ASR1000パントポリサーのロギングとモニタリング

内容

概要

このドキュメントでは、パントポリサー機能と、Ciscoアグリゲーションサービスルータ(ASR)1000およびサービス統合型ルータ(ISR)G3デバイスでの新しい変更について説明します。パントポリサーはデフォルトで有効になっており、すべてのコントロールプレーンパントされたトラフィックをポリシングします。パントポリサーおよびパント関連のドロップの詳細については、「Cisco ASR 1000シリーズサービスルータでのパケットドロップ」を参照してください。最近、パントポリサーのロギングと動作にいくつかの変更が加えられました。これは、共通のCLIユーザにデバイスでのパケットドロップの理由を特定するための明確なロギングメカニズムを提供することを目的としています。

インターフェイス単位パントポリサー

これはPolarisリリース16.4で導入されました。

これにより、ネットワーク管理者はインターフェイスごとにパントポリサー制限を設定できます。これは、膨大な数のパントトラフィックを送信するインターフェイスを特定する場合に特に役立ちます。そのため、トラブルシューティング時間が短縮され、パケットキャプチャの代替となります。この機能の前に、パントトラフィックの送信元インターフェイスを知る必要がある場合は、時間とリソースを大量に消費するパケットキャプチャを実行する必要がありました。

設定と確認

```
Router(config)#platform punt-intf rate < packet per second>

Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#punt-control enable
```

この設定により、インターフェイスごとのパントポリシングモニタリングが有効になります。たとえば、特定のインターフェイスだけでなくグローバルにもパント制御レートを1000に設定した場合、デバイスはこの特定のインターフェイスのパント廃棄を30秒間追跡します。30秒間隔が経過すると、ルータは次のようなログを表示し、パント違反イベントが発生したことを管理者に警

告します。

```
*Jun 21 23:01:01.476: %IOSXE-5-PLATFORM:  F1: cpp_cp: QFP:0.1 Thread:076 TS:00000044123616602847
%PUNT_INJECT-5-DROP_PUNT_INTF: punt interface policer drop packet from GigabitEthernet0/0/0
```

30秒は大きな間隔であるため、インターフェイスの最新のパントドロップを確認できるコマンドが導入されました。

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-intf-drop
latest
Punt Intf Drop Statistics (lastest 1000 dropped packets):

     Interface                         Packets
 ------------------------------------------
     GigabitEthernet0/0/0              1000
```

ドロップの統計情報をクリアして、リアルタイムドロップを監視できます。

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-intf-drop
latest clear
Punt Intf Drop Statistics (lastest 1000 dropped packets):

     Interface                         Packets
 ------------------------------------------
Router#
```

デフォルトのパントポリサーの口ギング

インターフェイスごとに、パントポリサーを明示的に設定する必要があります。ただし、グローバルなASRデバイスでは、原因ごとのパントポリサーが常にアクティブです。最近リリース16.6.1イメージでは、口ギングが原因パントポリサーごとに実装されています。これ以降、原因ごとのパント違反が発生するたびに口グが生成されます。

最初の口グの時点から、ルータはパントの原因を30秒間監視します。30秒後に別のドロップアクティビティが発生すると、別の口グが生成されます。

口グメッセージは次のようになります。そのため、punt cause 60のドロップが表示されます。

```
F1: cpp_cp: QFP:0.1 Thread:035 TS:00000000089593031387 %PUNT_INJECT-5-DROP_PUNT_CAUSE: punt
cause policer drop packet cause 60
```

パントの原因に関連する詳細を確認するには、次のコマンドを使用します。

```
BGL14.Q.20-ASR1006-1#show platform hardware qfp active infrastructure punt config cause 60
QFP Punt Table Configuration

Punt table base addr : 0x48F46010
 punt cause index     60
 punt cause name      IP subnet or broadcast packet
 maximum instances    1
 punt table address : 0x48F46100
 instance[0] ptr    : 0x48F46910
   QFP interface handle : 3
   Interface name       : internal1/0/rp:1
   instance address        : 0x48F46910
   fast failover address   : 0x48F2B884
```

```
   Low priority policer    : 70
   High priority policer   : 71
```

この口グ以外にも、パントドロップをモニタするために古いコマンドを常に使用できます。

```
Router#show platform hardware qfp active infrastructure punt statistics type punt-drop
Router#show platform hardware qfp active infrastructure punt statistics type per-cause
Router#show platform hardware qfp active infrastructure punt statistics type global-drop
```

結論

punt-per cause loggingとインターフェイスごとのpunt-monitoringの導入により、パント関連の問題を切り分ける優れたツールが提供されます。QFPステータスにパントドロップが表示される場合は、問題をさらに切り分けるために、説明されているツールを使用する必要があります。