

نود اھالصالو (ARP) ناونعلا لیلحت لوکوتورب ةفصاع نود اھالصالو Nexus 7000 ءاطخأ فاشکتسال یلخادلا قاطنلا طاقنلا

تایوتحمل

[ةمدقملا](#)

[ةیفلخللا](#)

[یرذج ببس](#)

[لحللا](#)

ةمدقملا

لخاد رورم ةكرح ی نود، اھالصالو ARP ةفصاع ءاطخأ فاشکتسال ةیفك دننتمسلا اذھ حضوی ARP.

ةیفلخللا

ةئیب یف نودھاشن امك (DoS) ةمدخلل ضفر یلع ءاش موجه ةبائتمب ARP Storm موجه ربتعی تانایبلا زكرم.

وھ ARP ةمزح ءلعمل ءاشلا لوھملا قطنم:

- (MAC) ثبلا ءهجو طئاسو یل لوصول یف مكحتلا عم ARP ةمزح
- حاتفملا یل بسنتنی یأ، MAC ةیاع Unicast عم ARP ةمزح

(SVI) لوھملا ءیرهظلا ءهجالو تاناك اذل جم انربلا یف ARP ةیلمع ءطساوب اھتجالعم متتس ءل بقتسملا VLAN ءكبش یف لیغشلا دق.

ءكبش یف ARP ببلط لاسرا یف رمئسی رثكأ وأ دھاو راض فیضم كانه ناك اذل، قطنملا اذھ جم انربلا یف ARP ببلط ءلعم متتس. ھذھ VLAN ءكبش نع ءرابع لوھملا نوک ی شیح، VLAN یرتس، مدقألا اھرادصلو Cisco تالوھم جڈامن ضعب یف. لوھملا زواجت یف ببستت یللاتلابو اءل لوغشم ماظنلاو لالعوئسم یتح ءیزكرملا ءلعملا ءدحو ماخذتسا لڈات ARP ءیلمع نا یھ موجهلا اذھ عبئتل ءل ءاشلا قیڑطلا. یلخال مكحتلا یوتسم تانایب رورم ءكرح ءلعملا ARP ءفصاعل MAC رءصم ددحتل قاطنلا لخاد طاقنلا لیغش.

رېثأتللا اذھ لیلقت متی، ءمچتلا ءابوبك Nexus 7000 لمعی شیح تانایبلا زكرم یف Inband لیغش كنانكم اب لازي ال. [Nexus 7000 Series Switches تالوھم یلع CoPP](#) ءطساوب رءصم ددحتل [Nexus 7000 نم اھلحو تالکشملا فاشکتسال لیلد یلع Ethalyzer](#) Capture یلع لمعی قرط عاطق درجم وھ (CoPP) "مكحتلا یوتسم میظنت" نال ارظن ARP ءفصاعل MAC ءدحو یل ARP ءفصاع ءعرس ءیرفت یلع لمعی ال ھنكلو ARP ءفصاع ءعرس ءاطبلا ءیزكرملا ءلعملا.

ثیح ویرانیسلا اذھ نع اذام:

- لفسأ SVI
- ءیزكرملا ءلعملا ءدحو یف ءلزالا ARP ءمزح نیمضت متی ال

• ARP عملية بـسبب الـاع (CPU) ةـزكـرم ةـجـلـاعـم ةـدـحـو دـجـوت الـ
ARP لـمـتـكـي مـل ، لـاـثـمـلـا لـيـبـس يـلـع ، ةـلـصـلـا تـاـذ ARP ةـلـكـشـم يـرـي لـوـحـمـلـا لـاـزـي الـ ، كـلـذـلـم و
اـهـي فـي بـسـلـا يـه ARP ةـفـصـاع نـوـكـت نـا لـمـتـحـمـلـا نـم لـهـو . رـشـابـمـلـا لـصـتـمـلـا فـيـضـمـلـا فـي
Nexus 7000 يـلـع مـعـن يـه ةـبـاـجـالـا .

يـرـذـج بـبـس

ARP بـلـط مـوقـيـس ، CoPP فـي ARP ةـمـزـح ةـيـلـمـع مـعـدـل ، Nexus 7000 طـخـلـا ةـقـاطـب مـيـمـصـت فـي
ةـدـاعـا كـرـحـم فـي CoPP ةـطـسـا و بـلـدـعـمـلـا دـيـدـحـت مـتـي مـث (LIF) ةـصـاـخ ةـيـقـطـنـم ةـهـجـا و لـيـغـشـت بـ
و (VLAN) ةـيـرـهـاـظـلـا ةـيـلـحـمـلـا ةـكـبـشـلـل يـلـعـال SVI دـوـج و نـع رـظـنـلـا ضـغـب ثـدـحـي اـذـه . (FE) هـيـجـوـتـلـا
الـ .

ARP بـلـط لـاـسـرا مـدـع وـه FE هـتـذـخـتـا يـذـلـا يـئـاـهـنـلـا هـيـجـوـتـلـا ةـدـاعـا رـارـق نـوـكـي اـمـنـيـب ، يـلـلـاـتـلـا بـو
ةـيـرـهـاـظـلـا ةـيـلـحـمـلـا ةـكـبـشـلـل يـلـعـال SVI دـوـج و مـدـع ةـلـاـح فـي (ةـيـزـكـرـمـلـا ةـجـلـاعـمـلـا ةـدـحـو لـخـاـدـل
طـرـفـمـلـا ARP بـلـط مـع CoPP عـبـشـت يـلـا كـلـذـي دـؤـي . اـثـدـحـم لـاـزـي الـ CoPP دـاـعـ نـا فـ ، (VLAN)
نـكـلـو ةـطـرـفـم ةـيـلـخـاـدـا ARP مـزـح يـا يـرت نـل ، وـيـرـانـيـسـلـا اـذـه فـي . عـوـرـشـمـلـا ARP دـر/بـلـط طـاـقـسـا و
ARP ةـفـصـاع بـرـثـاـتـت لـاـزـت الـ

لـوـالـا CoPP مـوـي فـي كـوـلـسـلـا اـذـهـل هـلـيـجـسـت مـت [CSCub47533](#) نـسـحـم اـطـخـا نـيـدـلـا .

لـحـلـل

تـارـاـيـخـلـا دـحـا و . وـيـرـانـيـسـلـا اـذـه فـي ARP ةـفـصـاع رـدـصـم دـيـدـحـتـلـا ةـلـيـلـق تـارـاـيـخـا كـانـه نـوـكـت دـق
وـه ةـلـاعـفـلـا :

- ARP ةـفـصـاع اـهـنـم يـتـاـتـي تـلـا ةـدـحـولـا دـيـدـحـت الـوـا

```
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

...

- ىلا جاتحت دق .ةدحول ا برضت يتلا ARP مزح عيمج طاقتل ال [ELAM](#) ارجا مدختسأ ،ايناث
ةفلاخملا ARP ةمزح طاقتل اة صرف نإف ،ةفصاع تشدح اذا نكلو .تارم ةدع كلذب مايقلا
ELAM طاقتل ا نم VLAN و MAC ردصم ىلع فرعت .بحس لل ARP ةمزح نم ريثكب لصفأ

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا