ACL de MAC d'utilisation des trames de contrôle de la couche 2 sur des Commutateurs de gamme Catalyst 4500

Contenu

[Introduction](#)
[Problème](#)
[Solution](#)

Introduction

Ce document décrit le comportement de la liste de contrôle d'accès de MAC (ACL de MAC) sur le trafic non-IP d'avion de contrôle sur des Commutateurs de gamme Catalyst 4500. L'ACL de MAC peut être utilisé afin de filtrer le trafic non-IP sur un VLAN et sur un port de la couche physique 2 (L2).

Pour plus d'informations sur les protocoles non-IP pris en charge dans la commande mac access-list extended, référez-vous la référence de commandes de Cisco IOS® de commutateur de gamme Catalyst 4500.

Problème

Assumez cette configuration :

```
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
!
```

> **Note**: Cet ACL ne refuse pas le trafic d'avion du contrôle L2 comme des trames CDP/UDLD/VTP/PAgP avec le MAC de destination = le 0100.0ccc.cccc qui est livré d'arrivée dans l'interface GigabitEthernet2/4.

Sur des Commutateurs du Catalyst 4500, il y a un ACL incorporé généré par le système qui donne un coup de volée le trafic d'avion du contrôle L2 à la CPU qui a la priorité au-dessus d'un ACL défini par l'utilisateur, afin de classifier ce trafic. Par conséquent, un ACL défini par l'utilisateur ne réalise pas ce but. Ce comportement est spécifique à la plate-forme du Catalyst 4500, d'autres Plateformes pourrait avoir différents comportements.

Solution

Cette méthode peut être utilisée pour relâcher le trafic au port d'entrée ou à la CPU, s'il y a un besoin de faire ainsi.

> **Attention** : Des étapes ici sont destinées pour relâcher toutes les trames qui ont le MAC de destination = le 0100.0ccc.cccc qui entre sur une interface spécifique. Cette adresse MAC est utilisée par les Protocol Data Unit d'avion de contrôle UDLD/DTP/VTP/Pagp (PDU).

Si l'objectif est de maintenir l'ordre ce trafic et de ne pas relâcher la totalité, la Réglementation du plan de commande est une solution préférée. Référez-vous en configurant la Réglementation du plan de commande sur le Catalyst 4500

Étape 1. Qualité de service (QoS) de paquet de contrôle d'enable pour le cdp-VTP :

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

Cette étape génère un ACL généré par le système :

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

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

> **Note**: MAC ACL Désigné défini par l'utilisateur (comme affiché ici) peut également être utilisé au lieu de l'ACL défini par système comme généré plus tôt. L'utilisez ACL généré par le système ou défini par l'utilisateur afin d'économiser les ressources associatives ternaires en mémoire (TCAM).

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

Étape 2. Créez un class-map afin d'apparier le trafic qui frappe cet ACL :

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

Étape 3. Créez un trafic de carte et de police de stratégie avec lequel la classe d'étape 2 de correspondances se conforment action = baisse et dépassent l'action = la baisse :

```
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#
```

Étape 4. Appliquez le policy-map d'arrivée sur le port L2 où ce trafic doit être abandonné :

```
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
```

ACLs généré par le système semblable peut être utilisé d'autres trames du contrôle L2 au cas où ils devraient être maintenus l'ordre ou lâchés. Référez-vous le paquet de contrôle QoS de la couche 2 pour des détails et suivant les indications de l'image.

```
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