レイヤ2 制御フレームのために MAC ACL を Catalyst 4500 スイッチ使用して下さい

目次

概要

この資料は Catalyst 4500 シリーズ スイッチのコントロール プレーン 非 IP トラフィックの MAC アクセス・コントロール・リスト（MAC ACL）の動作を記述したものです。 MAC ACL は VLAN と物理的 な レイヤ2 （L2）ポートの非 IP トラフィックをフィルタリングするために使用することができます。

MAC access-list 延長コマンドのサポートされた非 IP プロトコルに関する詳細については、Catalyst 4500 シリーズ スイッチ Cisco IOS ® コマンドレファレンスを参照して下さい。

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 は宛先が付いている CDP/UDLD/VTP/PAgP 帯のような L2 コントロール プレーン トラフィックをインターフェイス GigabitEthernet2/4 で受信来る MAC = 0100.0ccc.cccc 拒否しません。

Catalyst 4500 スイッチ、このトラフィックを分類するためにユーザが定義する ACL に優先する CPU に L2 コントロール プレーン トラフィックを、パントするシステムにより生成される内蔵 ACL があります。 それ故に、ユーザが定義する ACL はこの目的を実現させません。 この動作は Catalyst 4500 プラットフォームに特定、他のプラットフォーム異なる動作を持つかもしれません です。

解決策

そうする必要がある場合この方式が入力ポートまたは CPU でトラフィックを廃棄するのに使用することができます。

> **注意**： ここのステップは宛先を特定のインターフェイスで入る MAC = 0100.0ccc.cccc 備えているすべての帯を廃棄するように意図されています。 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）使用されます。

目標がこのトラフィックのポリシングを行ない、全部を廃棄しないことである場合コントロール プレーン ポリシングは好まれたソリューションです。 参照しま [Catalyst 4500 のコントロール プレーン ポリシングを設定します]

ステップ 1. cdp 可変端末プロトコルのための有効制御パケット サービス品質（QoS）:

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

このステップはシステムにより生成される 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:**（ここに示されている）ユーザが定義するネームド MAC ACL も先に生成されるようにシステムによって定義される ACL の代りに使用することができます。 Ternary Content Addressable Memory（TCAM）リソースを節約するためにシステムにより生成されるかユーザが定義する ACL 使用して下さい。

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

ステップ 2.トラフィックを一致するために class-map を作成して下さいこの ACL を見つける:

```
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.操作 = ドロップするステップ 2 クラスと準拠する一致するポリシングを行ない、操作 = ドロップするを超過して下さいポリシー マップを作成し、トラフィックを:

```
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.このトラフィックが廃棄される必要がある L2 ポートで受信 policy-map を適用して下さい:

```
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
```

同じようなシステムにより生成される ACL は他の L2 制御フレームにポリシングが行われるか、または廃棄される必要があれば使用することができます。 詳細についてはおよびイメージに示すようにレイヤ2 制御パケット QoS を参照して下さい。

```
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