

Kann ein ARP-Paketsturm BFD-Sitzungen auf der Nexus 7000-Plattform beeinträchtigen?

Inhalt

[Einführung](#)

[F. Da Cisco NX-OS den BFD-Betrieb auf kompatiblen Modulen verteilen kann, die BFD unterstützen, stellt sich die Frage, ob ein ARP-Paket-Sturm Auswirkungen auf BFD-Sitzungen auf der Nexus 7000-Plattform hat.](#)

[Details zur Einrichtung](#)

[ARP-Sturm beginnt](#)

[ARP Storm beginnt mit Auswirkungen auf die Kontrollebene](#)

[Was passiert, wenn ein ARP-Paketsturm aufhört?](#)

[Schlussfolgerung](#)

Einführung

Dieses Dokument beschreibt die Auswirkungen von ARP Packet Storm auf Kontrollebenenprotokolle wie BFD, OSPF und andere, die auf Nexus 7000-Switches ausgeführt werden.

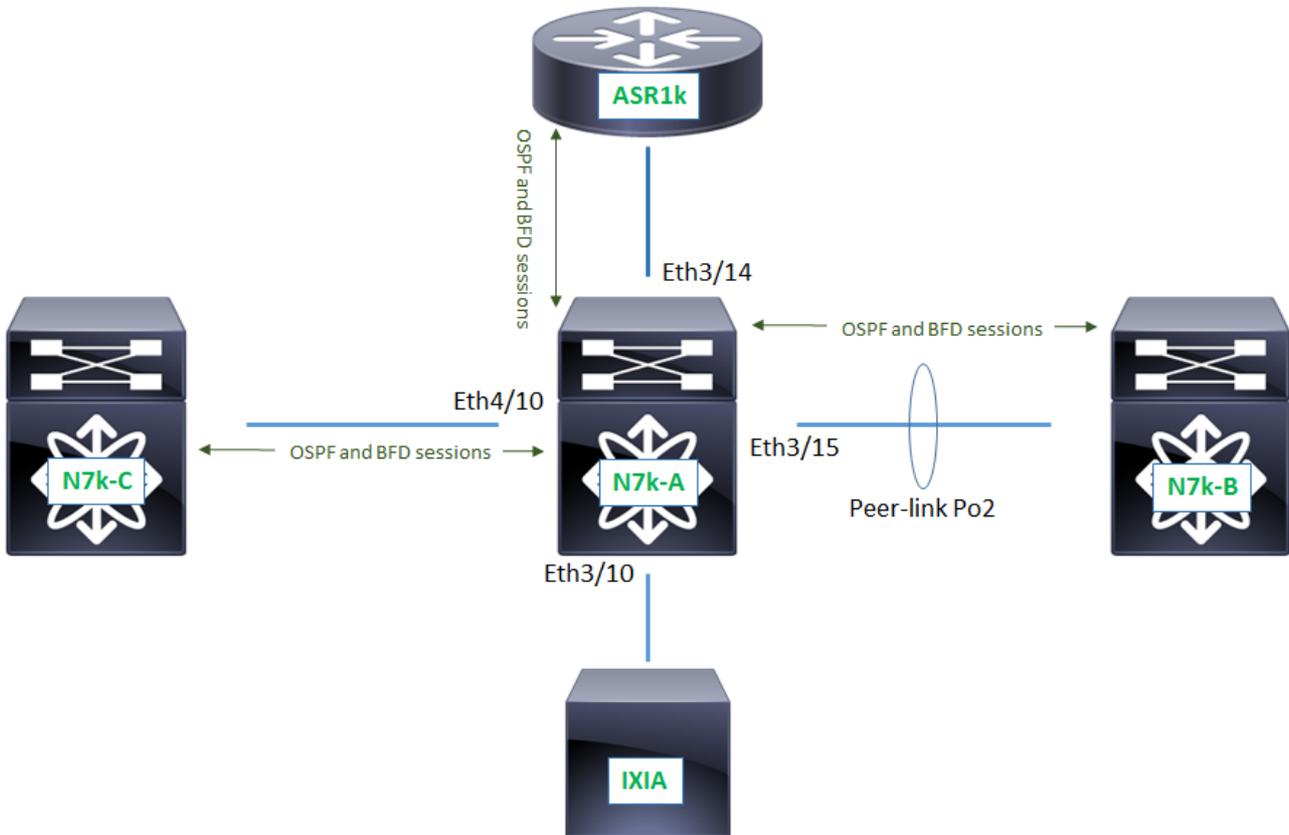
Unterstützt von Nishad Mohiuddin, Nikolay Kartashev, Cisco TAC Engineers.

F. Da Cisco NX-OS den BFD-Betrieb auf kompatiblen Modulen verteilen kann, die BFD unterstützen, würde ein ARP-Paketsturm Auswirkungen auf BFD-Sitzungen auf der Nexus 7000-Plattform haben?

Antwort: Im Allgemeinen kann ein ARP-Paketsturm negative Auswirkungen auf die Stabilität von BFD-Sitzungen haben, die auf dem Nexus 7000 ausgeführt werden. Die genauen Symptome hängen von der Langlebigkeit und der Größenordnung des ARP Packet Storm-Ereignisses ab. Nachstehend finden Sie die Testergebnisse des Cisco TAC-Labornetzwerks.

Details zur Einrichtung

Die folgende Lab-Einrichtung wurde entwickelt, um die Auswirkungen von Mengen des ARP-Datenverkehrs auf die CPU des Nexus 7000 zu testen.



Hier wird N7k-A als Device Under Test (DUT) verwendet. DUT ist ein Nexus 7009-Switch mit der folgenden Hardwarekonfiguration.

```
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 hat die folgenden Geräte angeschlossen:

- N7k-B ist ein vPC-Peer, der an die Schnittstelle Ethernet 3/15 angeschlossen ist.
- ASR1k ist ein Layer-3-Nachbar, der mit Ethernet 3/14-Schnittstelle verbunden ist.
- N7k-C ist ein Layer-3-Nachbar, der an die Schnittstelle Ethernet 4/10 angeschlossen ist.
- Der IXIA Traffic Generator ist in VLAN 6 mit Ethernet 3/10-Schnittstelle verbunden, die als Layer-2-Access-Port konfiguriert ist.

DUT hat drei BFD-Sitzungen, eine auf der Linecard in Steckplatz 4 Richtung N7k-C und zwei auf der Linecard in Steckplatz 3 Richtung N7k-B und 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#

DUT verfügt außerdem über drei OSPF-Sitzungen, eine auf der Linecard in Steckplatz 4 Richtung N7k-C und zwei auf der Linecard in Steckplatz 3 in Richtung N7k-B und 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 ist bei BFD registriert.

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

Die ARP-Tabelle auf N7k-A enthält außerdem Einträge für alle drei BFD/OSPF-Nachbarn.

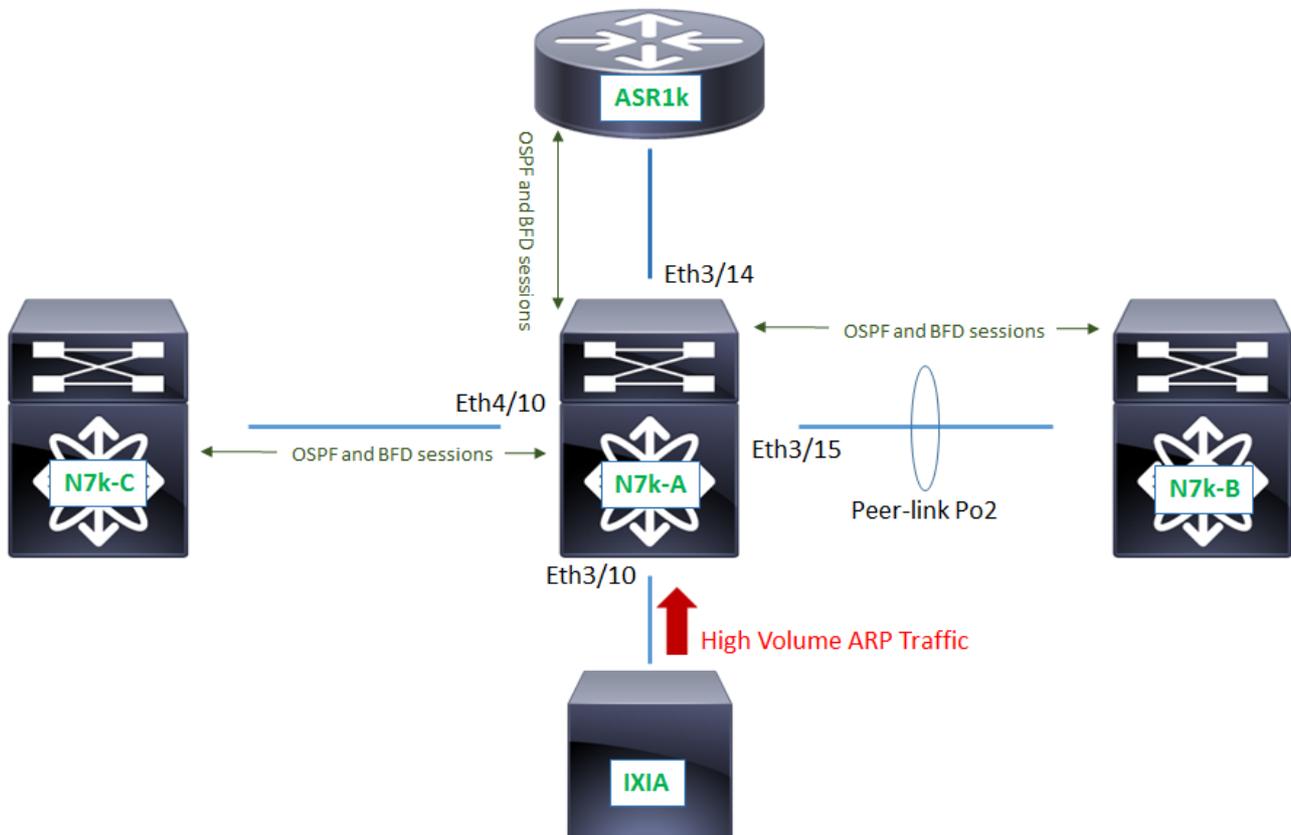
N7k-A# **show ip arp**

```
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#

ARP-Sturm beginnt

Der IXIA Traffic Generator wird verwendet, um einen instabilen Teil des Netzwerks zu simulieren. Dies führt zu einem hohen Volumen an ARP-Datenverkehr, der an DUT gesendet wird, wie im folgenden Diagramm gezeigt wird.



Die folgende Ausgabe zeigt einen Anstieg des Eingangsdatenverkehrs an der Schnittstelle Ethernet 3/10, an der der IXIA Traffic Generator angeschlossen ist. Diese Pakete werden als Broadcast-ARP-Pakete in VLAN 6 empfangen.

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

Da in diesem Szenario eine Kopie jedes Broadcast-ARP-Pakets an die CPU auf Nexus 700-A gesendet wird, nimmt die Anzahl der verletzten Bytes auf Modul 3 in CoPP zu

```
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#
```

Hinweis: Beachten Sie, dass in Steckplatz 4 keine beschädigten Bytes auf dem Modul vorhanden sind, da die Quelle des Broadcast-ARP-Sturms nur mit Schnittstelle auf Modul 3

verbunden ist.

Zu dem Zeitpunkt, zu dem der ARP-Sturm beginnt, sind die oben genannten Ausgaben normalerweise die ersten (und einzigen) Zeichen, die auf ein Netzwerkproblem hinweisen. In den meisten Fällen werden diese Zeichen unbemerkt oder von den Netzwerkbetreibern übersehen und führen schnell zu einer Situation, die zu großen Verbindungsproblemen führt.

ARP Storm beginnt mit Auswirkungen auf die Kontrollebene

Standardmäßig ist der ARP-Timeout-Wert auf der Nexus 7000-Plattform für 25 Minuten oder 1500 Sekunden konfiguriert. Der Nexus-Switch muss regelmäßig die lokalen ARP-Cache-Einträge aktualisieren, um die IP-to-MAC-Auflösung seiner nächsten Hop-Layer-3-Nachbarn auf dem neuesten Stand zu halten.

Im Folgenden sehen Sie die Ausgabe der ARP-Cachetabelle für DUT, nachdem die Einträge im ARP-Cache abgelaufen sind.

```
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#
```

Beachten Sie, dass ARP-Cache-Einträge für Geräte, die an die Linecard in Steckplatz 3 angeschlossen sind, den **INCOMPLETE**-Status anzeigen, während der Eintrag für den Switch N7k-C, der an die Linecard in Steckplatz 4 angeschlossen ist, wie erwartet erfolgreich aktualisiert wird.

Die folgenden DUT-Protokollmeldungen weisen auf die Auswirkungen auf die Kontrollebene hin

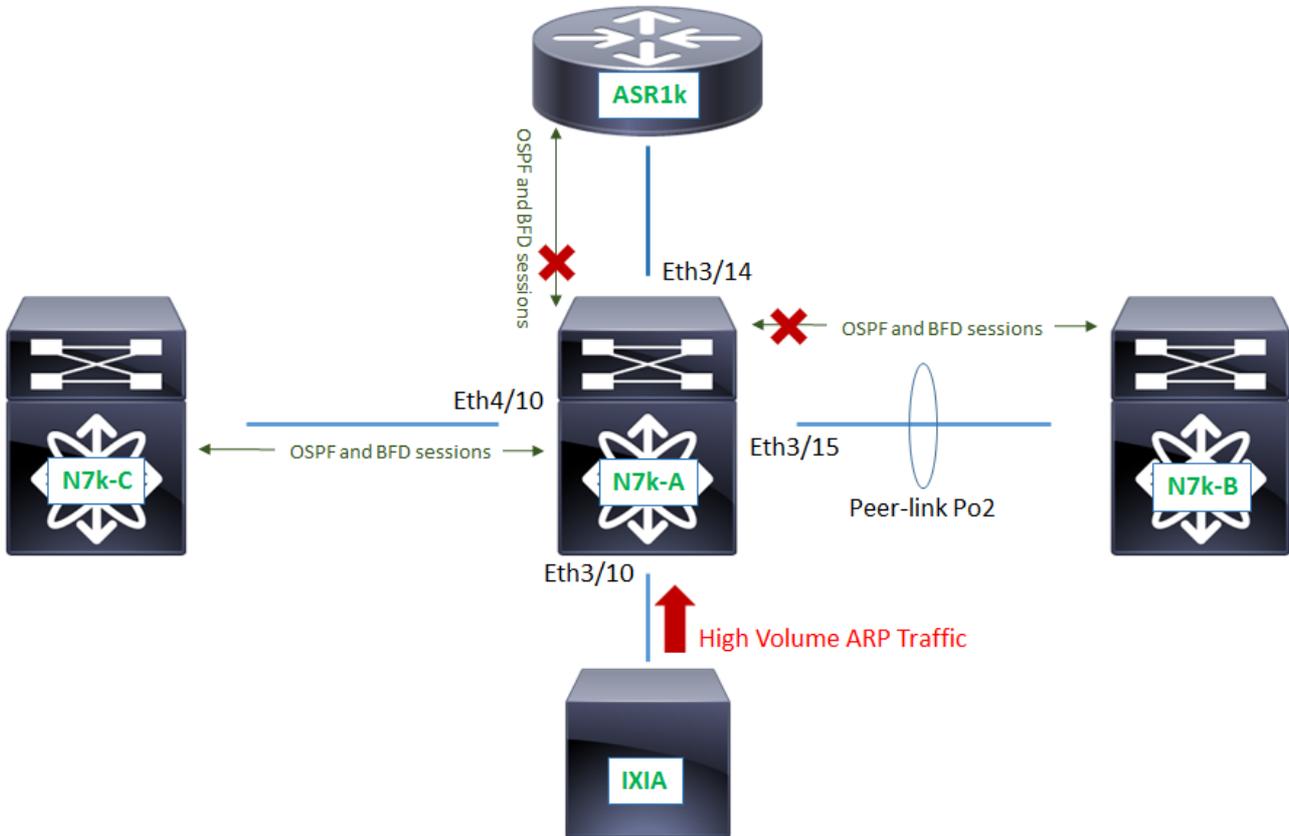
```
N7k-A# show logging log
```

```
...
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#
```

Beachten Sie in dieser Ausgabe, dass OSPF zwischen dem EXSTART-Zustand und dann zurück in den INIT-Status wechselt. Dies liegt daran, dass OSPF Unicast zum Austausch von Präfixen

während des EXSTART-Zustands verwendet. Da die ARP-Auflösung auf dem Modul in Steckplatz 3 zum Zeitpunkt des ARP-Paketsturms unvollständig ist, wird der Routenaustausch niemals abgeschlossen, sodass die OSPF-Adjacency nicht gebildet wird.

Hinweis:Die Auflösung von ARP zu IP zu MAC beim nächsten Hop beruht auf Unicast, ebenso wie der BFD-Betrieb. Da wir zu dem Schluss kommen können, dass BFD die Auflösung von ARP für einen ordnungsgemäßen Betrieb erfordert.



Die folgenden Ausgaben bestätigen die Auswirkungen eines ARP-Paketsturms auf BFD- und OSPF-Sitzungen des Moduls in Steckplatz 3. Entgegen dieser BFD- und OSPF-Sitzung(en) am Modul in Steckplatz 4 sind eingerichtet und stabil.

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#

Was passiert, wenn ein ARP-Paketsturm aufhört?

Wenn ein ARP-Paketsturm beendet wird, erfolgt die folgende Wiederherstellung automatisch, und das Netzwerk beginnt zu konvergieren und genießt den stabilen Zustand, der vor dem ARP-Broadcast-Sturm auftrat.

1. ARP-Cache-Einträge werden auf N7k-A aufgelöst
2. BFD-Sitzungen auf Modul in Steckplatz 3 wieder einrichten
3. Wiederherstellung von OSPF-Sitzungen auf Modul in Steckplatz 3

Schlussfolgerung

Obwohl Cisco NX-OS den BFD-Betrieb an kompatible Module verteilen kann, die BFD unterstützen, verursachen große Mengen von ARP-Datenverkehr, der die CPU des Switches über einen längeren Zeitraum als die Zeit bis zur Aktualisierung der lokalen ARP-Cache-Einträge auf der Nexus 7000-Plattform erreicht, Instabilität in BFD-Sitzungen und allen mit BFD registrierten Clientprotokollen.

Dies kann dem BFD-Vorgang zugeschrieben werden, der die ARP-Auflösung des nächsten Hop erfordert, der Unicast ist. Sollte der ARP-Cache-Eintrag für den nächsten Hop nicht rechtzeitig aktualisiert werden, schlägt die bzw. werden die BFD-Sitzungen fehl.