Éviter l'insuffisance TCAM ACL et QoS sur les commutateurs Catalyst 4500

Contenu

Introduction

Les commutateurs de la gamme Cisco Catalyst 4500 et Catalyst 4948 prennent en charge la liste de contrôle d'accès du débit câblé (ACL) et la fonction QoS avec l'utilisation de la mémoire associative ternaire (TCAM). L'activation des ACL et des politiques ne réduit pas la performance de commutation ou du routage du commutateur tant que les ACL sont complètement chargés dans la TCAM. Si la TCAM est entièrement utilisée, les paquets peuvent être expédiés par l'intermédiaire du CPU, ce qui peut réduire la performance de ces paquets. Ce document fournit des détails relatifs aux éléments suivants :

- Les différents types de TCAM que les Catalyst 4500 et Catalyst 4948 utilisent
- Comment le Catalyst 4500 programme les TCAM
- Comment configurer de manière optimale les listes de contrôle d’accès et la TCAM sur le commutateur afin d’éviter l’épuisement de la TCAM

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateurs de la gamme Catalyst 4500
- Commutateurs de la gamme Catalyst 4948

Remarque : Ce document s'applique uniquement aux commutateurs basés sur le logiciel Cisco IOS® et ne s'applique pas aux commutateurs basés sur Catalyst OS (CatOS).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Afin de mettre en oeuvre les différents types de listes de contrôle d'accès et de politiques QoS dans le matériel, les tables de recherche de matériel (TCAM) des programmes Catalyst 4500 et divers registres matériels dans le Supervisor Engine. Lorsqu'un paquet arrive, le commutateur effectue une recherche de table matérielle (recherche TCAM) et décide d'autoriser ou de refuser le paquet.

Le Catalyst 4500 prend en charge différents types de listes de contrôle d'accès. Le tableau 1 présente ces types de listes de contrôle d'accès.

Tableau 1 - Types de listes de contrôle d'accès pris en charge sur les commutateurs Catalyst 4500

Type ACL	Où Elle Est Appliquée	Trafic contrôlé	Direction
RACL [1]	Port L3 [2], canal L3 ou SVI [3] (VLAN)	Trafic IP routé	Entrant ou sortant
VACL [4]	VLAN (via la commande **vlan filter**)	Tous les paquets qui sont acheminés vers ou depuis un VLAN ou qui sont pontés dans un VLAN	Sans direction
PACL [5]	Port L2 [6] ou canal L2	Tout le trafic IP et le trafic non IPv4 [7] (via ACL MAC)	Entrant ou sortant

[1] RACL = liste de contrôle d'accès du routeur

[2] L3 = couche 3

[3] SVI = interface virtuelle commutée

[4] VACL = VLAN ACL

[5] PACL = port ACL

[6] L2 = couche 2

[7] IPv4 = IP version 4

Architecture de programmation matérielle QoS et ACL du Catalyst 4500

Le TCAM du Catalyst 4500 comporte le nombre d'entrées suivant :

- 32 000 entrées pour la liste de contrôle d'accès de sécurité, également appelée liste de contrôle d'accès de fonctionnalité
- 32 000 entrées pour la liste de contrôle d'accès QoS

Pour les listes de contrôle d'accès de sécurité et de qualité de service, les entrées sont dédiées de la manière suivante :

- 16 000 entrées pour la direction d'entrée
- 16 000 entrées pour la direction de sortie

La Figure 3 montre l'affectation des entrées TCAM. Reportez-vous à la section Types de TCAM pour plus d'informations sur les TCAM.

Le tableau 2 présente les ressources ACL disponibles pour divers moteurs de supervision et commutateurs Catalyst 4500.

Tableau 2 - Ressources de la liste de contrôle d'accès Catalyst 4500 sur différents moteurs de supervision et commutateurs

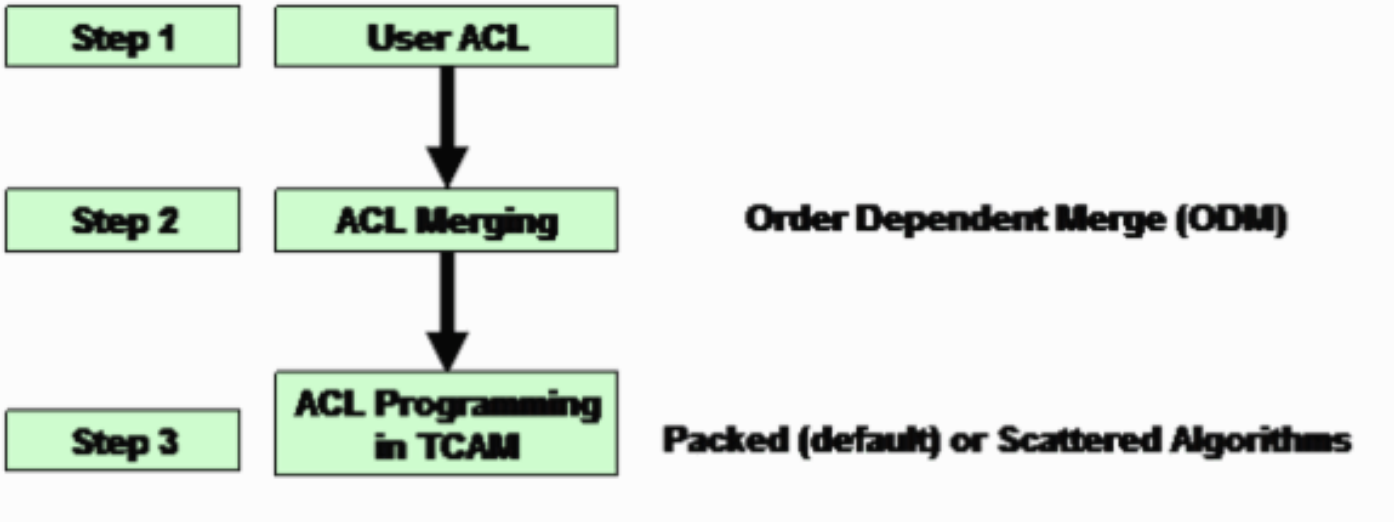
Product (produit)	Version TCAM	Fonction TCAM (par direction)	QoS TCAM (par direction)
Supervisor Engine II+	2	8 000 entrées, 1 000 masques	8 000 entrées, 1 000 masques
Supervisor Engine II+TS/III/IV/V et WS-C4948	2	16 000 entrées, 2 000 masques	16 000 entrées, 2 000 masques
Supervisor Engine V-10GE et WS-C4948-10GE	3	16 000 entrées, 16 000 masques	16 000 entrées, 16 000 masques

Le Catalyst 4500 utilise des TCAM dédiés et distincts pour le routage de monodiffusion et de multidiffusion IP. Le Catalyst 4500 peut avoir jusqu'à 128 000 entrées de route partagées par les routes de monodiffusion et de multidiffusion. Toutefois, ces détails ne sont pas abordés dans ce document. Ce document traite uniquement des problèmes de sécurité et d'épuisement de la

TCAM QoS.

La Figure 1 montre les étapes de programmation des listes de contrôle d'accès dans les tables matérielles du Catalyst 4500.

Figure 1 - Étapes du programme des listes de contrôle d'accès sur les commutateurs Catalyst 4500



Étape 1

Cette étape implique l'une des actions suivantes :

- Configuration et application d'une liste de contrôle d'accès ou d'une politique de qualité de service à une interface ou à un VLANLa création d'une liste de contrôle d'accès peut avoir lieu de manière dynamique. Un exemple est le cas de la fonctionnalité IP Source Guard (IPSG). Avec cette fonctionnalité, le commutateur crée automatiquement une liste de contrôle d'accès pour les adresses IP associées au port.
- Modification d'une liste de contrôle d'accès existante

Remarque : la configuration d'une liste de contrôle d'accès ne génère pas de programmation TCAM. La liste de contrôle d'accès (stratégie QoS) doit être appliquée à une interface afin de programmer la liste de contrôle d'accès dans le TCAM.

Étape 2

La liste de contrôle d'accès doit être fusionnée avant d'être programmée dans les tables matérielles (TCAM). La fusion programme plusieurs ACL (PACL, VACL ou RACL) dans le matériel de manière combinée. De cette manière, une seule recherche matérielle est nécessaire pour vérifier l'ensemble des listes de contrôle d'accès applicables dans le chemin de transfert logique de paquet.

Par exemple, dans la Figure 2, un paquet acheminé de PC-A vers PC-C peut potentiellement avoir ces listes de contrôle d'accès :

- PACL d'entrée sur le port PC-A
- Une VACL sur VLAN 1
- Une RACL d'entrée sur l'interface VLAN 1 dans la direction d'entrée

Ces trois listes de contrôle d'accès sont fusionnées de sorte qu'une seule recherche dans le

TCAM d’entrée soit suffisante pour prendre la décision d’autoriser ou de refuser le transfert. De même, une seule recherche de sortie est nécessaire car le TCAM est programmé avec le résultat fusionné de ces trois listes de contrôle d'accès :

- La sortie RACL sur l'interface VLAN 2
- VACL VLAN 2
- PACL de sortie sur le port PC-C

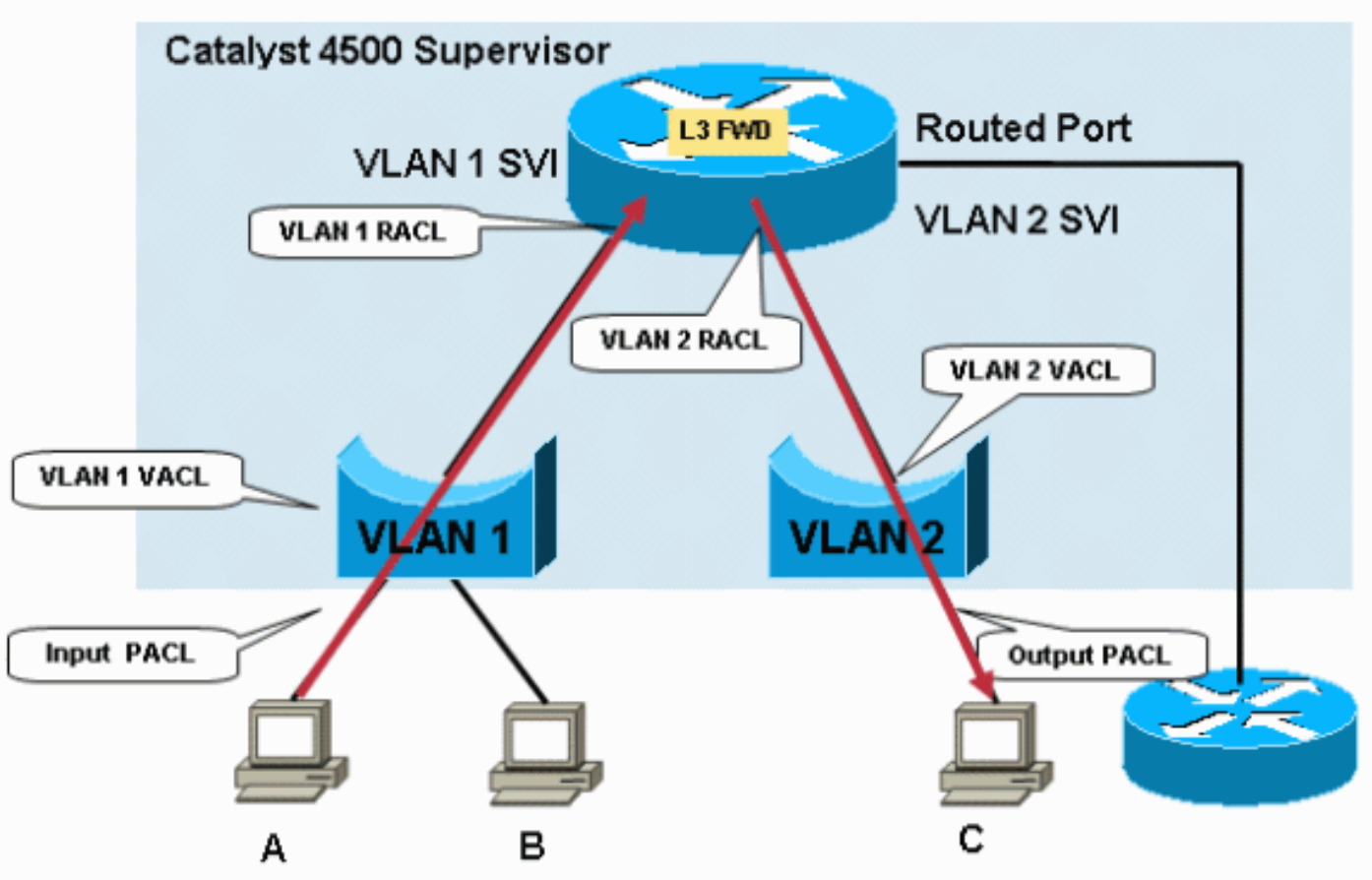
Avec une seule recherche d’entrée et une seule recherche de sortie, il n’y a aucune pénalité dans le transfert matériel des paquets lorsque l’une ou l’autre de ces listes de contrôle d’accès se trouve dans le chemin de transfert de paquets.

Remarque : Les recherches TCAM d'entrée et de sortie se produisent en même temps dans le matériel. Une erreur commune est que la recherche TCAM de sortie se produit après la recherche TCAM d'entrée, comme le suggère le flux de paquets logique. Ces informations sont importantes à comprendre car la stratégie de sortie Catalyst 4500 ne peut pas correspondre aux paramètres QoS modifiés de la stratégie d'entrée. Dans le cas d'une liste de contrôle d'accès de sécurité, l'action la plus sévère se produit. Le paquet est abandonné dans l'une ou l'autre des situations suivantes :

- Si le résultat de la recherche d'entrée est ignoré et que le résultat de la recherche de sortie est autorisé
- Si le résultat de la recherche d'entrée est autorisé et le résultat de la recherche de sortie est ignoré

Remarque : le paquet est autorisé si les résultats de la recherche d'entrée et de sortie sont autorisés.

Figure 2 : filtrage via des listes de contrôle d'accès de sécurité sur les commutateurs Catalyst 4500



La fusion des listes de contrôle d'accès sur le Catalyst 4500 dépend de l'ordre. Le processus est également appelé fusion dépendante des commandes (ODM). Avec ODM, les entrées de liste de contrôle d'accès sont programmées dans l'ordre dans lequel elles apparaissent dans la liste de contrôle d'accès. Par exemple, si une liste de contrôle d'accès contient deux entrées de contrôle d'accès (ACE), le commutateur programme d'abord ACE 1, puis ACE 2. Cependant, la dépendance de l'ordre n'est qu'entre les ACE d'une liste de contrôle d'accès spécifique. Par exemple, les ACE de la liste de contrôle d'accès 120 peuvent commencer avant les ACE de la liste de contrôle d'accès 100 dans la TCAM.

Étape 3

La liste de contrôle d'accès fusionnée est programmée dans le TCAM. La TCAM d'entrée ou de sortie pour ACL ou QoS est divisée en deux régions : PortAndVlan et PortOrVlan. La liste de contrôle d'accès fusionnée est programmée dans la région PortAndVlan de la TCAM si une configuration comporte *les deux* listes de contrôle d'accès dans le même chemin de paquet :

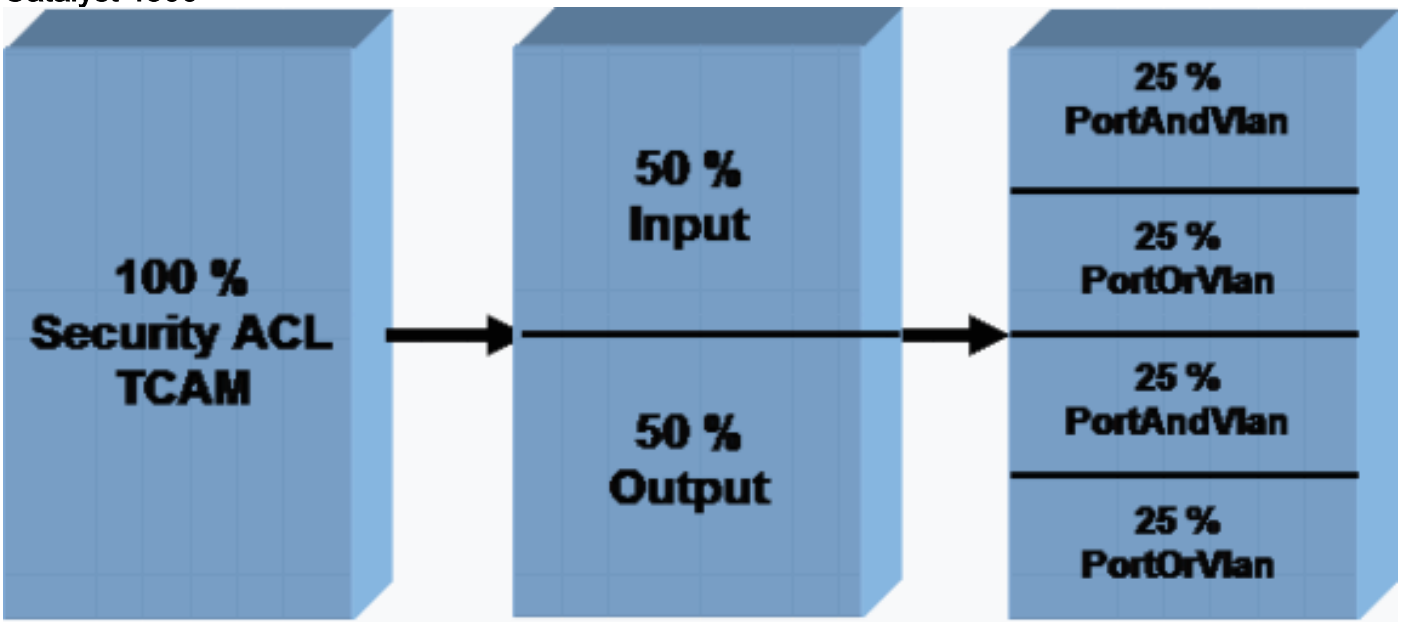
- UN PACL**Remarque :** la liste de contrôle d'accès (PACL) est une liste de contrôle d'accès de filtrage normale ou une liste de contrôle d'accès dynamique créée par IPSG.
- VACL ou RACL

Une liste de contrôle d'accès est programmée dans la région PortOrVlan de la TCAM si un chemin particulier du paquet ne comporte qu'une liste de contrôle d'accès (PACL), une liste de contrôle d'accès (VACL) ou une liste de contrôle d'accès (RACL). La Figure 3 illustre le découpage TCAM des listes de contrôle d'accès de sécurité pour différents types de listes de contrôle d'accès. La QoS a une TCAM dédiée, séparée et taillée de la même manière.

Actuellement, vous ne pouvez pas modifier l'allocation TCAM par défaut. Cependant, il est prévu de fournir la possibilité de modifier l'allocation TCAM disponible pour les régions PortAndVlan et PortOrVlan dans les versions logicielles futures. Cette modification vous permettra d'augmenter ou de diminuer l'espace pour PortAndVlan et PortOrVlan dans les TCAM d'entrée ou de sortie.

Remarque : Toute augmentation de l'allocation pour la région PortAndVlan entraînera une diminution équivalente pour la région PortOrVlan dans le TCAM d'entrée ou de sortie.

Figure 3 - Structure TCAM des listes de contrôle d'accès de sécurité sur les commutateurs Catalyst 4500



La commande **show platform hardware ACL statistics use brief** affiche cette utilisation TCAM par région pour les TCAM ACL et QoS. Le résultat de la commande montre les masques et les entrées disponibles et les divise par région, comme dans la Figure 3. Cet exemple de sortie provient d'un Supervisor Engine II+ Catalyst 4500 :

Remarque : Reportez-vous à la section Types de TCAM de ce document pour plus d'informations sur les masques et les entrées.

```
Switch#show platform hardware acl statistics utilization brief
                                      Entries/Total(%)  Masks/Total(%)
                                     -----------------  ---------------
            Input  Acl(PortAndVlan)  2016 / 4096 ( 49)   252 /  512 ( 49)
            Input  Acl(PortOrVlan)      6 / 4096 (  0)     5 /  512 (  0)
            Input  Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Input  Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Acl(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortAndVlan)     0 / 4096 (  0)     0 /  512 (  0)
            Output Qos(PortOrVlan)      0 / 4096 (  0)     0 /  512 (  0)
            L4Ops: used 2 out of 64
```

Types de TCAM

Le Catalyst 4500 utilise deux types de TCAM, comme le montre le tableau 2. Cette section présente la différence entre les deux versions TCAM afin que vous puissiez sélectionner le produit approprié pour votre réseau et votre configuration.

TCAM 2 utilise une structure dans laquelle huit entrées partagent un masque. Par exemple, huit adresses IP dans les ACE. Les entrées doivent avoir le même masque que le masque qu'elles partagent. Si les ACE ont des masques différents, les entrées doivent utiliser des masques séparés si nécessaire. Cette utilisation de masques séparés peut entraîner une épuisement des masques. L'épuisement des masques dans la TCAM est l'une des raisons courantes de l'épuisement de la TCAM.

TCAM 3 n'a aucune restriction de ce type. Chaque entrée peut avoir son propre masque unique dans le TCAM. L'utilisation complète de toutes les entrées disponibles dans le matériel est possible, quel que soit le masque de ces entrées.

Afin de démontrer cette architecture matérielle, l'exemple de cette section montre comment une TCAM 2 et une ACL de programme TCAM 3 dans le matériel.

```
access-list 101 permit ip host 8.1.1.1 any
access-list 101 deny ip 8.1.1.0 0.0.0.255 any
```

Cet exemple de liste de contrôle d’accès comporte deux entrées qui ont deux masques différents. L'entrée ACE 1 est une entrée d'hôte et possède donc un masque /32. ACE 2 est une entrée de sous-réseau avec un masque /24. Étant donné que la deuxième entrée a un masque différent, les entrées vides dans le masque 1 ne peuvent pas être utilisées et un masque distinct est utilisé dans le cas du TCAM 2.

Ce tableau montre comment cette liste de contrôle d'accès est programmée dans TCAM 2 :

Masques	Entrées

Masque 1 Correspondance : les 32 bits de l'adresse IP source « Ne vous en souciez pas » : Tous les bits restants	IP source = 8.1.1.1
	Entrée vide 2
	Entrée vide 3
	Entrée vide 4
	Entrée vide 5
	Entrée vide 6
	Entrée vide 7
	Entrée vide 8
Correspondance **du masque 2** : les 24 bits les plus significatifs de l'adresse IP source « Ne vous souciez pas » : Tous les bits restants	IP source = 8.1.1.0
	Entrée vide 2
	Entrée vide 3
	Entrée vide 4
	Entrée vide 5
	Entrée vide 6
	Entrée vide 7

	Entrée vide 8

Même si des entrées gratuites sont disponibles dans le cadre du masque 1, la structure TCAM 2 empêche la population d'ACE 2 dans l'entrée vide 2 pour le masque 1. L'utilisation de ce masque n'est pas autorisée car le masque d'ACE 2 ne correspond pas au masque /32 d'ACE 1. Le TCAM 2 doit programmer l'ACE 2 à l'aide d'un masque distinct, un masque /24.

Cette utilisation d'un masque distinct peut entraîner une épuisement plus rapide des ressources disponibles, comme le montre le tableau 2. Les autres listes de contrôle d'accès peuvent toujours utiliser les entrées restantes du masque 1. Cependant, dans la plupart des cas, l'efficacité de la TCAM 2 est élevée, mais n'est pas de 100 %. L'efficacité varie selon chaque scénario de configuration.

Ce tableau présente la même liste de contrôle d'accès programmée dans le TCAM 3. TCAM 3 alloue un masque pour chaque entrée :

Masques	Entrées
Masque 32 bits pour adresse IP 1	IP source = 8.1.1.1
Masque 24 bits pour adresse IP 2	IP source = 8.1.1.0
Masque vide 3	Entrée vide 3
Masque vide 4	Entrée vide 4
Masque vide 5	Entrée vide 5
Masque vide 6	Entrée vide 6
Masque vide 7	Entrée vide 7
Masque vide 8	Entrée vide 8
Masque vide 9	Entrée vide 9
Masque vide 10	Entrée vide 10
Masque vide 11	Entrée vide 11
Masque vide 12	Entrée vide 12
Masque vide 13	Entrée vide 13
Masque vide 14	Entrée vide 14
Masque vide 15	Entrée vide 15
Masque vide 16	Entrée vide 16

Dans cet exemple, les 14 entrées restantes peuvent chacune avoir des entrées avec différents masques, sans restrictions. Par conséquent, la TCAM 3 est beaucoup plus efficace que la TCAM 2. Cet exemple est trop simplifié pour illustrer la différence entre les versions TCAM. Le logiciel Catalyst 4500 dispose de nombreuses optimisations pour augmenter l'efficacité de la programmation dans TCAM 2 pour un scénario de configuration pratique. La section Suboptimal TCAM Programming Algorithm for TCAM 2 de ce document traite de ces optimisations.

Pour TCAM 2 et TCAM 3 sur Catalyst 4500, les entrées TCAM sont partagées si la même liste de contrôle d'accès est appliquée à différentes interfaces. Cette optimisation permet d'économiser de l'espace TCAM.

Dépannage de l'épuisement TCAM

Lorsque la TCAM est épuisée sur les commutateurs Catalyst 4500 lors de la programmation d'une liste de contrôle d'accès de sécurité, une application partielle de la liste de contrôle d'accès se produit via le chemin logiciel. Les paquets qui correspondent aux ACE qui ne sont pas appliqués dans le TCAM sont traités dans le logiciel. Ce traitement dans le logiciel entraîne une utilisation élevée du CPU. Comme la programmation de la liste de contrôle d'accès Catalyst 4500 dépend de l'ordre, la liste de contrôle d'accès est toujours programmée de haut en bas. Si une liste de contrôle d'accès spécifique ne s'intègre pas entièrement à la TCAM, les entrées de contrôle d'accès situées en bas de la liste de contrôle d'accès ne sont probablement pas programmées dans la TCAM.

Un message d'avertissement apparaît lorsqu'un dépassement de TCAM se produit. Voici un exemple :

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
Security: 140 - insufficient hardware TCAM masks.
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing will be software switched.
```

Vous pouvez également voir ce message d'erreur dans la sortie de la commande **show logging** si vous avez activé syslog. La présence de ce message indique de manière concluante qu'un certain traitement logiciel aura lieu. Par conséquent, il peut y avoir une utilisation élevée du CPU. La liste de contrôle d'accès qui a déjà été programmée dans la TCAM reste programmée dans la TCAM si la capacité de la TCAM est épuisée lors de l'application de la nouvelle liste de contrôle d'accès. Les paquets qui correspondent aux listes de contrôle d'accès qui ont déjà été programmées continuent d'être traités et transférés dans le matériel.

Remarque : si vous apportez des modifications à une liste de contrôle d'accès de grande taille, le message TCAM dépassé peut s'afficher. Le commutateur tente de reprogrammer la liste de contrôle d'accès dans TCAM. Dans la plupart des cas, la nouvelle liste de contrôle d'accès modifiée peut être entièrement reprogrammée dans le matériel. Si le commutateur peut reprogrammer la liste de contrôle d'accès dans son intégralité dans le TCAM, ce message s'affiche :

```
*Apr 12 08:50:21: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All configured ACLs
now fully loaded in hardware TCAM - hardware switching / QoS restored
```

Utilisez la commande **show platform software acl input summary interface *interface-id*** afin de vérifier que la liste de contrôle d'accès est entièrement programmée dans le matériel.

Ce résultat montre la configuration de la liste de contrôle d'accès 101 vers VLAN 1 et la vérification que la liste de contrôle d'accès est entièrement programmée dans le matériel :

Remarque : si la liste de contrôle d'accès n'est pas entièrement programmée, un message d'erreur TCAM-exhaustion peut s'afficher.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip access-group 101 in
Switch(config-if)#end
Switch#
Switch#show platform software acl input summary interface vlan 1
Interface Name                 : Vl1
  Path(dir:port, vlan)         : (in :null, 1)
```

```
    Current TagPair(port, vlan) : (null, 0/Normal)
    Current Signature           : {FeatureCam:(Security: 101)}
  Type                          : Current
    Direction                   : In
    TagPair(port, vlan)         : (null, 0/Normal)
    FeatureFlatAclId(state)     : 0(FullyLoadedWithToCpuAces)
    QosFlatAclId(state)         : (null)
    Flags                       : L3DenyToCpu
```

Le champ `Flags` (`L3DenyToCpu`) indique que, si un paquet est refusé en raison de la liste de contrôle d'accès, le paquet est pointé vers le processeur. Le commutateur envoie ensuite un message ICMP (Internet Control Message Protocol) inaccessible. Ce comportement est le comportement par défaut. Lorsque les paquets sont transmis au processeur, une utilisation élevée du processeur peut se produire sur le commutateur. Cependant, dans le logiciel Cisco IOS Version 12.1(13)EW et ultérieure, ces paquets sont limités à la vitesse du processeur. Dans la plupart des cas, Cisco vous recommande de désactiver la fonctionnalité qui envoie des messages ICMP inaccessibles.

Ce résultat montre la configuration du commutateur pour ne pas envoyer de messages ICMP inaccessibles et la vérification de la programmation TCAM après la modification. L'état de la liste de contrôle d'accès 101 est désormais `FullyLoaded`, comme le montre le résultat de la commande. Le trafic refusé ne va pas au processeur.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#no ip unreachables
Switch(config-if)#end

Switch#show platform software acl input summary interface vlan 1
Interface Name                : Vl1
  Path(dir:port, vlan)        : (in :null, 1)
    Current TagPair(port, vlan) : (null, 1/Normal)
    Current Signature           : {FeatureCam:(Security: 101)}
  Type                          : Current
    Direction                   : In
    TagPair(port, vlan)         : (null, 1/Normal)
    FeatureFlatAclId(state)     : 0(FullyLoaded)
    QosFlatAclId(state)         : (null)
    Flags                       : None
```

Remarque : si la TCAM QoS est dépassée lors de l'application d'une certaine stratégie QoS, cette stratégie spécifique *n*'est *pas* appliquée à l'interface ou au VLAN. Le Catalyst 4500 n'implémente pas la stratégie QoS dans le chemin du logiciel. Par conséquent, l'utilisation du CPU ne augmente pas lorsque la TCAM QoS est dépassée.

```
*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERR: Input Policy Map: 10Mbps - hardware TCAM
limit, qos being disabled on relevant interface.

*May 13 08:01:28: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Policy Map: 10Mbps - no
available hardware TCAM entries.
```

Émettez la commande **show platform cpu packet statistics.** Déterminez si la file d'attente de `traitement du logiciel de la liste de contrôle d'accès` reçoit un nombre élevé de paquets. Un nombre élevé de paquets indique l'épuisement du TCAM de sécurité. Cette épuisement de TCAM entraîne l'envoi de paquets au processeur pour le transfert de logiciels.

```
Switch#show platform cpu packet statistics
```

```
!--- Output suppressed. Packets Received by Packet Queue  Queue                  Total
5 sec avg 1 min avg 5 min avg 1 hour avg ---------------------- -------------- --------- ------
--- --------- ---------- Control                        57902635        22         16
12          3 Host Learning                   464678          0          0          0          0 L3
Fwd Low                        623229          0          0          0          0 L2 Fwd
Low                     11267182          7          4          6          1 L3 Rx
High                           508          0          0          0          0 L3 Rx
Low                       1275695         10          1          0          0 ACL
fwd(snooping)               2645752          0          0          0          0 ACL log,
unreach                51443268          9          4          5          5 ACL sw
processing             842889240       1453       1532       1267       1179

Packets Dropped by Packet Queue

Queue                    Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- -------------- --------- --------- --------- ----------
L2 Fwd Low                          3270          0          0          0          0
ACL sw processing                  12636          0          0          0          0
```

Si vous constatez que la file d'attente de `traitement des logiciels de la liste de contrôle d'accès` ne reçoit pas une quantité excessive de trafic, reportez-vous à Utilisation élevée du CPU sur les commutateurs Catalyst 4500 basés sur le logiciel Cisco IOS pour d'autres causes possibles. Ce document fournit des informations sur la façon de dépanner d'autres scénarios d'utilisation élevée du CPU.

Le TCAM Catalyst 4500 peut déborder pour les raisons suivantes :

- Algorithme de programmation TCAM non optimal pour TCAM 2
- Utilisation excessive des opérations de couche 4 (L4Ops) dans une liste de contrôle d'accès
- Listes de contrôle d'accès excessives pour le Supervisor Engine ou le type de commutateur

Algorithme de programmation TCAM sous-optimal pour TCAM 2

Comme le discute la section Types de TCAM, l'efficacité de TCAM 2 est plus faible en raison du fait que huit entrées partagent un masque. Le logiciel Catalyst 4500 permet deux types d'algorithmes de programmation TCAM pour TCAM 2 qui améliorent l'efficacité de TCAM 2 :

- Emballé : adapté à la plupart des scénarios de liste de contrôle d'accès de sécuritéRemarque : il s'agit de la valeur par défaut.
- Scattered : utilisé dans le scénario IPSG

Vous pouvez changer l'algorithme en algorithme dispersé, mais cela n'aide généralement pas si vous avez configuré uniquement des listes de contrôle d'accès de sécurité, telles que les listes RACL. L'algorithme de diffusion n'est efficace que dans les scénarios où la même liste de contrôle d'accès, petite ou similaire, est répétée sur de nombreux ports. Ce scénario est le cas avec une passerelle IPSG activée sur plusieurs interfaces. Dans le scénario IPSG, chaque liste de contrôle d'accès dynamique :

- Possède un petit nombre d'entréesCela inclut les autorisations pour les adresses IP autorisées et un refus à la fin afin d'empêcher l'accès du port par des adresses IP non autorisées.
- Est répété pour tous les ports d'accès configurésLa liste de contrôle d'accès est répétée pour un maximum de 240 ports sur un Catalyst 4507R.

Remarque : TCAM 3 utilise l'algorithme compressé par défaut. Comme la structure TCAM est un masque par entrée, l'algorithme compressé est le meilleur algorithme possible. Par conséquent, l'option d'algorithme dispersé n'est pas activée sur ces commutateurs.

Cet exemple se trouve sur un Supervisor Engine II+ configuré pour la fonctionnalité IPSG. Le résultat montre que, bien que seulement 49 % des entrées soient utilisées, 89 % des masques sont consommés :

```
Switch#show platform hardware acl statistics utilization brief

                                    Entries/Total(%)   Masks/Total(%)
                                   -----------------   ---------------
          Input  Acl(PortAndVlan)  2016 / 4096 ( 49)    460 /  512 ( 89)
          Input  Acl(PortOrVlan)      6 / 4096 (  0)      4 /  512 (  0)
          Input  Qos(PortAndVlan)     0 / 4096 (  0)      0 /  512 (  0)
          Input  Qos(PortOrVlan)      0 / 4096 (  0)      0 /  512 (  0)
          Output Acl(PortAndVlan)     0 / 4096 (  0)      0 /  512 (  0)
          Output Acl(PortOrVlan)      0 / 4096 (  0)      0 /  512 (  0)
          Output Qos(PortAndVlan)     0 / 4096 (  0)      0 /  512 (  0)
          Output Qos(PortOrVlan)      0 / 4096 (  0)      0 /  512 (  0)
          L4Ops: used 2 out of 64
```

Dans ce cas, une modification de l'algorithme de programmation de l'algorithme compressé par défaut à l'algorithme dispersé vous aide. L'algorithme dispersé réduit l'utilisation totale du masque de 89 % à 49 %.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list hardware entries scattered
Switch(config)#end
Switch#show platform hardware acl statistics utilization brief

                                    Entries/Total(%)   Masks/Total(%)
                                   -----------------   ---------------
          Input  Acl(PortAndVlan)  2016 / 4096 ( 49)    252 /  512 ( 49)
          Input  Acl(PortOrVlan)      6 / 4096 (  0)      5 /  512 (  0)
          Input  Qos(PortAndVlan)     0 / 4096 (  0)      0 /  512 (  0)
          Input  Qos(PortOrVlan)      0 / 4096 (  0)      0 /  512 (  0)
          Output Acl(PortAndVlan)     0 / 4096 (  0)      0 /  512 (  0)
          Output Acl(PortOrVlan)      0 / 4096 (  0)      0 /  512 (  0)
          Output Qos(PortAndVlan)     0 / 4096 (  0)      0 /  512 (  0)
          Output Qos(PortOrVlan)      0 / 4096 (  0)      0 /  512 (  0)
          L4Ops: used 2 out of 64
```

Pour plus d'informations sur les meilleures pratiques en matière de fonctionnalités de sécurité sur les commutateurs Catalyst 4500, reportez-vous aux Méthodes Recommandées pour les superviseurs des fonctionnalités de sécurité de Catalyst 4500.

Utilisation excessive des L4Ops dans une liste de contrôle d'accès

Le terme L4Ops fait référence à l'utilisation des mots clés **gt**, **lt**, **neq** et **range** dans la configuration de la liste de contrôle d'accès. Le Catalyst 4500 a des limites sur le nombre de ces mots clés que vous pouvez utiliser dans une liste de contrôle d'accès unique. La limite, qui varie selon le Supervisor Engine et le commutateur, est de six ou huit L4Ops par ACL. Le tableau 3 indique la limite par Supervisor Engine et par ACL.

Tableau 3 - Limite L4Op par liste de contrôle d'accès sur différents moteurs de supervision et commutateurs Catalyst 4500

Product (produit)	L4Op
Supervisor Engine II+/ II+TS	32 (6 par liste de contrôle d'accès)

Supervisor Engine III/IV/V et WS-C4948	32 (6 par liste de contrôle d'accès)
Supervisor Engine V-10GE et WS-C4948-10GE	64 (8 par liste de contrôle d'accès)

Si la limite L4Op par liste de contrôle d'accès est dépassée, un message d'avertissement s'affiche sur la console. Le message est similaire à ceci :

```
%C4K_HWACLMAN-4-ACLHWPROGERR: Input Security: severn - hardware TCAM limit, some
packet processing will be software switched.
19:55:55: %C4K_HWACLMAN-4-ACLHWPROGERRREASON: Input Security: severn - hardware TCAM L4
operators/TCP flags usage capability exceeded.
```

En outre, si la limite L4Op est dépassée, l'ACE spécifique est développé dans le TCAM. Résultats d'utilisation TCAM supplémentaires. Cet ACE sert d'exemple :

```
access-list 101 permit tcp host 8.1.1.1 range 10 20 any
```

Avec cet ACE dans une liste de contrôle d'accès, le commutateur utilise une seule entrée et une L4Op. Cependant, si six L4Ops sont déjà utilisés dans cette liste de contrôle d'accès, cette ACE est étendue à 10 entrées dans le matériel. Une telle extension peut potentiellement utiliser beaucoup d'entrées dans la TCAM. Une utilisation prudente de ces L4Ops empêche le débordement TCAM.

Remarque : si ce cas concerne les moteurs de supervision Supervisor Engine V-10GE et WS-C4948-10GE, huit opérations L4Ops précédemment utilisées dans la liste de contrôle d'accès aboutissent à une extension ACE.

Gardez ces éléments à l'esprit lorsque vous utilisez L4Op sur des commutateurs Catalyst 4500 :

- Les opérations de couche 4 sont considérées comme différentes si l'opérateur ou l'opérande diffèrent.Par exemple, cette liste de contrôle d'accès contient trois opérations de couche 4 différentes, car **gt 10** et **gt 11** sont considérées comme deux opérations de couche 4 différentes :
  ```
  access-list 101 permit tcp host 8.1.1.1 any gt 10
  access-list 101 deny tcp host 8.1.1.2 any lt 9
  access-list 101 deny tcp host 8.1.1.3 any gt 11
  ```
- Les opérations de couche 4 sont considérées comme différentes si le même opérateur/couple opératoire s'applique une fois à un port source et une fois à un port de destination.Voici un exemple :
  ```
  access-list 101 permit tcp host 8.1.1.1 gt 10 any
  access-list 101 permit tcp host 8.1.1.2 any gt 10
  ```
- Les commutateurs Catalyst 4500 partagent les L4Ops lorsque cela est possible.Dans cet exemple, les lignes en ***caractères gras en italique*** montrent ce scénario :Utilisation L4Op pour ACL 101 = 5Utilisation L4Op pour ACL 102 = 4 **Remarque :** Le mot clé **eq** ne consomme aucune ressource matérielle L4Op.Utilisation totale des L4Op = 8**Remarque :** les listes de contrôle d'accès 101 et 102 partagent une opération L4Op.**Remarque :** L4Op est partagé même si le protocole, tel que TCP ou UDP (User Datagram Protocol), ne correspond pas ou si l'action permit/deny ne correspond pas.

Listes de contrôle d'accès excessives pour le Supervisor Engine ou le type de commutateur

Comme le montre le tableau 2, la TCAM est une ressource limitée. Vous pouvez dépasser la ressource TCAM de n'importe quel Supervisor Engine si vous configurez des listes de contrôle d'accès excessives ou des fonctionnalités comme IPSG avec un nombre élevé d'entrées IPSG.

Si vous dépassez l'espace TCAM de votre Supervisor Engine, procédez comme suit :

- Si vous disposez d'un Supervisor Engine II+ et que vous exécutez une version du logiciel Cisco IOS *antérieure* à la version 12.2(18)EW du logiciel Cisco IOS, effectuez une mise à niveau vers la dernière version de maintenance du logiciel Cisco IOS version 12.2(25)EWA.La capacité TCAM a été augmentée dans les versions ultérieures.
- Si vous utilisez la surveillance DHCP et IPSG et que vous commencez à manquer de TCAM, utilisez la dernière version de maintenance EWA du logiciel Cisco IOS version 12.2(25)et utilisez l'algorithme de diffusion dans le cas des produits TCAM 2.**Remarque :** L'algorithme diffusé est disponible dans le logiciel Cisco IOS Version 12.2(20)EW et ultérieure.La dernière version offre également des améliorations pour une meilleure utilisation de TCAM avec la surveillance DCHP et les fonctions DAI (Dynamic Address Resolution Protocol).
- Si vous commencez à manquer de TCAM parce que la limite L4Op est dépassée, essayez de réduire l'utilisation L4Op dans la liste de contrôle d'accès afin d'empêcher le débordement TCAM.
- Si vous utilisez de nombreuses listes de contrôle d'accès ou politiques similaires sur différents ports du même VLAN, agrégez-les en une seule liste de contrôle d'accès ou stratégie sur l'interface VLAN.Cette agrégation économise un peu d'espace TCAM. Par exemple, lorsque vous appliquez des politiques basées sur la voix, la QoS basée sur les ports par défaut est utilisée pour la classification. Cette QoS par défaut peut entraîner un dépassement de la capacité TCAM. Si vous basez la QoS sur VLAN, vous réduisez l'utilisation de TCAM.
- Si vous avez encore des problèmes avec l'espace TCAM, pensez à un Supervisor Engine haut de gamme, tel que le Supervisor Engine V-10GE ou le Catalyst 4948-10GE.Ces produits utilisent le matériel TCAM 3 le plus efficace.

Résumé

Le Catalyst 4500 programme les listes de contrôle d’accès configurées à l’aide de la TCAM. Le TCAM permet l'application des listes de contrôle d'accès dans le chemin de transfert matériel sans impact sur les performances du commutateur. La performance est constante quelle que soit la taille de l'ACL car la performance des recherches ACL est à plein débit. Cependant, TCAM n'est pas une ressource inépuisable. Par conséquent, si vous configurez un nombre excessif d'entrées ACL, vous dépasserez la capacité TCAM. Le Catalyst 4500 a mis en oeuvre de nombreuses optimisations et fourni des commandes pour modifier l'algorithme de programmation de TCAM afin d'atteindre une efficacité maximale. Les produits TCAM 3 tels que Supervisor Engine V-10GE et Catalyst 4948-10GE offrent le plus de ressources TCAM pour les stratégies de sécurité ACL et QoS.

Informations connexes

- Pages de support pour les produits LAN

- Page de support sur la commutation LAN
- Support et documentation techniques - Cisco Systems