Nexus 7000インバンドキャプチャなしのAddress Resolution Protocol(ARP)ストームのトラブルシューティング

内容

概要

このドキュメントでは、インバンドARPトラフィックなしでARPストームをトラブルシューティングする方法について説明します。

背景

ARPストームは、データセンター環境で発生する一般的なサービス拒否(DoS)攻撃です。

ARPパケットを処理する一般的なスイッチロジックは次のとおりです。

- ブロードキャスト宛先Media Access Control(MAC)を持つARPパケット
- スイッチに属するユニキャスト宛先MACを持つARPパケット

スイッチ仮想インターフェイス(SVI)が受信側のVlanでアップしている場合、ソフトウェアのARPプロセスによって処理されます。

このロジックにより、1つ以上の悪意のあるホストがVlanでARP要求を送信し続ける場合、スイッチがそのVlanのゲートウェイになります。ARP要求はソフトウェアで処理されるため、スイッチが圧倒されます。一部の古いCiscoスイッチのモデルとバージョンでは、ARPプロセスがCPU使用率を高いレベルまで引き上げ、システムがビジー状態で、他のコントロールプレーントラフィックを処理できないことがわかります。このような攻撃をトレースする一般的な方法は、

Nexus 7000がアグリゲーションゲートウェイとして機能するデータセンターでは、Nexus 7000シリーズスイッチのCoPPによってこのような影響が軽減されます。Control Plane Policing(CoPP)は単なる帯域幅の減速ですが、ARPストームをCPUに放出することはないので、Nexus 7000のトラブルシューティングガイドでインバンドキャプチャEthanalyzerを実行して、ARPストームの送信元MACを特定をできます。

このシナリオでは、次のことを行います。

- SVIがダウンしている
- 過剰なARPパケットがCPUにパントされない
- ARPプロセスが原因でCPU使用率が高くない

ただし、スイッチにはARP関連の問題が引き続き表示されます。たとえば、直接接続されたホストのARPが不完全であるなど。ARPストームによって引き起こされる可能性はありますか。

答えはNexus 7000ではyesです。

根本原因

Nexus 7000ラインカードの設計では、CoPPでARPパケットプロセスをサポートするために、ARP要求によって特別な論理インターフェイス(LIF)が駆動され、その後、フォワーディングエンジン(FE)のCoPPによってレート制限されます。 これは、SVIがVLANに対して起動しているかどうかにかかわらず発生します。

したがって、FEによる最終的な転送の決定は、インバンドCPUにARP要求を送信しないことです（VLANに対するSVIがアップしていない場合）。CoPPカウンタは引き続き更新されます。これにより、過剰なARP要求でCoPPが飽和状態になり、正当なARP要求/応答がドロップされます。このシナリオでは、過剰なインバンドARPパケットは表示されませんが、ARPストームの影響を受けます。

このCoPPの1日目の動作に関する拡張バグCSCub47533が報告されています。

解決方法

このシナリオでは、ARPストームの送信元を特定するためのオプションがいくつかあります。効果的なオプションの1つは次のとおりです。

- 最初に、ARPストームの発信元となるモジュールを特定します

```
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
...
```

- 2つ目は、ELAM手順を使用して、モジュールにヒットするすべてのARPパケットをキャプチャします。何回か行う必要があります。しかし、ストームが発生している場合は、違反した

ARPパケットをキャプチャする機会は、通常のARPパケットよりもはるかに優れています。
ELAMキャプチャから送信元MACとVlanを特定します。