Nexus 7000 はインバンド キャプチャなしでアドレス解決プロトコル（ARP）嵐を解決します

目次

概要

この資料にインバンド ARPトラフィックなしで ARP 嵐を、解決する方法を記述されています。

背景説明

ARP 嵐はデータセンタ 環境で見るよくあるサービス拒絶（DoS）攻撃です。

ARPパケットを処理するよくあるスイッチ ロジックはそれです:

- ブロードキャスト Destination Media Access Control（MAC）の ARPパケット
- スイッチに属するユニキャスト 送信先MAC の ARPパケット、

Switch Virtual Interface（SVI）が受信 VLAN に稼働している場合ソフトウェアの ARPプロセスによって処理されます。

このロジックによって、あれば 1つ以上の malicous ホストはスイッチがその VLAN のゲートウェイである VLAN で ARP要求を送信 し続けます。 ARP要求はソフトウェアでそれ故に原因になります圧倒されるスイッチの処理されます。 より古い Ciscoスイッチ モデルおよびバージョンでは、ARPプロセスが高レベルまで CPU使用を奪取 し、システムが他のコントロール プレーン トラフィックを処理するには余りにも使用中であることがわかります。そのような攻撃をトレースする一般的な方法は ARP 嵐の発信元MAC を識別するためにインバンド キャプチャを実行することです。

Nexus 7000 が集約 ゲートウェイとして機能しているデータセンタでは、Nexus 7000 シリーズスイッチのそのような影響は CoPP によって減ります。 コントロール プレーン ポリシング（CoPP）が CPU に急ぐ ARP 嵐を減速していたりしかし not elminating ちょうど強盗であるのでまだ ARP 嵐の発信元MAC を識別するために Nexus 7000 トラブルシューティングガイドのインバンド キャプチャ Ethanalyzer を実行する可能性があります。

このシナリオかについてどのように:

- SVI はダウンしています
- CPU へパントである余分な ARPパケット無し
- ARPプロセスによる高CPU 無し

スイッチはまだしかし ARP 関連問題を見ても、例えば直接接続されたホストに不完全な ARP があります。 それは ARP 嵐によって多分引き起こされますか。

返事は Nexus 7000 にはいあります。

根本的原因

関連 7000 ラインカード 設計では、CoPP の ARPパケット プロセスをサポートするために、ARP要求は特別な論理インターフェイス（LIF）をですフォワーディングエンジン（FE）の CoPP によって制限された比率駆動します。 これは関係のためのまたはない SVI が VLAN ある起こりません。

それ故に、FE によってなされる最終的な転送の決定は（ケースで SVI 無し VLAN のために）インバンド CPU へ ARP要求を送信 しないことであるが、CoPP カウンターはまだアップデートされます。 それは余分な ARP要求と CoPP に飽和しました導き、廃棄は ARP要求/応答を正当化します。 このシナリオでは、余分なインバンド ARPパケットを ARP 嵐からまだ見影響を受けます。

この CoPP 日 1 動作のためにファイルされる拡張 な 不具合 CSCub47533 があります。

解決策

このシナリオの ARP 嵐のソースを識別する少数のオプションがある可能性があります。 1 つの有効なオプションは次のとおりです:

- 最初にどのモジュールから ARP 嵐が来るか識別して下さい

```
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
...
```

- モジュールを押すすべての ARPパケットをキャプチャ する第 2 使用 ELAM プロシージャ。 数回それをする必要があるかもしれません。 しかし続く嵐があれば違反 ARPパケットをキャプチャ する可能性は legetimate ARPパケットより大いによくあります。 ELAM キャプチャ

からの発信元MAC および VLAN を識別して下さい。