Verwendung der MAC ACL für Layer-2-Kontrollrahmen auf Catalyst Switches der Serie 4500

Inhalt

Einführung

In diesem Dokument wird das Verhalten der MAC Access Control List (MAC ACL) auf der Kontrollebene (nicht IP-Datenverkehr) auf Catalyst Switches der Serie 4500 beschrieben. MAC ACL kann verwendet werden, um Nicht-IP-Datenverkehr in einem VLAN und einem physischen Layer-2-Port (L2) zu filtern.

Weitere Informationen zu den unterstützten Nicht-IP-Protokollen im erweiterten MAC-Zugriffslisten-Befehl finden Sie in der Cisco IOS® Befehlsreferenz für den Catalyst Switch der Serie 4500.

Problem

Nehmen wir an, diese Konfiguration:

```
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
!
```

> **Hinweis**: Diese ACL verweigert keinen L2-Steuerungsebenen-Datenverkehr wie CDP/UDLD/VTP/PAgP-Frames mit Ziel-MAC = 0100.0ccc.cccc, der in die Schnittstelle GigabitEthernet2/4 eingeht.

Auf Catalyst Switches der Serie 4500 gibt es eine systemeigene integrierte Zugriffskontrollliste, die den Datenverkehr der L2-Kontrollebene an die CPU überträgt. Diese hat Vorrang vor einer benutzerdefinierten Zugriffskontrollliste, um diesen Datenverkehr zu klassifizieren. Eine benutzerdefinierte Zugriffskontrollliste erfüllt diesen Zweck also nicht. Dieses Verhalten ist spezifisch für die Catalyst 4500-Plattform, da andere Plattformen möglicherweise unterschiedliche Verhaltensweisen haben.

Lösung

Diese Methode kann verwendet werden, um den Datenverkehr am Eingangsport oder an der CPU zu verwerfen, wenn dies erforderlich ist.

> **Vorsicht**: Die Schritte hier sind dazu gedacht, alle Frames, die das Ziel MAC = 0100.0ccc.cccc haben, die auf einer bestimmten Schnittstelle eintreffen, zu verwerfen. Diese MAC-Adresse wird von UDLD/DTP/VTP/Pagp Control Plane Protocol Data Units (PDUs) verwendet.

Wenn das Ziel darin besteht, diesen Datenverkehr zu kontrollieren und ihn nicht vollständig zu verwerfen, ist eine Kontrollebenenüberwachung eine bevorzugte Lösung. Weitere Informationen finden Sie unter Konfigurieren der Control Plane Policing für Catalyst 4500.

Schritt 1: Aktivieren von Control-Packet Quality of Service (QoS) für cdp-vtp:

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

Dieser Schritt generiert eine vom System generierte ACL:

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

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

> **Hinweis**: Anstelle der zuvor generierten, vom System definierten ACL kann auch eine benutzerdefinierte MAC ACL (wie hier gezeigt) verwendet werden. Verwenden Sie entweder eine vom System generierte oder eine benutzerdefinierte ACL, um Ternary Content Addressable Memory (TCAM)-Ressourcen zu speichern.

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

Schritt 2: Erstellen Sie eine Klassenzuordnung, um den Datenverkehr, der auf diese ACL trifft, abzugleichen:

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

Schritt 3: Erstellen Sie eine Richtlinienzuordnung und einen Richtlinienverkehr, der mit der Klasse für Schritt 2 übereinstimmt. Die Aktion gilt für "drop" und "überschreiten" = Drop:

```
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#
```

Schritt 4: Wenden Sie die Richtlinienzuweisung für eingehenden Datenverkehr an den L2-Port an, an dem dieser Datenverkehr verworfen werden muss:

```
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
```

Ähnliche, vom System generierte ACLs können für andere L2-Kontrollrahmen verwendet werden, falls sie überwacht oder verworfen werden müssen. Weitere Details und wie im Bild dargestellt finden Sie in der QoS des Layer-2-Steuerungspakets.

```
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