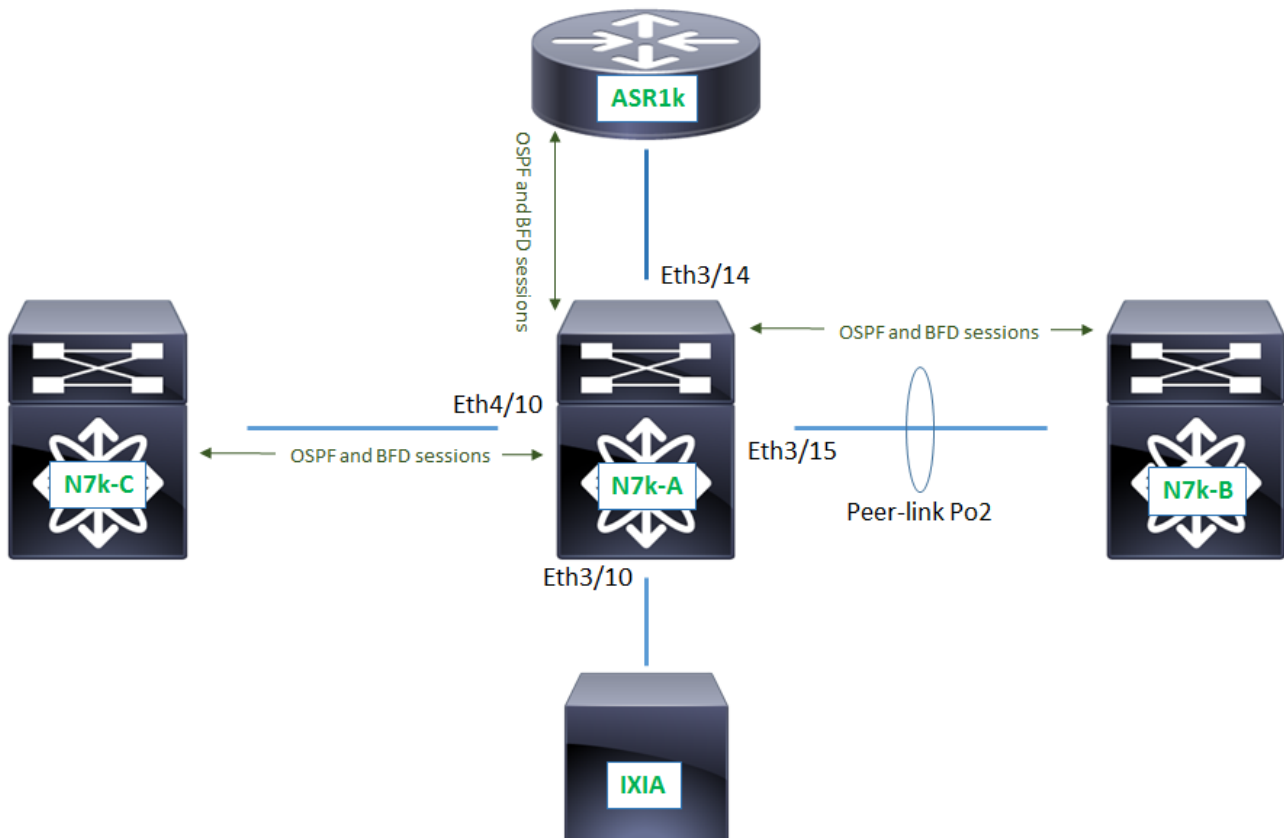
Contribuído por Nishad Mohiuddin, Nikolay Kartashev, Engenheiros do TAC da Cisco.

P. Como o Cisco NX-OS pode distribuir a operação de BFD para módulos compatíveis que suportam BFD, uma tempestade de pacotes ARP teria algum impacto nas sessões de BFD na plataforma Nexus 7000?

A. Em geral, uma tempestade de pacotes ARP pode ter um impacto negativo na estabilidade das sessões BFD em execução no switch Nexus 7000. Os sintomas exatos dependem da solidão e magnitude do evento ARP Packet Storm. Abaixo estão os resultados dos testes da rede do laboratório Cisco TAC.

Detalhes da configuração do laboratório

A configuração do laboratório a seguir foi criada para testar o impacto de quantidades de tráfego ARP atingindo a CPU do switch Nexus 7000.



Aqui, N7k-A é usado como dispositivo em teste (DUT). O DUT é um switch Nexus 7009 com a seguinte configuração de hardware

```
N7k-A# show module
Mod Ports Module-Type Model Status
-----
1 0 Supervisor module-1X N7K-SUP1 active *
2 0 Supervisor module-1X N7K-SUP1 ha-standby
3 32 10 Gbps Ethernet Module N7K-M132XP-12 ok
4 32 10 Gbps Ethernet Module N7K-M132XP-12 ok
N7k-A#
```

N7k-A tem os seguintes dispositivos conectados a ele

- N7k-B é um peer VPC, conectado à interface Ethernet 3/15
- ASR1k é um vizinho da Camada 3, conectado à interface Ethernet 3/14
- N7k-C é um vizinho da Camada 3, conectado à interface Ethernet 4/10
- O gerador de tráfego IXIA está na vlan 6, conectada à interface Ethernet 3/10, que está configurada como porta de acesso da camada 2

O DUT tem três sessões de BFD, uma na placa de linha no slot 4 para N7k-C e duas na placa de linha no slot 3 para N7k-B e ASR1k

```
N7k-A# show bfd neighbors

OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
10.80.6.173 10.80.6.174 1090519061/4105 Up 4951(3) Up Eth3/14

10.80.1.162 10.80.1.161 1090519054/1090519044 Up 4203(3) Up Eth4/10

10.80.1.61 10.80.1.62 1090519060/1090519059 Up 5921(3) Up Vlan6
```

N7k-A#

O DUT também tem três sessões OSPF, uma no cartão de linha no slot 4 para N7k-C e duas no cartão de linha no slot 3, para N7k-B e ASR1k.

N7k-A# **show ip ospf neighbors**

```
OSPF Process ID 1
Total number of neighbors: 3
Neighbor ID Pri State Up Time Address Interface
10.80.0.2 1 FULL/ - 00:13:26 10.80.1.62 Vlan6
10.80.4.25 1 FULL/DR 00:12:40 10.80.6.174 Eth3/14
10.80.0.3 1 FULL/DR 20:15:07 10.80.1.161 Eth4/10
N7k-A#
```

OSPF registrado com BFD

```
router ospf 1
bfd
router-id 10.80.0.1
```

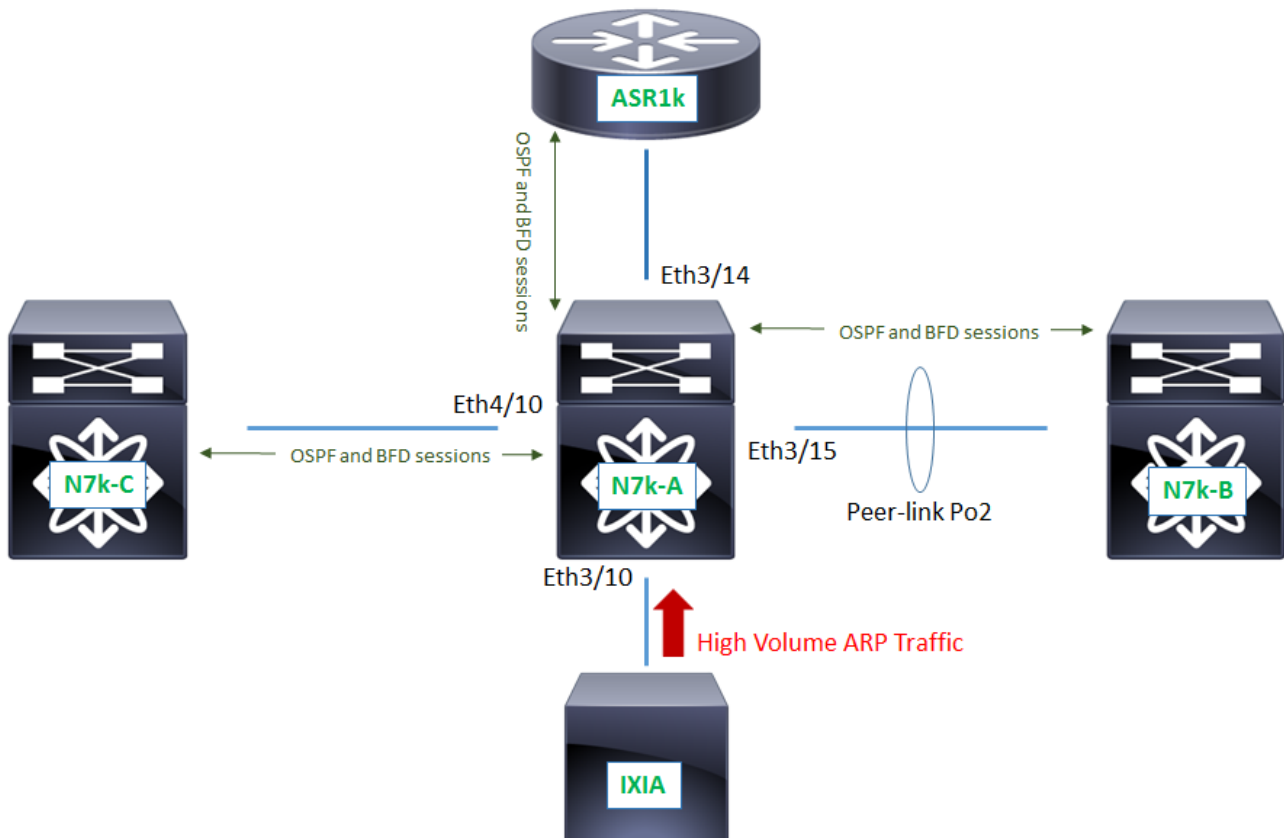
Além disso, a tabela ARP em N7k-A tem entradas para todos os três vizinhos BFD/OSPF

N7k-A# **show ip arp**

```
Address Age MAC Address Interface
10.80.1.62 00:13:30 4055.390f.48c1 Vlan6
10.80.6.174 00:12:46 88f0.774b.0700 Ethernet3/14
10.80.1.161 00:15:13 6c9c.ed44.6841 Ethernet4/10
N7k-A#
```

A tempestade ARP começa

O Gerador de Tráfego IXIA é usado para simular parte instável da rede, o que resulta em um alto volume de tráfego ARP enviado ao DUT, como pode ser visto no diagrama abaixo



A saída a seguir mostra um aumento do tráfego de entrada na interface Ethernet 3/10, onde o Gerador de Tráfego IXIA está conectado. Esses são pacotes ARP de broadcast recebidos na vlan 6

```
N7k-A# show interface Ethernet3/10 | grep "30 seconds input rate"
30 seconds input rate 3102999976 bits/sec, 6062053 packets/sec
N7k-A#
```

Como uma cópia de cada pacote ARP de broadcast é enviada à CPU em N7k-A neste cenário, vemos um aumento de bytes violados no módulo 3 em CoPP

```
N7k-A# show 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 protocol arp
set cos 1
police cir 680 kbps , bc 250 ms
module 3 :
conformed 2295040 bytes; action: transmit
violated 20569190016 bytes; action: drop

module 4 :
conformed 128 bytes; action: transmit
violated 0 bytes; action: drop

N7k-A#
```

Note: Observe que *não há bytes violados no módulo no slot 4*, já que a origem da tempestade ARP de broadcast está conectada apenas à interface no módulo 3

No ponto em que a tempestade ARP começa, as saídas acima são geralmente os primeiros (e únicos) sinais que indicam um problema na rede. Na maioria dos casos, esses sinais passam despercebidos ou são ignorados pelos operadores de rede e avançam rapidamente para uma situação que leva a grandes problemas de conectividade.

A tempestade ARP começa a impactar o plano de controle

Por padrão, o valor de tempo limite ARP na plataforma Nexus 7000 é configurado para 25 minutos ou 1500 segundos. O switch Nexus precisa atualizar periodicamente as entradas do cache ARP local para manter atualizada a resolução IP para MAC de seus vizinhos de camada 3 do próximo salto.

A saída a seguir é a saída da tabela de cache ARP no DUT após as entradas de cache ARP expirarem.

```
N7k-A# show ip arp
```

```
Address Age MAC Address Interface
10.80.1.62 00:00:06 INCOMPLETE Vlan6
10.80.6.174 00:00:10 INCOMPLETE Ethernet3/14
10.80.1.161 00:12:59 6c9c.ed44.6841 Ethernet4/10
N7k-A#
```

Observe que as entradas de cache ARP para dispositivos conectados à placa de linha no slot 3 mostram o status **INCOMPLETE**, enquanto a entrada para o switch N7k-C, que está conectado à placa de linha no slot 4, está sendo atualizada com êxito conforme esperado.

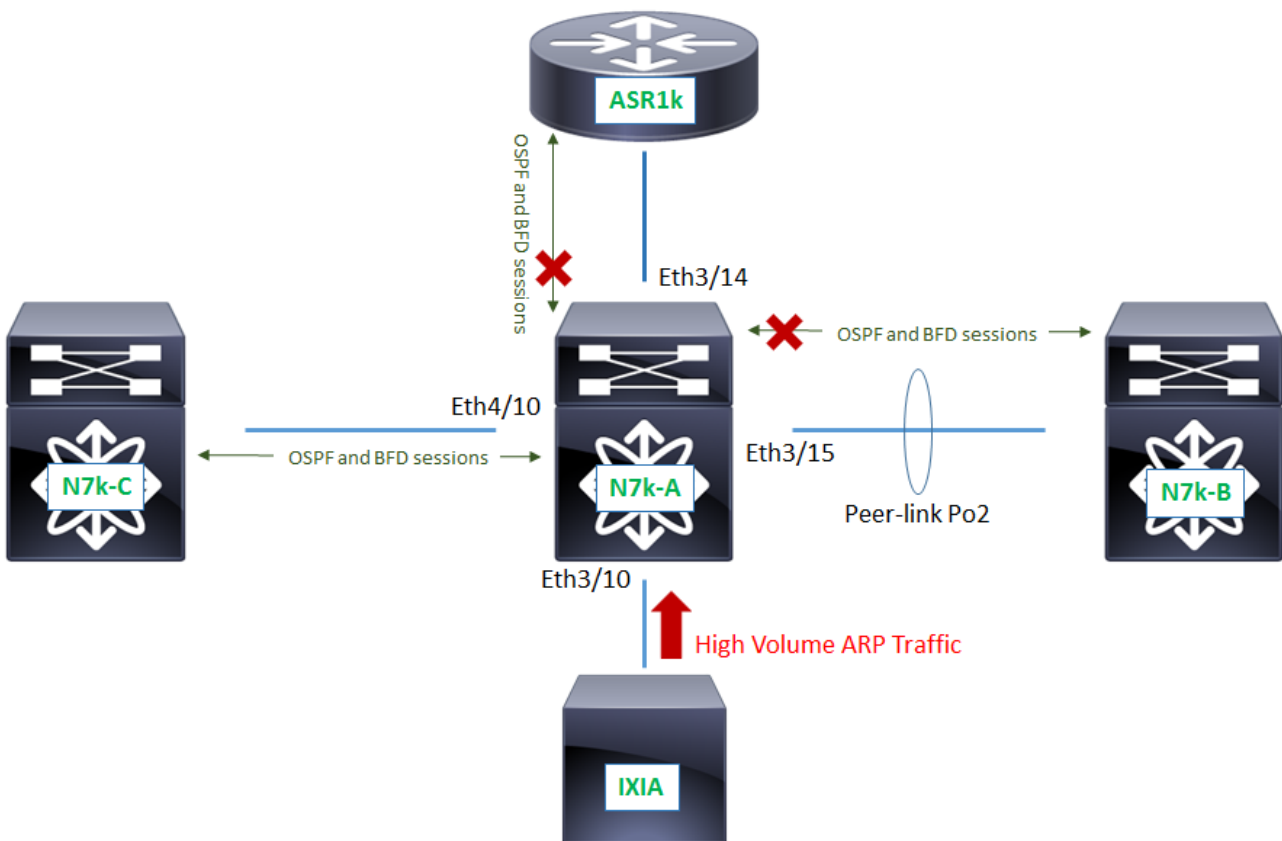
As seguintes mensagens de registro DUT indicam o impacto no nível do plano de controle

```
N7k-A# show logging log
```

```
...
2016 Nov 16 22:12:55 N7k-A %BFD-5-SESSION_STATE_DOWN: BFD session 1090519060 to neighbor
10.80.1.62 on interface Vlan6 has gone down. Reason: 0x3.
2016 Nov 16 22:12:55 N7k-A %OSPF-5-ADJCHANGE: ospf-1 [10600] Nbr 10.80.1.62 on Vlan6 went DOWN
2016 Nov 16 22:12:55 N7k-A %BFD-5-SESSION_REMOVED: BFD session to neighbor 10.80.1.62 on
interface Vlan6 has been removed
2016 Nov 16 22:12:56 N7k-A %OSPF-5-ADJCHANGE: ospf-1 [10600] Nbr 10.80.1.62 on Vlan6 went
EXSTART
2016 Nov 16 22:13:40 N7k-A %OSPF-5-ADJCHANGE: ospf-1 [10600] Nbr 10.80.6.174 on Ethernet3/14
went DOWN
2016 Nov 16 22:13:40 N7k-A %BFD-5-SESSION_STATE_DOWN: BFD session 1090519061 to neighbor
10.80.6.174 on interface Eth3/14 has gone down. Reason: 0x3.
2016 Nov 16 22:13:40 N7k-A %OSPF-5-ADJCHANGE: ospf-1 [10600] Nbr 10.80.6.174 on Ethernet3/14
went EXSTART
2016 Nov 16 22:13:46 N7k-A %BFD-5-SESSION_REMOVED: BFD session to neighbor 10.80.6.174 on
interface Eth3/14 has been removed
2016 Nov 16 22:15:45 N7k-A %OSPF-5-ADJCHANGE: ospf-1 [10600] Nbr 10.80.6.174 on Ethernet3/14
went INIT
...
N7k-A#
```

Observe nesta saída que o OSPF alterna entre o estado DOWN e EXSTART e, em seguida, de volta para o estado INIT. Isso ocorre porque o OSPF usa unicast para trocar prefixos durante o estado EXSTART. Como a resolução ARP está incompleta no módulo no slot 3 no momento da tempestade de pacotes ARP, a troca de rotas nunca é concluída, resultando na não formação da adjacência OSPF.

Nota: A resolução ARP para IP para MAC do próximo salto depende do unicast como a operação BFD. Dado que podemos concluir que o BFD exige que o ARP seja resolvido para uma operação adequada.



As seguintes saídas confirmam o impacto de uma tempestade de pacotes ARP em sessões BFD e OSPF no módulo no slot 3. Ao contrário dessa(s) sessão(s) BFD e OSPF no módulo no slot 4, são estabelecidas e permanecem estáveis.

N7k-A# **show bfd neighbors**

```
OurAddr NeighAddr LD/RD RH/RS Holdown(mult) State Int
10.80.1.162 10.80.1.161 1090519054/1090519044 Up 5764(3) Up Eth4/10
```

N7k-A#

N7k-A# **show ip ospf neighbors**

```
OSPF Process ID 1
Total number of neighbors: 3
Neighbor ID Pri State Up Time Address Interface
10.80.0.2 1 EXSTART/ - 00:02:54 10.80.1.62 Vlan6
10.80.4.25 1 INIT/DR 00:00:05 10.80.6.174 Eth3/14
10.80.0.3 1 FULL/DR 20:29:28 10.80.1.161 Eth4/10
```

N7k-A#

O que acontece quando um ARP Packet Storm para?

Quando uma tempestade de pacotes ARP é interrompida, a seguinte recuperação ocorre automaticamente e a rede começa a convergir e desfruta do estado estável que ocorreu antes da tempestade de broadcast ARP.

1. Entradas de cache ARP são resolvidas em N7k-A
2. Sessões BFD no módulo no slot 3 restabelecem
3. Sessões OSPF no módulo no slot 3 restabelecem

Conclusão

Embora o Cisco NX-OS possa distribuir a operação de BFD para módulos compatíveis que suportam BFD, grandes volumes de tráfego ARP atingindo a CPU do switch por um período maior que o tempo restante para atualizar entradas de cache ARP locais na plataforma Nexus 7000 causarão instabilidade em sessões de BFD e em quaisquer protocolos de cliente registrados com BFD.

Isso pode ser atribuído à operação BFD, que exige a resolução ARP do próximo salto, que é unicast. Se a entrada da cache ARP para o próximo salto não for atualizada a tempo, as sessões de BFD falharão.