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

Contenu

Introduction

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

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

Problème

Assume après 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
!
```

Notez que cet ACL ne refusera pas à contrôle de la couche 2 le trafic plat comme des trames CDP/UDLD/VTP/PAgP avec le MAC de destination = être livré 0100.0ccc.cccc d'arrivée dans l'interface GigabitEthernet2/4.

Sur des Commutateurs du Catalyst 4500, il y a un ACL incorporé généré par le système qui le trafic plat de contrôle de la couche 2 de coups de volée à la CPU qui a la priorité au-dessus d'un ACL défini par l'utilisateur pour 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 peut avoir différents comportements.

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

Solution

Des étapes ci-dessous sont destinées pour relâcher toutes les trames qui ont le MAC de destination = le 0100.0ccc.cccc étant livré dedans sur une interface spécifique. Cette adresse MAC est utilisée en l'avion PDU de contrôle UDLD/DTP/VTP/Pagp. Veuillez exercer l'attention.

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 s'il vous plaît en configurant la Réglementation du plan de commande sur le Catalyst 4500

Étape 1) Paquet de contrôle QoS d'enable pour le cdp-VTP.

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

Cette étape génère l'ACL généré par le système suivant

```
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 ci-dessous) peut également être utilisé au lieu de l'ACL défini par système comme généré ci-dessus. L'utilisez s'il vous plaît ACL généré par le système ou défini par l'utilisateur pour économiser des ressources TCAM.

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

Étape 2) Créez un class-map pour 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 une carte de stratégie et le trafic de police s'assortissant au-dessus de la classe avec 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 de la couche 2 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 de contrôle de la couche 2 au cas où ils devraient être maintenus l'ordre ou lâchés. Veuillez se référer le paquet de contrôle QoS de la couche 2 pour des détails.

```
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