

Possibile impatto di una tempesta di pacchetti ARP sulle sessioni BFD sulla piattaforma Nexus 7000

Sommario

[Introduzione](#)

[D. Dal momento che Cisco NX-OS può distribuire l'operazione BFD a moduli compatibili che supportano BFD, un pacchetto ARP avrebbe un impatto sulle sessioni BFD sulla piattaforma Nexus 7000?](#)

[Dettagli configurazione lab](#)

[Inizia la tempesta ARP](#)

[La tempesta ARP inizia a colpire il Control Plane](#)

[Cosa succede quando si arresta una tempesta di pacchetti ARP?](#)

[Conclusioni](#)

Introduzione

Questo documento descrive l'impatto di ARP Packet Storm sui protocolli Control Plane come BFD, OSPF e altri, in esecuzione sugli switch Nexus 7000.

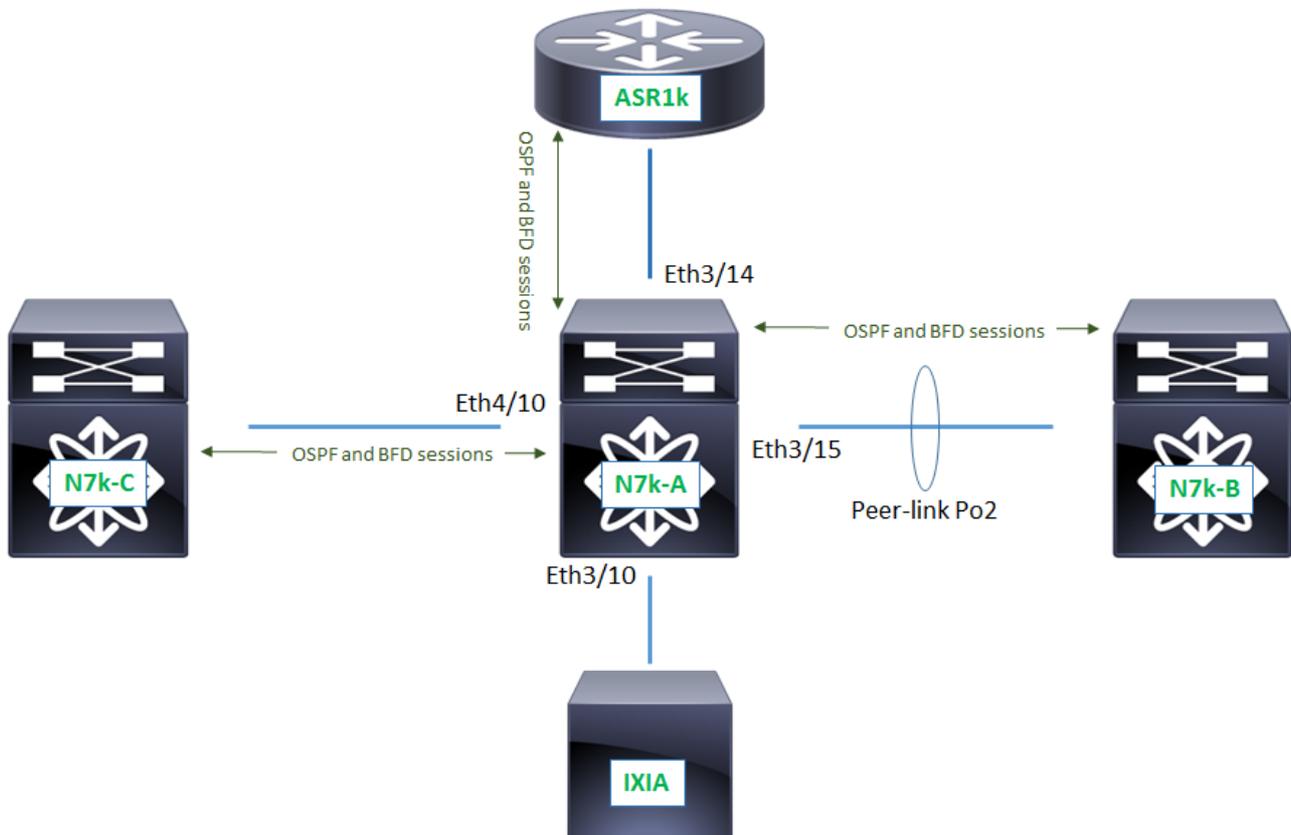
Contributo di Nishad Mohiuddin, Nikolay Kartashev, Cisco TAC Engineers.

D. Dal momento che Cisco NX-OS può distribuire il BFD ai moduli compatibili che supportano BFD, un pacchetto ARP avrebbe un impatto sulle sessioni BFD sulla piattaforma Nexus 7000?

R. In generale, una tempesta di pacchetti ARP può avere un impatto negativo sulla stabilità delle sessioni BFD in esecuzione sullo switch Nexus 7000. I sintomi esatti dipendono dalla longevità e dall'intensità dell'evento ARP Packet Storm. Di seguito vengono riportati i risultati dei test eseguiti da Cisco TAC lab network.

Dettagli configurazione lab

La seguente configurazione lab è stata progettata per testare l'impatto di quantità di traffico ARP sulla CPU dello switch Nexus 7000.



In questo caso, N7k-A viene utilizzato come DPT (Device Under Test). DUT è uno switch Nexus 7009 con la seguente configurazione 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 dispone dei seguenti dispositivi collegati

- N7k-B è un peer VPC collegato all'interfaccia Ethernet 3/15
- ASR1k è un router adiacente di layer 3, collegato all'interfaccia Ethernet 3/14
- N7k-C è un router adiacente di layer 3, collegato all'interfaccia Ethernet 4/10
- IXIA Traffic Generator si trova nella vlan 6, collegata all'interfaccia Ethernet 3/10, configurata come porta di accesso di layer 2

DUT ha tre sessioni BFD, una su scheda di linea nello slot 4 verso N7k-C, e due su scheda di linea nello slot 3 verso 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#

DUT ha anche tre sessioni OSPF, una sulla scheda di linea nello slot 4 verso N7k-C, e due sulla scheda di linea nello slot 3, verso 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 registrato con BFD

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

Inoltre, la tabella ARP su N7k-A ha voci per tutti e tre i BFD/OSPF adiacenti

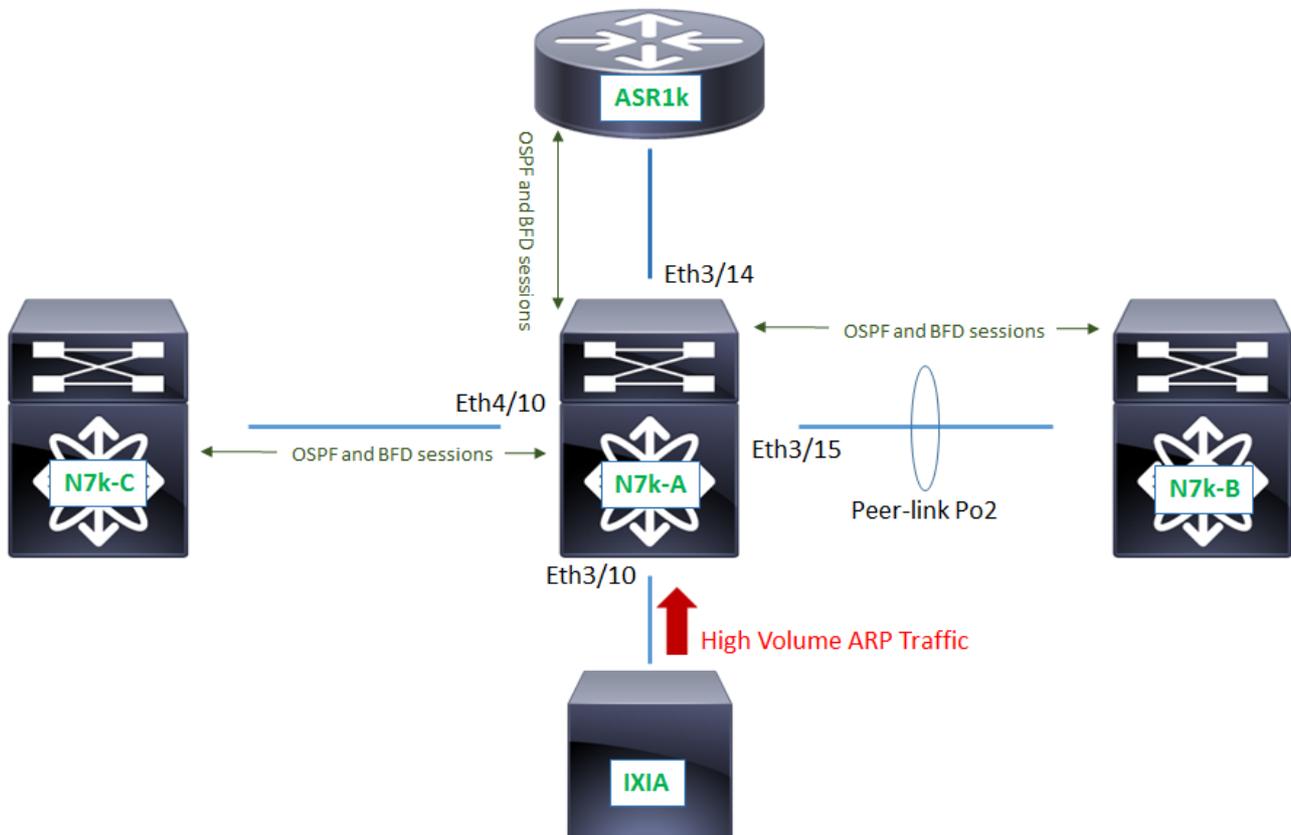
N7k-A# **show ip arp**

```
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#

Inizia la tempesta ARP

Il generatore di traffico IXIA viene usato per simulare una parte instabile della rete, il che risulta in un elevato volume di traffico ARP inviato alla DUT, come si può vedere nel diagramma sottostante



L'output seguente mostra un aumento del traffico di input sull'interfaccia Ethernet 3/10, a cui è collegato il generatore di traffico IXIA. Si tratta di pacchetti ARP broadcast ricevuti nella 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#
```

Poiché in questo scenario viene inviata alla CPU una copia di ogni pacchetto ARP di trasmissione su N7k-A, si verifica un aumento dei byte violati sul modulo 3 in 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#
```

Nota: Notare che non ci sono byte violati sul modulo nello slot 4, poiché la fonte di broadcast ARP storm è collegata all'interfaccia solo sul modulo 3

Nel punto in cui inizia la tempesta ARP, le uscite precedenti sono in genere i primi (e unici) segnali che indicano un problema sulla rete. Nella maggior parte dei casi, questi segnali passano inosservati o vengono ignorati dagli operatori di rete e si trasformano rapidamente in una situazione che comporta problemi di connettività rilevanti.

La tempesta ARP inizia a colpire il Control Plane

Per impostazione predefinita, il valore di timeout ARP sulla piattaforma Nexus 7000 è configurato per 25 minuti o 1500 secondi. Lo switch Nexus deve aggiornare periodicamente le voci della cache ARP locale per mantenere aggiornata la risoluzione IP-MAC dei router adiacenti del layer 3 dell'hop successivo.

Di seguito è riportato l'output della tabella della cache ARP in DUT dopo la scadenza delle voci della cache ARP.

```
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#
```

Si noti che le voci della cache ARP per i dispositivi collegati alla scheda di linea nello slot 3 mostrano lo stato **INCOMPLETE**, mentre la voce per lo switch N7k-C, collegato alla scheda di linea nello slot 4, viene aggiornata correttamente.

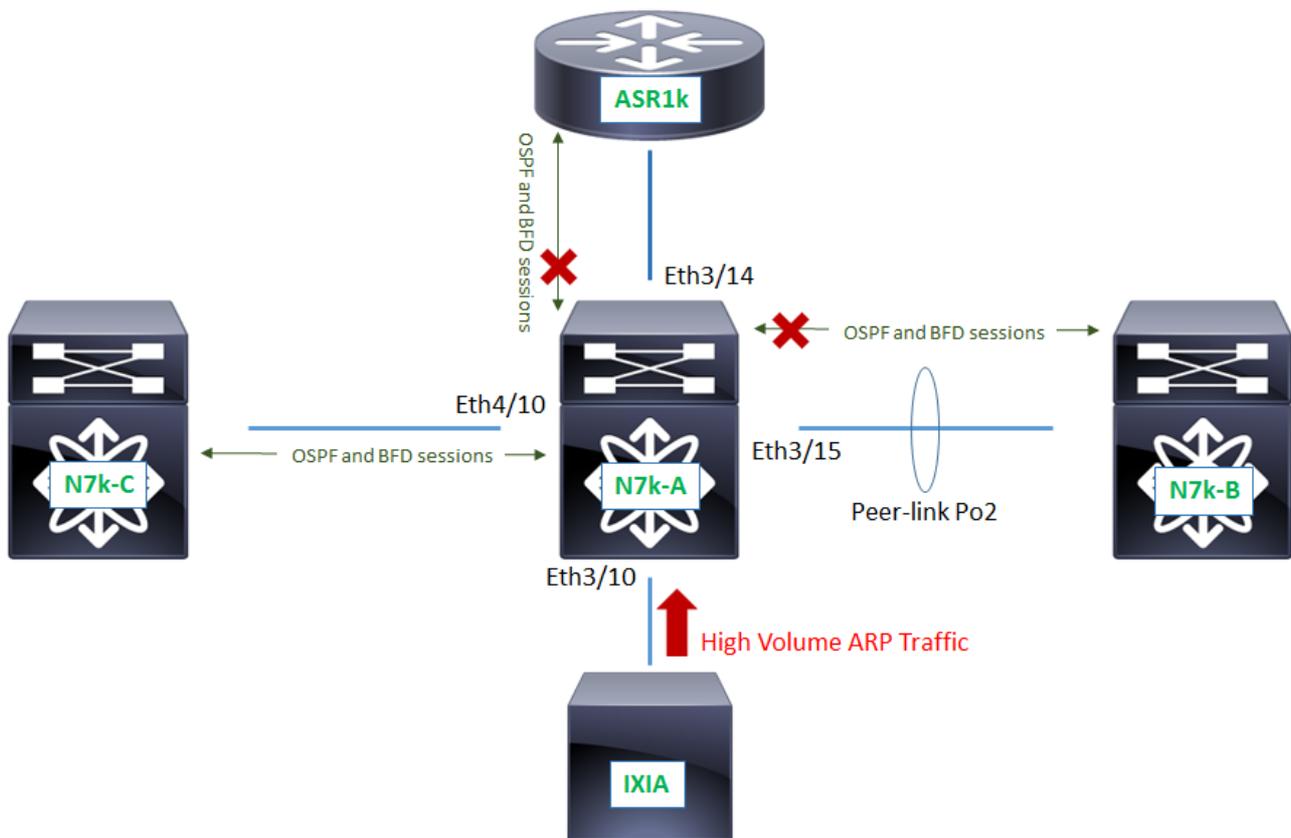
I seguenti messaggi di log DUT indicano l'impatto sul livello del Control Plane

```
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#
```

In questo output, OSPF passa dallo stato DOWN allo stato EXSTART e quindi allo stato INIT. Ciò si verifica perché OSPF utilizza unicast per lo scambio di prefissi durante lo stato EXSTART. Poiché la risoluzione ARP è incompleta sul modulo nello slot 3 al momento della tempesta del pacchetto ARP, lo scambio di route non viene mai completato e di conseguenza l'adiacenza OSPF non si forma.

Nota La risoluzione da ARP a IP-MAC dell'hop successivo dipende dalla modalità unicast, come del resto il funzionamento BFD. Dato che si può concludere che la BFD richiede la risoluzione dell'ARP per un corretto funzionamento.



I seguenti output confermano l'impatto di un pacchetto ARP storm su entrambe le sessioni BFD e OSPF sul modulo nello slot 3. Contrariamente a queste sessioni BFD e OSPF sul modulo nello slot 4, vengono stabiliti e rimangono stabili.

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#

Cosa succede quando si arresta una tempesta di pacchetti ARP?

Quando si arresta una tempesta di pacchetti ARP, il ripristino seguente si verifica automaticamente e la rete inizia a convergere e a godere dello stato stabile che aveva prima della tempesta di trasmissione ARP.

1. Le voci della cache ARP vengono risolte in N7k-A
2. Ristabilire le sessioni BFD sul modulo nello slot 3
3. Ripristino delle sessioni OSPF sul modulo nello slot 3

Conclusioni

Anche se Cisco NX-OS è in grado di distribuire il funzionamento dei BFD ai moduli compatibili che supportano i BFD, elevati volumi di traffico ARP che colpiscono la CPU dello switch per un periodo di tempo superiore a quello necessario per aggiornare le voci della cache ARP locale sulla piattaforma Nexus 7000 causeranno instabilità nelle sessioni BFD e nei protocolli client registrati con BFD.

Questa condizione può essere attribuita all'operazione BFD che richiede la risoluzione ARP dell'hop successivo unicast. Se la voce della cache ARP per l'hop successivo non viene aggiornata in tempo, le sessioni BFD avranno esito negativo.