Catalyst 4500 シリーズ スイッチでのレイヤ 2 コントロール フレーム用 MAC ACL の使用

目次

概要

MAC アクセス コントロール リスト（MAC ACL）を使用して、VLAN または物理レイヤ 2 ポートで IP 以外のトラフィックをフィルタリングできます。 このドキュメントでは、Catalyst 4500 シリーズ スイッチのコントロール プレーンの IP 以外のトラフィックに対する MAC ACL の動作について説明します。

mac access-list extended コマンドでサポートされている IP 以外のプロトコルの詳細については、『Catalyst 4500 シリーズ スイッチ Cisco IOS コマンド リファレンス』を参照してください。

問題

次の設定を想定します。

```
mac access-list extended udld
 deny any host 0100.0ccc.cccc
 permit any any
!
interface GigabitEthernet2/4
 switchport mode trunk
 udld port aggressive
 mac access-group udld in
!
```

この ACL では、レイヤ 2 コントロール プレーン トラフィック（例：宛先 MAC が 0100.0ccc.cccc で、インターフェイス GigabitEthernet2/4 からインバウンドで着信する CDP/UDLD/VTP/PAgP フレーム）が拒否されません。

Catalyst 4500 スイッチには、レイヤ 2 コントロール プレーン トラフィックを CPU にパントするシステム生成の組み込み ACL があります。この ACL は、このトラフィックを分類する際にユーザ定義の ACL よりも優先されます。 したがってユーザ定義 ACL はこの目的を果たしません。この動作は Catalyst 4500 プラットフォームに特有のものであり、その他のプラットフォームでは動作が異なります。

このトラフィックを入力ポートまたは CPU でドロップする必要がある場合に、そのようにドロップするには、以下で説明する手順を使用できます。

解決策

以下の手順は、宛先 MAC が 0100.0ccc.cccc であり特定のインターフェイスに着信するすべてのフレームをドロップすることを目的としています。 この MAC アドレスは UDLD/DTP/VTP/Pagp コントロール プレーン PDU により使用されます。 十分に注意してください。

目的がこのトラフィックをポリシングすることであり、すべてのトラフィックをドロップすることではない場合は、コントロール プレーン ポリシングが推奨されます。 「Catalyst 4500 でのコントロール プレーン ポリシングの設定」を参照してください。

手順 1) cdp-vtp のコントロール パケット QoS を有効にします。

```
Catalyst4500(config)#qos control-packets cdp-vtp
```

この手順では、次のシステム生成 ACL が生成されます。

```
Catalyst4500#show run | begin system-control

mac access-list extended system-control-packet-cdp-vtp
 permit any host 0100.0ccc.cccc
```

注: MAC ACL ACL TCAM ACL ACL

```
mac access-list extended udld
 permit any host 0100.0ccc.cccc
```

手順 2) この ACL にヒットするトラフィックに一致するクラスマップを作成します。

```
Catalyst4500(config)#class-map cdp-vtp
Catalyst4500(config-cmap)#match access-group name system-control-packet-cdp-vtp
Catalyst4500(config-cmap)#end
Catalyst4500#
```

手順 3) conform action として drop、exceed action として drop を指定し、前述のクラスに一致するポリシー マップとポリシー トラフィックを作成します。

```
Catalyst4500(config)#policy-map cdp-vtp-policy
Catalyst4500(config-pmap)#class cdp-vtp
Catalyst4500(config-pmap-c)#police 32000 conform-action drop exceed-action drop
Catalyst4500(config-pmap-c-police)#end
Catalyst4500#
```

手順 4) このトラフィックをドロップする必要があるレイヤ 2 ポートに、ポリシーマップをインバウンドで適用します。

```
Catalyst4500(config)#int gigabitEthernet 2/4
Catalyst4500(config-if)#service-policy input cdp-vtp-policy
Catalyst4500(config-if)#end

!
interface GigabitEthernet2/4
 switchport mode trunk
 udld port aggressive
 service-policy input cdp-vtp-policy
end
```

その他のレイヤ 2 コントロール フレームをポリシングまたはドロップする必要がある場合には、

これらのフレームに、類似するシステム生成 ACL を使用できます。 詳細については、「レイヤ 2 制御パケット QoS」を参照してください。

```
Catalyst4500(config)#qos control-packets ?
 bpdu-range        Enable QoS on BPDU-range packets
 cdp-vtp           Enable QoS on CDP and VTP packets
 eapol             Enable QoS on EAPOL packets
 lldp              Enable QoS on LLDP packets
 protocol-tunnel   Enable QoS on protocol tunneled packets
 sstp              Enable QoS on SSTP packets
 <cr>
```

Type of Packet that the Feature is Enabled On	Range of Address the Feature Acts On
BPDU-range	0180.C200.0000 BPDU 0180.C200.0002 OAM, LACP 0180.C200.0003 EAPOL
CDP-VTP	0100.0CCC.CCCC
SSTP	0100.0CCC.CCCD
LLDP	0180.C200.000E