# Vermijding van TCAM-expressie voor ACL en QoS op Catalyst 4500 Switches

## Inhoud



## Inleiding

Switches van Cisco Catalyst 4500 en Catalyst 4948 Series ondersteunen de controlelijst voor toegang via bedrading (ACL) en QoS-functie met gebruik van het adresseerbare geheugen (TCAM) voor content. Het inschakelen van ACL's en beleid verlaagt de switching- of routingprestaties van de switch niet zolang de ACL's volledig geladen zijn in de TCAM. Als de TCAM is uitgeput, kunnen de pakketten via het CPU-pad worden verzonden, waardoor de prestaties voor die pakketten kunnen worden verminderd. Dit document bevat informatie over:

- De verschillende soorten TCAM die Catalyst 4500 en Catalyst 4948 gebruiken
- Hoe Catalyst 4500 de TCAM's programmeert
- Configureer de ACL's en TCAM op de switch optimaal om uitputting van de TCAM-module te voorkomen

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 4500 Series switches
- Catalyst 4948 Series switches

**Opmerking:** Dit document is alleen van toepassing op Cisco IOS® software-gebaseerde switches en is niet van toepassing op Catalyst OS (CatOS)-gebaseerde switches.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

# Achtergrondinformatie

Om de verschillende typen ACL's en QoS-beleid in hardware te implementeren, dienen de Catalyst 4500-programma's hardware lookup-tabellen (TCAM) en verschillende hardwareregisters in de Supervisor Engine te worden geïnstalleerd. Wanneer een pakket arriveert, voert de switch een hardware-tabel raadpleging (TCAM lookup) uit en besluit het pakket toe te staan of te ontkennen.

Catalyst 4500 ondersteunt verschillende typen ACL's. Tabel 1 beschrijft deze typen ACL's.

**Tabel 1 - Typen ACL's die worden ondersteund op Catalyst 4500 Switches**

| ACL-type | indien van toepassing | Beperkt verkeer | Richting |
|---|---|---|---|
| RACL[1] | L3[2]-poort, L3-kanaal of SVI[3] (VLAN) | Routed IP-verkeer | In of uit |
| VACL[4] | VLAN (via de opdracht **VLAN**-filter) | Alle pakketten die in of uit een VLAN worden routed of die binnen een VLAN worden overbrugd | directioneel |
| PACL[5] | L2[6]-poort of L2-kanaal | Alle IP-verkeer en niet-IPv4[7]-verkeer (via MAC) | In of uit |

[1] RACL = router ACL

[2] L3 = Layer 3

[3] SVI = switched virtuele interface

[4] VACL = VLAN ACL

[5] PACL = poort

[6] L2 = Layer 2

[7] IPv4 = IP, versie 4

## Catalyst 4500 ACL en QoS hardware-programmeerarchitectuur

Catalyst 4500 TCAM heeft het volgende aantal items:

- 32.000 items voor security ACL, die ook bekend staat als optie ACL
- 32.000 items voor QoS ACL

Voor zowel security ACL als QoS ACL, worden de ingangen op de volgende manier toegewezen:

- 16.000 items voor de invoerrichting
- 16.000 items voor de uitvoerrichting

Afbeelding 3 toont de toewijding van de binnenkomst TCAM. Zie de sectie Typen van CAM voor meer informatie over CAMs.

Tabel 2 toont de ACL-bronnen die beschikbaar zijn voor diverse Catalyst 4500 Supervisor Engine en switches.

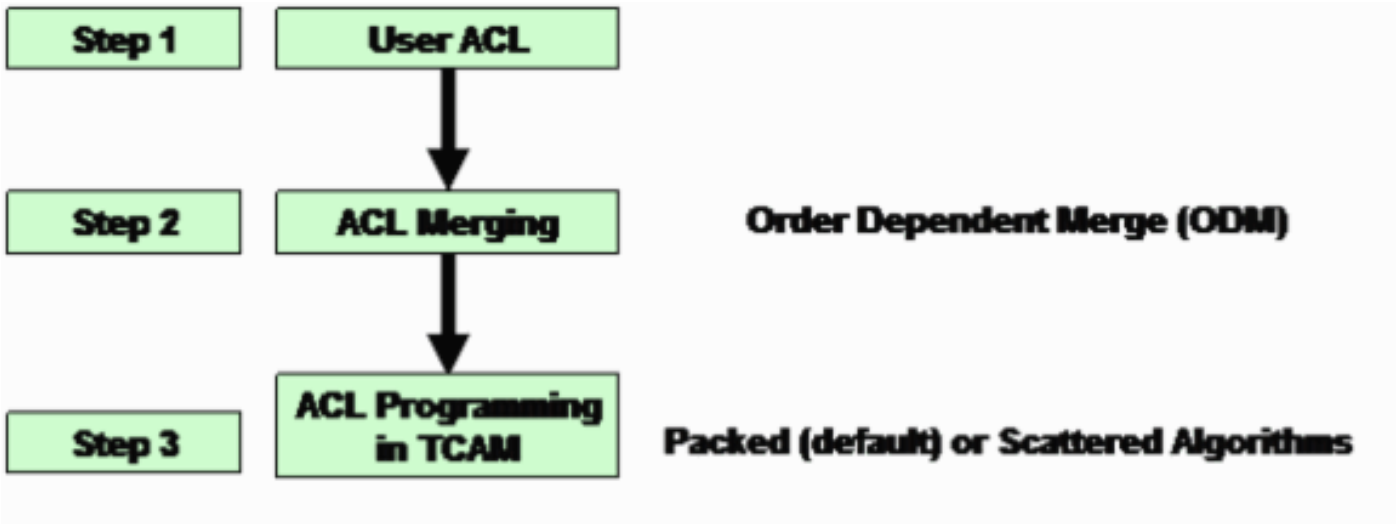
**Tabel 2 - Catalyst 4500 ACL-bronnen op diverse Supervisor Engine en Switches**

| Product | TCAM-versie | TCAM-functies (per richting) | QoS-CAM (per richting) |
|---|---|---|---|
| Supervisor Engine II+ | 2 | 8000 ingangen, 1000 maskers | 8000 ingangen, 1000 maskers |
| Supervisor Engine II+TS/III/IV/V en WS-C4948 | 2 | 16.000 lemma's, 2.000 | 16.000 lemma's, 2.000 |
| Supervisor Engine V-10GE en WS-C4948-10 GE | 3 | 16.000 items, 16.000 maskers | 16.000 items, 16.000 maskers |

Catalyst 4500 gebruikt afzonderlijke, toegewijde CAM's voor IP-unicast en multicast routing. Catalyst 4500 kan tot 128.000 routeingangen hebben die het unicast en de multicast routes delen. Deze details vallen echter buiten het toepassingsgebied van dit document. In dit document worden alleen kwesties behandeld met betrekking tot de beveiliging en de QoS-uitputting.

Afbeelding 1 toont de stappen om de ACL's in hardwaretabellen te programmeren op Catalyst 4500.

**Afbeelding 1 - Stappen naar programma ACL's op Catalyst 4500 Switches**




## Stap 1

Deze stap omvat één van deze acties:

- Configuratie en toepassing van een ACL of QoS beleid op een interface of VLANDe creatie van ACL kan dynamisch plaatsvinden. Een voorbeeld is het geval van de IP Source Guard (IPSG) optie. Met deze optie maakt de switch automatisch een PACL-adres (PACL-adres) dat aan de poort is gekoppeld.
- Wijziging van een ACL die reeds bestaat

**Opmerking:** De configuratie alleen van een ACL levert geen TCAM-programma op. Het ACL (QoS-beleid) moet op een interface worden toegepast om de ACL in de TCAM te programmeren.

## Stap 2

ACL moet worden samengevoegd voordat deze in de hardwaretabellen (TCAM) kan worden geprogrammeerd. De fusie programma's meerdere ACL's (PACL, VACL of RACL) op een gecombineerde manier op de hardware. Op deze manier is slechts één hardware raadpleging nodig om alle van toepassing zijnde ACLs in het pakje logisch het verzenden pad te controleren.

In Afbeelding 2 bijvoorbeeld kan een pakket dat van PC-A naar PC-C wordt routeerd deze ACL's hebben:

- Een invoer PACL op de PC-A poort
- Een VACL op VLAN 1
- Een input-RACL op de VLAN 1-interface in de invoerrichting

Deze drie ACL's worden samengevoegd zodat één raadpleging in de input-methode genoeg is om het doorvoerbesluit te nemen om toe te staan of te ontkennen. Op dezelfde manier is slechts één uitgang nodig omdat de TCAM geprogrammeerd is met het samengevoegde resultaat van deze drie ACL's:

- De uitvoer RACL op VLAN 2 interface
- VLAN 2 VACL
- De uitvoer PACL op de PC-C poort

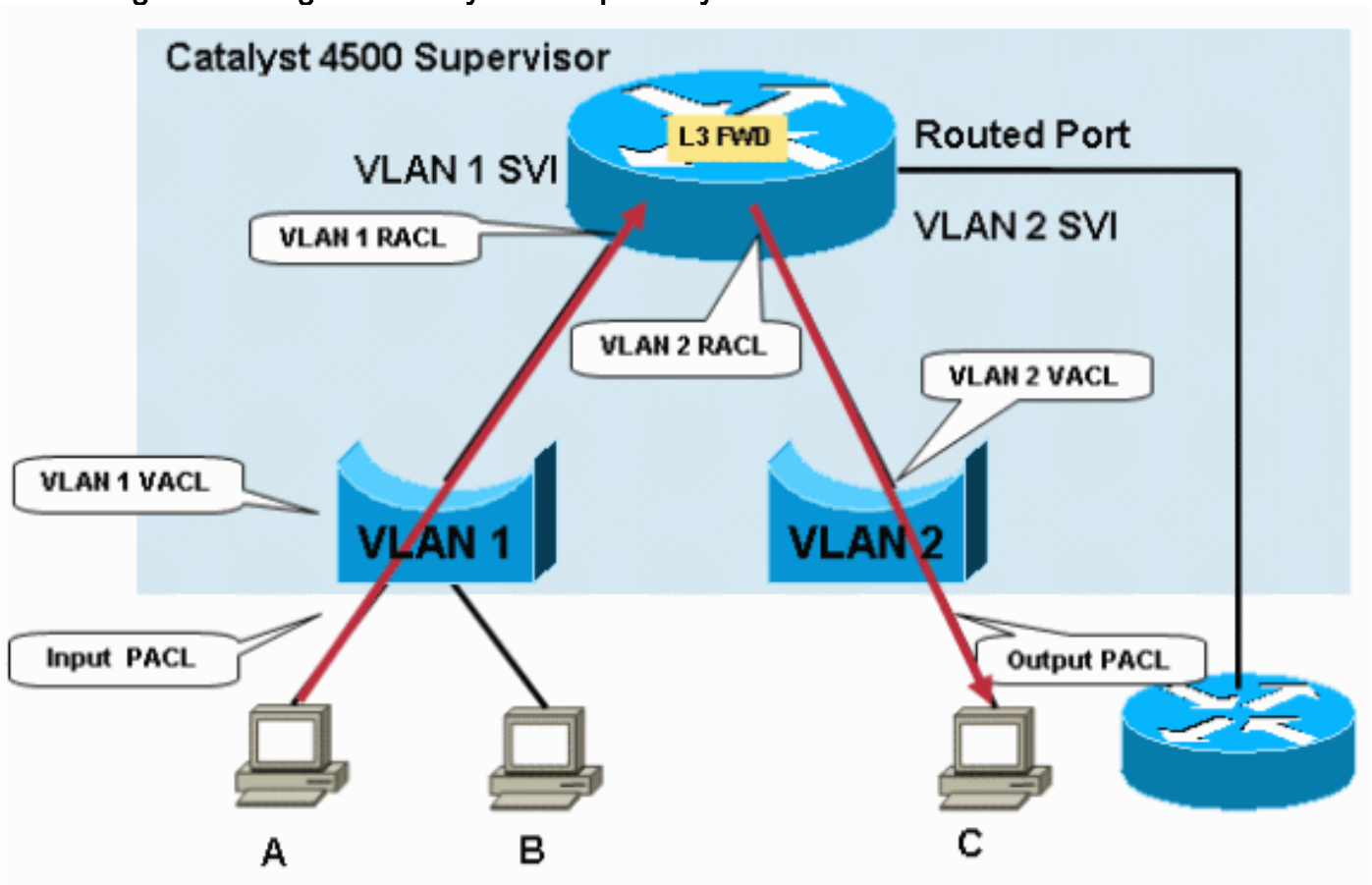
Met één raadpleging voor input en één voor uitvoer, is er geen straf hardware verzending van de pakketten wanneer om het even welke of al deze ACLs in het pakket versturende pad zijn.

**Opmerking:** de TCAM-raadpleging tijdens invoer en uitvoer gebeurt tegelijkertijd in de hardware. Een veel voorkomend misverstand is dat de uitvoer TCAM raadpleging plaatsvindt na de input TCAM raadpleging, zoals de logische pakketstroom suggereert. Deze informatie is belangrijk om te begrijpen omdat het Catalyst 4500 uitvoerbeleid niet kan matchen met door invoerbeleid gewijzigde QoS-parameters. In het geval van security ACL, komt de ernstigste actie voor. Het pakje is in een van deze situaties verbroken:

- Als het resultaat van de raadpleging van de input daalt en het resultaat van de raadpleging van de output is toestaan
- Als het resultaat van de raadpleging van de input toegestaan is en het resultaat van de raadpleging van de uitvoer daalt

**Opmerking:** Het pakket is toegestaan als de resultaten van de invoer- en uitvoerraadpleging toegestaan zijn.

**Afbeelding 2 - Filtering via security ACL's op Catalyst 4500 Switches**




De ACL die op Catalyst 4500 is samengevoegd is van volgorde afhankelijk. Het proces staat ook bekend als order-afhankelijke fusie (ODM). Met ODM worden ACL-items geprogrammeerd in de volgorde waarin ze in de ACL verschijnen. Als een ACL bijvoorbeeld twee toegangscontrolelijsten (ACE's) bevat, worden de switches ACE 1 eerst geprogrammeerd en daarna programma's ACE 2. Echter, de orderafhankelijkheid is alleen tussen ACE's binnen een specifieke ACL. Bijvoorbeeld, kunnen ACEs in ACL 120 beginnen vóór ACEs in ACL 100 in de TCAM.

## Stap 3

De samengevoegde ACL is geprogrammeerd in TCAM. De invoer- of uitvoernetwerkmodule voor ACL of QoS wordt verder gesplitst in twee regio's, PortAndVLAN en PortOfVLAN. De samengevoegde ACL wordt geprogrammeerd in het gebied PortAndVLAN van de TCAM als een

configuratie *beide* van deze ACL's in hetzelfde pakketpad heeft:

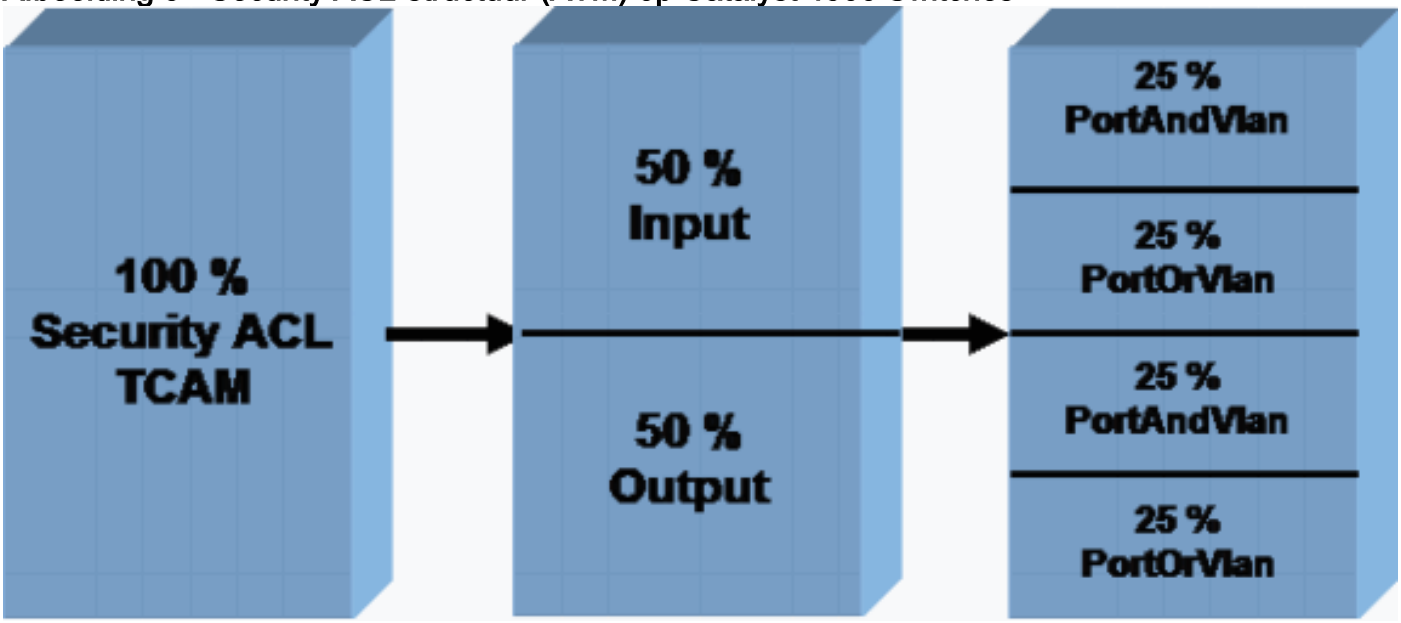
- A PACL**Opmerking:** De PACL is een normale filtering van ACL of door IPSG gemaakte dynamische ACL.
- Een VACL of RACL

Een ACL wordt geprogrammeerd in het gebied PortorVLAN van de TCAM als een bepaald pad van het pakket alleen een PACL of een VACL of een RACL heeft. Afbeelding 3 toont de security ACL-camera voor verschillende typen ACL's. QoS heeft een soortgelijke, afzonderlijke, toegewijde TCAM.

Op dit moment kunt u de standaardtoewijzing voor TCAM niet wijzigen. Er zijn echter plannen om de TCAM-toewijzing te kunnen wijzigen die beschikbaar is voor de regio's PortAndVlan en PortOfVLAN in toekomstige softwarereleases. Deze verandering zal u in staat stellen om de ruimte voor PortAndVLAN en PortOfVLAN in of de input of outputCAMs te vergroten of te verlagen.

**Opmerking:** Elke verhoging van de toewijzing voor het PortandVLAN-gebied zal resulteren in een equivalente afname voor het PortorVLAN-gebied in de input- of output-TCAM.

**Afbeelding 3 - Security ACL-structuur (ATM) op Catalyst 4500 Switches**




Het **korte** bevel van het **platform hardware ACL van de statistiek** van het gebruik van platform toont deze TCAM gebruik per gebied voor zowel ACL als QoS TCAMs. De opdrachtoutput toont de beschikbare maskers en items en verdeelt deze per regio, zoals in afbeelding 3. Deze voorbeelduitvoer is van een Catalyst 4500 Supervisor Engine II+:

**N.B.:** Zie het gedeelte Typen TCAM van dit document voor meer informatie over de maskers en items.

```
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
```

## Typen CAM

Catalyst 4500 gebruikt twee soorten CAM, zoals Tabel 2 laat zien. Deze sectie geeft het verschil weer tussen de twee TCAM-versies zodat u het juiste product kunt selecteren voor uw netwerk- en configuratie.

TCAM 2 gebruikt een structuur waarin acht items één masker delen. Een voorbeeld is acht IP adressen in ACEs. De inzendingen moeten hetzelfde masker hebben als het masker dat ze delen. Als de ACE's verschillende maskers hebben, moeten de ingangen indien nodig afzonderlijke maskers gebruiken. Dit gebruik van aparte maskers kan uitputting veroorzaken. De maskeruitputting in de TCAM is een van de gemeenschappelijke redenen voor de uitputting van de TCAM.

TCAM 3 heeft geen dergelijke beperking. Elke ingang kan zijn eigen uniek masker in de TCAM hebben. Volledig gebruik van alle items die beschikbaar zijn in hardware is mogelijk, ongeacht het masker van die items.

Om deze hardwarearchitectuur te demonstreren, toont het voorbeeld in deze sectie hoe een TCAM 2 en een TCAM 3 programma ACL's in hardware.

```
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
```

Deze steekproef ACL heeft twee ingangen met twee verschillende maskers. ACE 1 is een host entry en dus heeft het een /32 masker. ACE 2 is een netto ingang met een /24 masker. Omdat de tweede ingang een ander masker heeft, kunnen lege ingangen in masker 1 niet worden gebruikt en wordt een afzonderlijk masker gebruikt in het geval van TCAM 2.

Deze tabel laat zien hoe deze ACL in TCAM 2 is geprogrammeerd:

| Maskers | Vermeldingen |
|---|---|
| **masker 1** overeenkomende: alle 32 bits van het IP-bronadres "Geen zorgen": alle resterende bits | Bron IP = 8.1.1.1 |
| | Lege vermelding 2 |
| | Lege vermelding 3 |
| | Lege vermelding 4 |
| | Lege vermelding 5 |
| | Lege vermelding |

| | |
|---|---|
| | 6 |
| | Lege vermelding 7 |
| | Lege vermelding 8 |
| **masker 2** overeenkomend: belangrijkste 24 bits van het IP-bronadres "Geen zorgen": alle resterende bits | Bron IP = 8.1.1.0 |
| | Lege vermelding 2 |
| | Lege vermelding 3 |
| | Lege vermelding 4 |
| | Lege vermelding 5 |
| | Lege vermelding 6 |
| | Lege vermelding 7 |
| | Lege vermelding 8 |

Hoewel er vrije inzendingen beschikbaar zijn als onderdeel van masker 1, voorkomt de structuur van TCAM 2 de populatie van ACE 2 in de lege ingang 2 voor masker 1. Gebruik van dit masker is niet toegestaan omdat het masker van ACE 2 niet overeenkomt met het /32 masker van ACE 1. TCAM 2 moet ACE 2 met een afzonderlijk masker, een /24 masker, programmeren.

Dit gebruik van een afzonderlijk masker kan leiden tot een snellere uitputting van de beschikbare middelen, zoals Tabel 2 laat zien. Andere ACL's kunnen nog steeds de resterende waarden in masker 1 gebruiken. In de meeste gevallen is de efficiëntie van TCAM 2 hoog maar niet 100%. De efficiëntie varieert per configuratiescenario.

Deze tabel toont dezelfde ACL die is geprogrammeerd in TCAM 3. TCAM 3 wijst een masker toe voor elke invoer:

| Maskers | Vermeldingen |
|---|---|
| masker 32 bits voor IP-adres 1 | Bron IP = 8.1.1.1 |
| masker 24 bits voor IP-adres 2 | Bron IP = 8.1.1.0 |

| | |
|---|---|
| Lege masker 3 | Lege vermelding 3 |
| Lege masker 4 | Lege vermelding 4 |
| Lege masker 5 | Lege vermelding 5 |
| Lege masker 6 | Lege vermelding 6 |
| Lege masker 7 | Lege vermelding 7 |
| Leeg masker 8 | Lege vermelding 8 |
| Leeg masker 9 | Lege vermelding 9 |
| Leeg masker 10 | Lege vermelding 10 |
| Leeg masker 11 | Lege vermelding 11 |
| Leeg masker 12 | Lege vermelding 12 |
| Leeg masker 13 | Lege vermelding 13 |
| Leeg masker 14 | Lege vermelding 14 |
| Leeg masker 15 | Lege vermelding 15 |
| Leeg masker 16 | Lege vermelding 16 |

In dit voorbeeld kunnen de 14 resterende inzendingen elk inzendingen met verschillende maskers hebben, zonder beperkingen. Daarom is de TCAM 3 veel efficiënter dan de TCAM 2. Dit voorbeeld wordt overmatig vereenvoudigd om het verschil tussen de TCAM-versies te illustreren. De Catalyst 4500-software heeft talrijke optimalisaties om de efficiëntie van de programmering in TCAM 2 voor een praktisch configuratiescenario te verhogen. In het gedeelte Suboptimal CAM Programming Algorithm voor TCAM 2 in dit document worden deze optimalisaties besproken.

Voor zowel TCAM 2 als TCAM 3 op Catalyst 4500 worden de TCAM-items gedeeld als dezelfde ACL op verschillende interfaces wordt toegepast. Met deze optimalisatie wordt de TCAM-ruimte bespaard.

## Probleemoplossing voor TCAM-ontlading

Wanneer de uitputting van de TCAM op Catalyst 4500 switches plaatsvindt tijdens het programmeren van een security ACL, komt een gedeeltelijke toepassing van ACL via het softwarepad voor. De pakketten die overeenkomen met de ACE's die niet in TCAM worden toegepast worden in software verwerkt. Deze verwerking in software veroorzaakt een hoog CPU-gebruik. Omdat de programma's van Catalyst 4500 ACL van volgorde afhankelijk zijn, wordt ACL altijd van bovenaf geprogrammeerd. Als een specifieke ACL niet geheel in de TCAM past, worden de ACE's bij het onderste gedeelte van ACL waarschijnlijk niet geprogrammeerd in de TCAM.

Er verschijnt een waarschuwingsbericht als er een TCAM-overloop optreedt. Hierna volgt een voorbeeld:

```
%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.
```

U kunt deze foutmelding ook zien in de opdrachtoutput **van** de **show** houtkap als u syslog hebt ingeschakeld. De aanwezigheid van dit bericht geeft aan dat er software zal worden verwerkt. Bijgevolg kan er een hoog CPU-gebruik zijn. De ACL die al in de TCAM is geprogrammeerd, blijft geprogrammeerd in TCAM indien de uitputting van de TCAM-capaciteit optreedt tijdens de toepassing van de nieuwe ACL. De pakketten die overeenkomen met de ACL's die reeds

geprogrammeerd zijn worden verwerkt en in hardware doorgestuurd.

**N.B.:** Als u wijzigingen in een grote ACL aanbrengt, kan het TCAM-overtrokken bericht worden weergegeven. De switch probeert ACL in TCAM te herprogrammeren. In de meeste gevallen, kan de nieuwe, gewijzigde ACL volledig in hardware worden geherprogrammeerd. Als de switch ACL in zijn geheel kan herprogrammeren in de TCAM, verschijnt dit bericht:

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

Gebruik de opdracht **Show platform software kan interface *interface-id* openen** om te controleren of ACL volledig geprogrammeerd is in hardware.

Deze uitvoer toont de configuratie van ACL 101 aan VLAN 1 en controle dat ACL volledig geprogrammeerd is in hardware:

**Opmerking:** Als de ACL niet volledig geprogrammeerd is, kan een TCAM-uitputting foutmelding worden weergegeven.

```
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
```

Het veld `Vlaggen` (`L3DenyToCpu`) geeft aan dat, als een pakket vanwege de ACL wordt ontkend, het pakket op de CPU wordt gestraft. De switch stuurt dan een onbereikbaar bericht via Internet Control Message Protocol (ICMP). Dit gedrag is de standaard. Wanneer de pakketten op de CPU worden geleid, kan een hoog CPU-gebruik op de switch voorkomen. In Cisco IOS-softwarerelease 12.1(13)EW en later zijn deze pakketten echter beperkt tot de CPU. In de meeste gevallen, raadt Cisco u aan om de optie uit te schakelen die ICMP-onbereikbare berichten verstuurt.

Deze uitvoer toont de configuratie van de switch om ICMP-onbereikbare berichten niet te verzenden en de controle van de TCAM-programmering na de verandering. De status van ACL 101 wordt nu `volledig geladen` zoals de opdrachtoutput toont. Ontkend verkeer gaat niet naar de CPU.

```
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
```

**Opmerking:** Als de QoS-methode tijdens de toepassing van een bepaald QoS-beleid is overschreden, is dat specifieke beleid *niet* van toepassing op de interface of VLAN. Catalyst 4500 voert het QoS-beleid niet op het softwarepad uit. Daarom piekt het CPU-gebruik niet wanneer de QoS-CAM wordt overschreden.

```
*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.
```

Geef de opdracht **voor** de **pakketstatistieken van het platform uit**. Bepaal of de `ACL` sw `verwerkingsrij` een hoog aantal pakketten ontvangt. Een hoog aantal pakketten duidt op de uitputting van de veiligheidstest (CAM). Bij deze uitputting van de TCAM worden pakketten naar de CPU verzonden voor softwareverzending.

```
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
```

Als u vindt dat de `ACL`-verwerkingswachtrij `voor` ACL geen excessieve hoeveelheid verkeer ontvangt, raadpleegt u Gebruik van hoge CPU's op Cisco IOS-softwarerelease 4500 Switches voor andere mogelijke oorzaken. Het document bevat informatie over de manier waarop u andere toepassingsscenario's van hoge CPU's kunt oplossen.

Catalyst 4500 TCAM kan om deze redenen overstromen:

- Een suboptimaal CAM-programmeeralgoritme voor TCAM 2
- Het buitensporige gebruik van Layer 4-bewerkingen (L4Ops) in een
- Extreme ACL's voor Supervisor Engine of switch type

## Suboptimaal CAM-programmeeralgoritme voor TCAM 2

Zoals de sectie Typen van TCAM bespreekt is de efficiëntie van TCAM 2 lager door het feit dat acht ingangen één masker delen. Catalyst 4500-software maakt twee typen TCAM-programmeeralgoritmen mogelijk voor TCAM 2 die de efficiëntie van TCAM 2 verbeteren:

- Packet-Geschikt voor de meeste security ACL-scenario's**Opmerking:** dit is de standaard.
- Gesecreteerd-gebruikt in het IPSG-scenario

U kunt het algoritme in een verspreid algoritme veranderen, maar dit helpt niet typisch als u slechts veiligheid ACLs, zoals RACLs hebt gevormd. Het verspreid algoritme is slechts effectief in scenario's waar het zelfde of een gelijkaardig, klein ACL op talloze havens wordt herhaald. Dit scenario is het geval met een IPSG die op meerdere interfaces wordt geactiveerd. In het IPSG-scenario, elke dynamische ACL:

- Heeft een klein aantal itemsDit omvat vergunningen voor toegestane IP adressen en ontkennen aan het eind om toegang van de haven door onbevoegd IP adressen te verhinderen.
- Wordt herhaald voor alle geconfigureerde toegangspoortenDe ACL wordt herhaald voor maximaal 240 poorten op Catalyst 4507R.

**Opmerking:** TCAM 3 gebruikt de standaard-verpakte algoritme. Omdat de TCAM-structuur één masker per ingang is, is het verpakte algoritme het best mogelijke algoritme. Daarom is de optie verspreid algoritme niet ingeschakeld op deze switches.

Dit voorbeeld is op een Supervisor Engine II+ die voor de IPSG optie is geconfigureerd. De output laat zien dat, alhoewel slechts 49% van de items gebruikt wordt, 89% van de maskers geconsumeerd wordt:

```
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
```

In dit geval, helpt een verandering in het programmeeralgoritme van het standaard verpakte algoritme aan het verspreide algoritme. De verspreide algoritme vermindert het totale gebruik van het masker van 89 tot 49 procent.

```
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
```

Raadpleeg voor informatie over best practices voor beveiligingsfuncties op Catalyst 4500-switches de best practices voor Catalyst 4500 security functies voor toezichthouders.

## Overmatig gebruik van L4Ops in een ACL

Het begrip L4Ops verwijst naar het gebruik van de toetsen **t**, **lt**, **neq** en **bereik** in de ACL-configuratie. Catalyst 4500 heeft limieten op het aantal deze sleutelwoorden die u in één enkele ACL kunt gebruiken. De beperking, die door Supervisor Engine en switch varieert, is of zes of acht L4Ops per ACL. Tabel 3 toont de limiet per Supervisor Engine en per ACL.

**Tabel 3 - L4Op-limiet per ACL op verschillende Catalyst 4500 Supervisor Engine en Switches**

| Product | L4Op |
|---|---|
| Supervisor Engine II+/ II+TS | 32 (6 per ACL) |
| Supervisor Engine III/IV/V en WS-C4948 | 32 (6 per ACL) |
| Supervisor Engine V-10GE en WS-C4948-10 GE | 64 (8 per ACL) |

Als de L4Op limiet per ACL wordt overschreden, wordt er een waarschuwingsbericht op de console weergegeven. Het bericht lijkt hierop:

```
%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.
```

Indien de L4Op-limiet wordt overschreden, wordt het specifieke ACE in de TCAM uitgebreid. Aanvullende TCAM-gebruiksresultaten. Dit ACE is een voorbeeld van:

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

Met dit ACE in ACL gebruikt de switch slechts één ingang en één L4Op. Als echter al zes L4Ops in deze ACL worden gebruikt, wordt deze ACE uitgebreid naar 10 lemma's in de hardware. Een dergelijke uitbreiding kan een heleboel boekingen in de TCAM gebruiken. Voorzichtig gebruik van deze L4Ops voorkomt overflow met TCAM.

**Opmerking:** Als deze case Supervisor Engine V-10GE en WS-C4948-10GE betreft, hebben acht die eerder gebruikte L4Ops in de ACL-resultaten de ACE-uitbreiding tot gevolg.

Houd deze items in gedachten wanneer u L4Op op Catalyst 4500 switches gebruikt:

- L4-activiteiten worden als verschillend beschouwd indien de exploitant of de exploitant verschillen.Dit ACL bevat bijvoorbeeld drie verschillende L4-bewerkingen omdat **gt 10** en **gt 11** als twee verschillende L4-bewerkingen worden beschouwd:
  ```
  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
```

- L4-operaties worden als verschillend beschouwd indien dezelfde exploitant/exploitant-koppel één keer van toepassing is op een bronhaven en één keer op een bestemmingshaven.Hierna volgt een voorbeeld:
```
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
```

- Catalyst 4500 switches delen L4 Mbps wanneer mogelijk.In dit voorbeeld **tonen** de lijnen in ***vet gelaat cursief dit scenario***:L4Op gebruik voor ACL 101 = 5L4Op gebruik voor ACL 102 = 4 **Opmerking:** het **eq** sleutelwoord verbruikt geen van de L4Op hardware-middelen.Totaal L4Op-gebruik = **8Opmerking:** ACL 101 en 102 delen één L4Op.**Opmerking:** L4Op wordt gedeeld zelfs als het protocol, zoals TCP- of User Datagram Protocol (UDP), niet overeenkomt of de licentie/ontkennende actie niet overeenkomt.

## Extreme ACL's voor Supervisor Engine of Switch type

Zoals Tabel 2 laat zien is TCAM een beperkt middel. U kunt de middelen van TCAM van om het even welke Supervisor Engine overschrijden als u buitensporige ACLs of eigenschappen zoals IPSG met een hoog aantal IPSG ingangen vormt.

Als u de TCAM-ruimte voor uw Supervisor Engine overschrijdt, volgt u de volgende stappen:

- Als u een Supervisor Engine II+ hebt en u een Cisco IOS-softwarerelease hebt die *eerder* is dan Cisco IOS-softwarerelease 12.2(18)EW, upgrade naar de nieuwste Cisco IOS-softwarerelease 12.2(25)EWA-onderhoudsrelease.De capaciteit van de TCAM is toegenomen in de latere releases.
- Als u DHCP-snooping en IPSG gebruikt en u start met het verlopen van TCAM, gebruik dan de nieuwste Cisco IOS-softwarerelease 12.2(25)EWA onderhoudsrelease en gebruik het gedistribueerde algoritme in het geval van TCAM 2-producten.**Opmerking:** Het verspreid algoritme is beschikbaar in Cisco IOS-softwarerelease 12.2(20)EW en hoger.De laatste release heeft ook verbeteringen voor een beter TCAM-gebruik met DCHP-snooping en Dynamic Admission Protocol (ARP)-inspectie (DAI).
- Als u geen TCAM meer hebt omdat de L4Op limiet wordt overschreden, probeer dan het gebruik van L4Op in in ACL te verminderen om overloop van TCAM te voorkomen.
- Als u veel soortgelijke ACL's of beleid op verschillende poorten in hetzelfde VLAN gebruikt, aggregeert u deze in één ACL of beleid op de VLAN-interface.Deze aggregatie bespaart enige TCAM-ruimte. Bijvoorbeeld, wanneer u op stem gebaseerd beleid toepast, wordt de standaard op poort gebaseerde QoS gebruikt voor classificatie. Deze standaard QoS kan ertoe leiden dat de CAM-capaciteit wordt overschreden. Als u QoS op VLAN-gebaseerd switches, vermindert u het gebruik van TCAM.
- Als u nog steeds problemen hebt met de ruimte van TCAM, neem dan een end Supervisor Engine in, zoals de Supervisor Engine V-10GE of Catalyst 4948-10GE.Deze producten maken gebruik van de meest efficiënte TCAM 3-hardware.

# Samenvatting

Catalyst 4500 programma's van de geconfigureerde ACL's met gebruik van de TCAM. TCAM

staat toe om ACL's in de hardware-expediteur pad toe te passen zonder invloed op de prestaties van de switch. De prestaties zijn constant ondanks de grootte van ACL omdat de prestaties van de raadpleging van ACL bij lijnsnelheid zijn. TCAM is echter een eindige hulpbron. Daarom, als u een excessief aantal ACL ingangen vormt, overschrijdt u de capaciteit van de TCAM. Catalyst 4500 heeft talrijke optimalisaties geïmplementeerd en heeft opdrachten geleverd om het programmeeralgoritme van TCAM te variëren om een maximale efficiëntie te bereiken. TCAM 3-producten zoals de Supervisor Engine V-10GE en Catalyst 4948-10GE bieden de meeste TCAM-middelen voor security ACL en QoS-beleid.

## Gerelateerde informatie

- Productondersteuningspagina's voor LAN
- Ondersteuningspagina voor LAN-switching
- Technische ondersteuning en documentatie – Cisco Systems