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

内容

概要

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非IPトラフィックでのMACアクセスコントロールリスト(MAC ACL)の動作について説明します。MAC ACLは、VLANおよび物理レイヤ2(L2)ポート上の非IPトラフィックをフィルタリングするために使用できます。

MAC access-list extendedコマンドでサポートされている非IP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
!
```

> **注**：このACLでは、インターフェイスGigabitEthernet2/4で着信する宛先MAC = 0100.0ccc.ccccのCDP/UDLD/VTP/PAgPフレームなどのL2コントロールプレーントラフィックは拒否されません。

Catalyst 4500スイッチには、このトラフィックを分類するために、L2コントロールプレーントラフィックをユーザ定義ACLよりも優先されるCPUにパントするシステム生成の組み込みACLがあります。したがって、ユーザ定義ACLはこの目的を達成しません。この動作はCatalyst 4500プラットフォームに固有であり、他のプラットフォームの動作が異なる場合があります。

解決方法

この方法は、入力ポートまたはCPUでトラフィックをドロップする必要がある場合に使用できま

す。

> **注意**：この手順は、特定のインターフェイスに着信する宛先MAC = 0100.0ccc.ccccのすべてのフレームを廃棄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プロトコルデータユニット(PDU)で使用されます。

目的がこのトラフィックをポリシングし、すべてのトラフィックをドロップしない場合は、コントロールプレーンポリシングが推奨されるソリューションです。『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

ステップ1:cdp-vtpに対してcontrol-packet Quality of Service(QoS)を有効にします。

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

このステップでは、システムが生成したACLを生成します。

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

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

> **注**：ユーザ定義の名前付きMAC ACL（次に示す）を、以前に生成されたシステム定義ACLの代わりに使用することもできます。Ternary Content Addressable Memory(TCAM)リソースを保存するには、システム生成またはユーザ定義のACLを使用します。

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

ステップ2：このACLにヒットするトラフィックと一致するように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#
```

ステップ3：ステップ2クラスに一致するポリシーマップとポリシングトラフィックを、conform action = dropおよびexceed action = dropで作成します。

```
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#
```

ステップ4：このトラフィックをドロップする必要があるL2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
```

同様のシステム生成ACLは、ポリシングまたは廃棄が必要な場合に、他のL2制御フレームに使用できます。詳細と図に示すように、「レイヤ2制御パケットの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