Prevenzione dell'esaurimento di ACL e QoS TCAM sugli switch Catalyst 4500

Sommario

Introduzione

Gli switch Cisco Catalyst serie 4500 e Catalyst serie 4948 supportano la funzionalità wire-rate access control list (ACL) e QoS con l'utilizzo della memoria indirizzabile al contenuto ternario (TCAM). L'abilitazione degli ACL e delle policy non riduce le prestazioni di switching o routing dello switch finché gli ACL sono completamente caricati nel TCAM. Se il TCAM è esaurito, i pacchetti possono essere inoltrati tramite il percorso della CPU, il che può ridurre le prestazioni per quei pacchetti. In questo documento vengono fornite informazioni dettagliate su:

- I diversi tipi di TCAM utilizzati da Catalyst 4500 e Catalyst 4948
- Programmazione dei TCAM con Catalyst 4500
- Configurazione ottimale di ACL e TCAM sullo switch per evitare l'esaurimento del TCAM

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Catalyst serie 4500
- Switch Catalyst serie 4948

Nota: questo documento si applica solo agli switch con software Cisco IOS® e non agli switch con software Catalyst OS (CatOS).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Per implementare i diversi tipi di ACL e policy QoS nell'hardware, i programmi Catalyst 4500 hardware lookup table (TCAM) e vari registri hardware nel Supervisor Engine. Quando arriva un pacchetto, lo switch esegue una ricerca nella tabella dell'hardware (ricerca TCAM) e decide di autorizzare o rifiutare il pacchetto.

Catalyst 4500 supporta diversi tipi di ACL. La tabella 1 illustra questi tipi di ACL.

Tabella 1 - Tipi di ACL supportati sugli switch Catalyst 4500

Tipo ACL	Luogo Di Applicazione	Traffico controllato	Direzione
RACL[1]	Porta L3[2], canale L3 o SVI[3] (VLAN)	Traffico IP di routing	In entrata o in uscita
VACL[4]	VLAN (tramite il comando **vlan filter**)	Tutti i pacchetti instradati in entrata o in uscita da una VLAN o inseriti in una VLAN	Senza direzione
PACL[5]	Porta L2[6] o canale L2	Tutto il traffico IP e il traffico non IPv4[7] (tramite ACL MAC)	In entrata o in uscita

[1] RACL = ACL del router

[2] L3 = Layer 3

[3] SVI = interfaccia virtuale commutata

[4] VACL = ACL VLAN

[5] PACL = ACL della porta

[6] L2 = Layer 2

[7] IPv4 = IP versione 4

Architettura di programmazione hardware Catalyst 4500 ACL e QoS

Catalyst 4500 TCAM presenta il seguente numero di voci:

- 32.000 voci per l'ACL di sicurezza, noto anche come ACL di funzionalità
- 32.000 voci per ACL QoS

Per gli ACL di sicurezza e gli ACL QoS, le voci sono dedicate nel modo seguente:

- 16.000 voci per la direzione di ingresso
- 16.000 voci per la direzione di uscita

La Figura 3 mostra la dedica della voce TCAM. Vedere la sezione Tipi di TCAM per ulteriori informazioni sui TCAM.

La tabella 2 mostra le risorse ACL disponibili per diversi Supervisor Engine e switch Catalyst 4500.

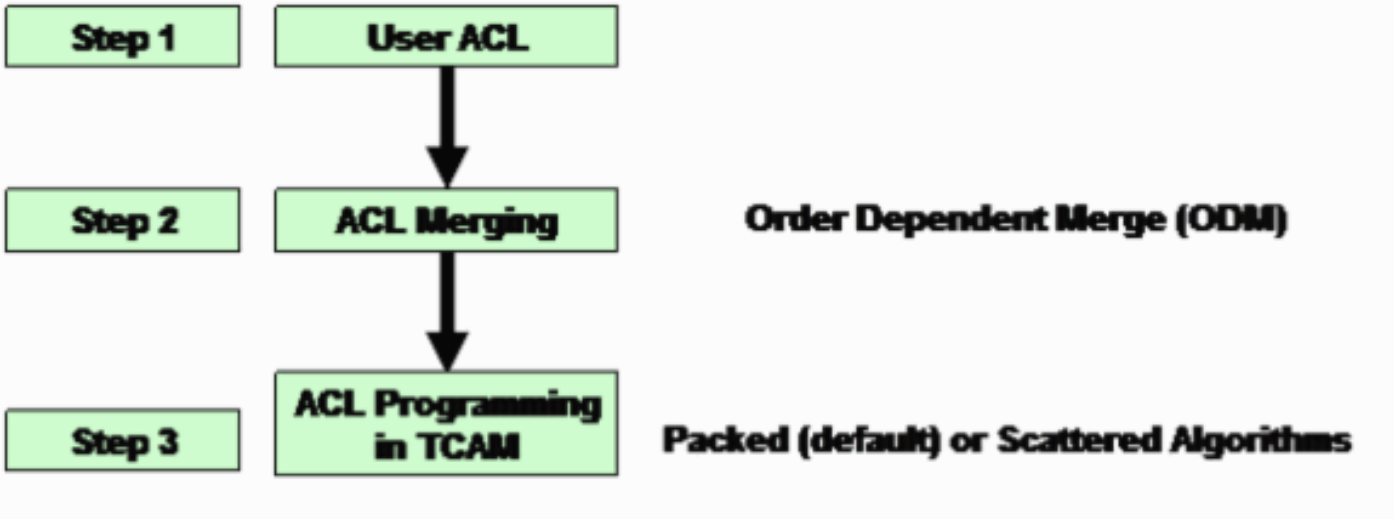
Tabella 2 - Risorse Catalyst 4500 ACL su diversi Supervisor Engine e switch

Prodotto	Versione TCAM	Funzione TCAM (per direzione)	QoS TCAM (per direzione)
Supervisor Engine II+	2	8000 voci, 1000 maschere	8000 voci, 1000 maschere
Supervisor Engine II+TS/III/IV/V e WS-C4948	2	16.000 voci, 2.000 maschere	16.000 voci, 2.000 maschere
Supervisor Engine V-10GE e WS-C4948-10GE	3	16.000 ingressi, 16.000 maschere	16.000 ingressi, 16.000 maschere

Catalyst 4500 utilizza TCAM dedicate e separate per il routing IP unicast e multicast. Catalyst 4500 può avere fino a 128.000 voci di route condivise dalle route unicast e multicast. Tuttavia, questi dettagli esulano dall'ambito di questo documento. In questo documento vengono trattati solo i problemi relativi alla sicurezza e all'esaurimento del QoS TCAM.

Nella figura 1 viene mostrata la procedura per programmare gli ACL nelle tabelle hardware di Catalyst 4500.

Figura 1 - Passi per programmare gli ACL sugli switch Catalyst 4500



Passaggio 1

Questa fase prevede una delle seguenti azioni:

- Configurazione e applicazione di una policy ACL o QoS su un'interfaccia o su una VLANLa creazione degli ACL può avvenire in modo dinamico. Ad esempio, la funzione IP Source Guard (IPSG). Con questa funzione, lo switch crea automaticamente un PACL per gli indirizzi IP associati alla porta.
- Modifica di un ACL già esistente

Nota: la configurazione di un ACL da sola non genera la programmazione TCAM. Per programmare l'ACL nel TCAM, l'ACL (politica QoS) deve essere applicato a un'interfaccia.

Passaggio 2

Prima di poter essere programmato nelle tabelle hardware (TCAM), l'ACL deve essere unito. I programmi uniscono più ACL (PACL, VACL o RACL) nell'hardware in modo combinato. In questo modo, è necessaria una sola ricerca nell'hardware per controllare tutti gli ACL applicabili nel percorso di inoltro logico dei pacchetti.

Ad esempio, nella Figura 2, un pacchetto indirizzato da PC-A a PC-C può avere i seguenti ACL:

- Un PACL di input sulla porta PC-A
- VACL sulla VLAN 1
- Un ingresso RACL sull'interfaccia VLAN 1 nella direzione di input

Questi tre ACL vengono uniti in modo che una singola ricerca nel TCAM di input sia sufficiente per prendere la decisione di inoltro di consentire o negare. Analogamente, è necessaria una sola ricerca in uscita perché il TCAM viene programmato con il risultato dell'unione dei tre ACL:

- L'output RACL sull'interfaccia VLAN 2
- Il VACL VLAN 2
- Il PACL di output sulla porta PC-C

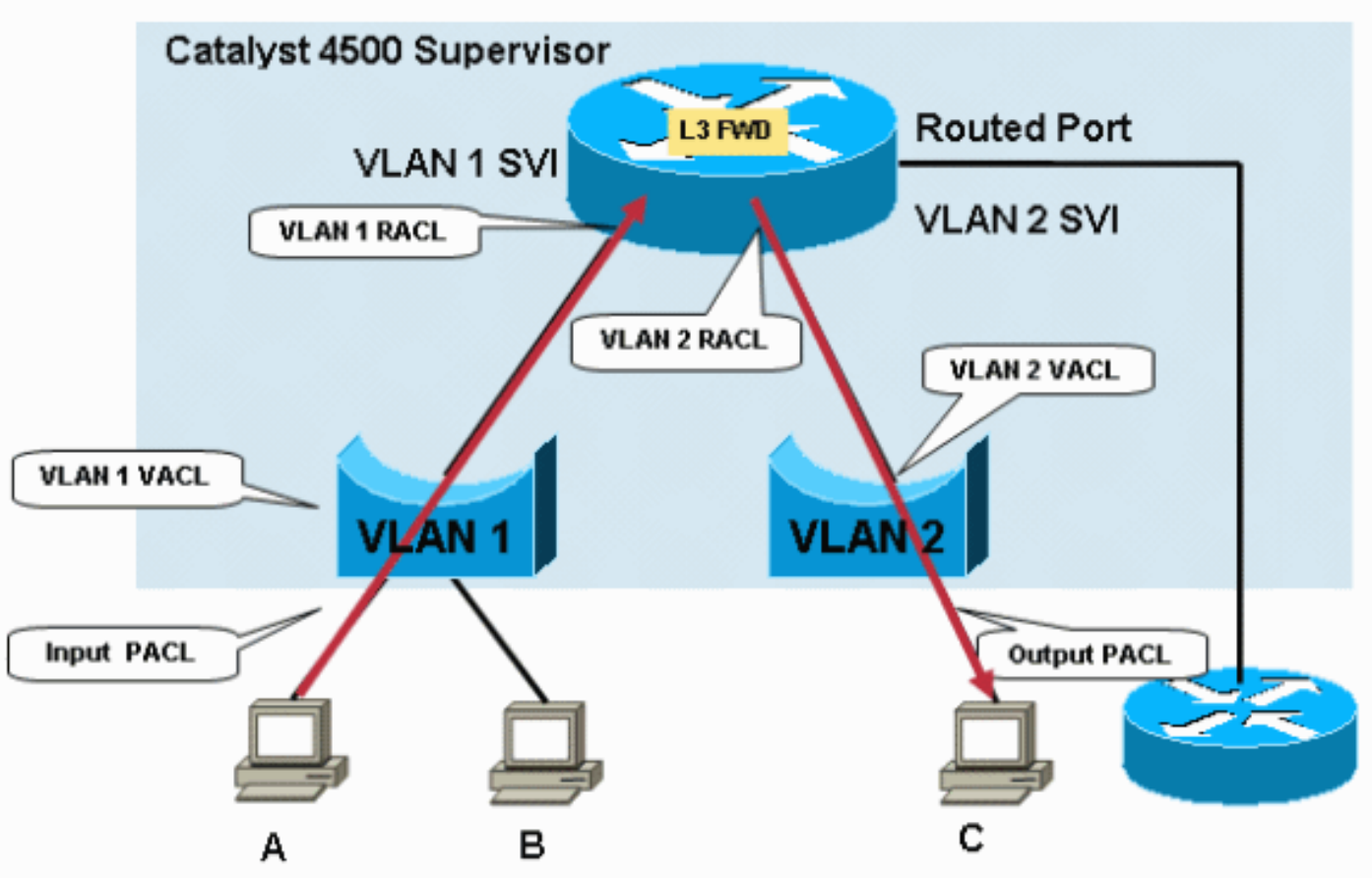
Con una singola ricerca di input e una di output, non c'è penalità nell'inoltro hardware dei pacchetti quando uno o tutti questi ACL sono nel percorso di inoltro dei pacchetti.

Nota: le ricerche TCAM di input e output si verificano contemporaneamente nell'hardware. Un comune fraintendimento è che la ricerca TCAM in output si verifichi dopo la ricerca TCAM in input, come suggerisce il flusso logico del pacchetto. Questa informazione è importante da comprendere perché i criteri di output di Catalyst 4500 non possono corrispondere sui parametri QoS modificati dei criteri di input. Nel caso di ACL di sicurezza, si verifica l'azione più grave. Il pacchetto viene scartato in una di queste situazioni:

- Se il risultato della ricerca di input è drop e il risultato della ricerca di output è allow
- Se il risultato della ricerca di input è permesso e il risultato della ricerca di output è eliminato

Nota: il pacchetto è autorizzato se i risultati della ricerca di input e di output sono consentiti.

Figura 2 - Filtraggio tramite ACL di sicurezza sugli switch Catalyst 4500



L'unione degli ACL su Catalyst 4500 dipende dall'ordine. Questo processo è noto anche come ODM (Order Dependent Merge). Con ODM, le voci ACL vengono programmate nell'ordine in cui appaiono nell'ACL. Ad esempio, se un ACL contiene due voci di controllo di accesso (ACE), lo switch programma prima ACE 1 e poi ACE 2. Tuttavia, la dipendenza dall'ordine è solo tra le ACE all'interno di un ACL specifico. Ad esempio, le voci ACE nell'ACL 120 possono iniziare prima delle voci ACE nell'ACL 100 nella TCAM.

Passaggio 3

L'ACL unito è programmato nel TCAM. Il TCAM di input o output per ACL o QoS viene ulteriormente suddiviso in due aree, PortAndVlan e PortOrVlan. L'ACL unito viene programmato nell'area PortAndVlan del TCAM se una configurazione ha *entrambi* gli ACL nello stesso percorso di pacchetto:

- UN PACL**Nota:** il PACL è un normale ACL filtrante o un ACL dinamico creato da IPSG.

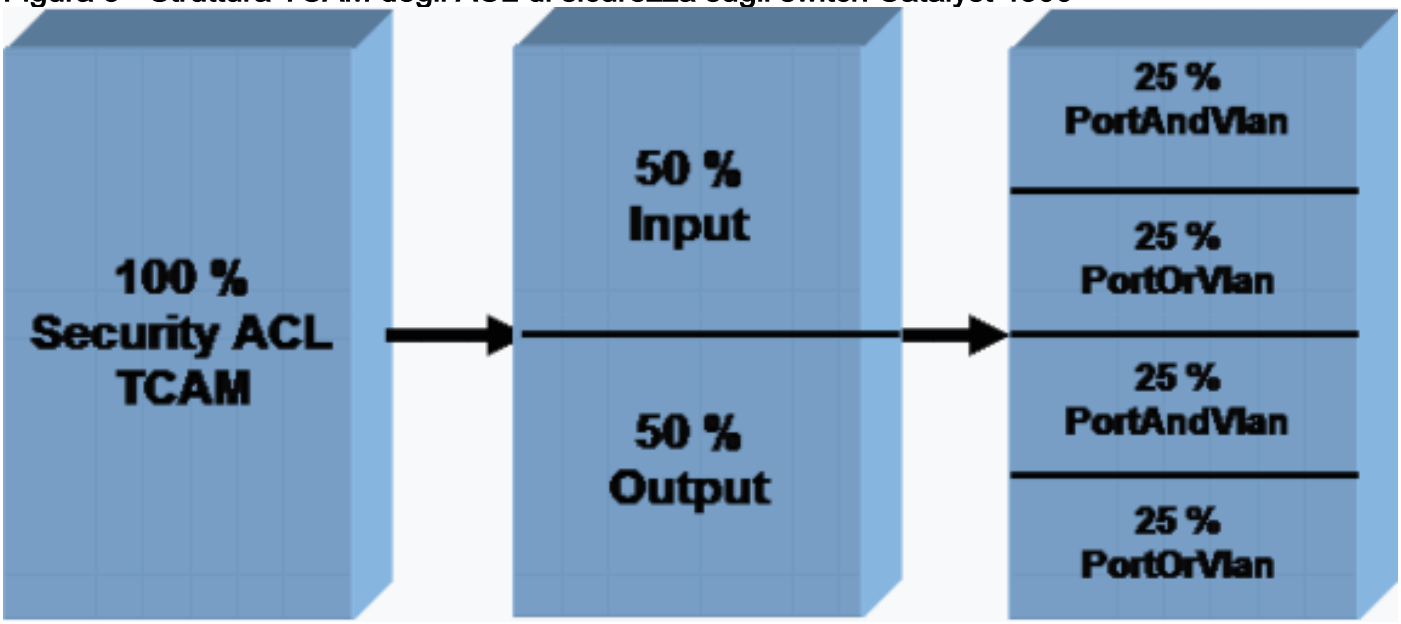
- VACL o RACL

Un ACL viene programmato nella regione PortOrVlan del TCAM se un particolare percorso del pacchetto ha solo un PACL, un VACL o un RACL. Nella figura 3 viene mostrata l'immagine TCAM dell'ACL di sicurezza per diversi tipi di ACL. QoS ha un TCAM dedicato, separato e scolpito in modo simile.

Attualmente non è possibile modificare l'allocazione predefinita TCAM. Tuttavia, è prevista la possibilità di modificare l'allocazione TCAM disponibile per le aree PortAndVlan e PortOrVlan nelle future versioni del software. Questa modifica consente di aumentare o diminuire lo spazio per PortAndVlan e PortOrVlan nelle TCAM di input o di output.

Nota: qualsiasi aumento nell'allocazione per l'area PortAndVlan determinerà una riduzione equivalente per l'area PortOrVlan nel TCAM di input o output.

Figura 3 - Struttura TCAM degli ACL di sicurezza sugli switch Catalyst 4500



Il comando **show platform hardware ACL statistics usage brief** visualizza l'utilizzo del TCAM per area sia per gli ACL che per i TCAM QoS. L'output del comando mostra le maschere e le voci disponibili e le divide per area, come mostrato nella Figura 3. Questo output di esempio è stato generato da un Catalyst 4500 Supervisor Engine II+:

Nota: vedere la sezione Tipi di TCAM di questo documento per ulteriori informazioni sulle maschere e le voci.

```
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
```

Tipi di TCAM

Catalyst 4500 utilizza due tipi di TCAM, come mostrato nella Tabella 2. Questa sezione presenta le differenze tra le due versioni TCAM in modo da poter selezionare il prodotto appropriato per la rete e la configurazione.

TCAM 2 utilizza una struttura in cui otto voci condividono una maschera. Un esempio è costituito da otto indirizzi IP nelle ACE. Le voci devono avere la stessa maschera che condividono. Se le voci ACE hanno maschere diverse, è necessario utilizzare maschere separate in base alle esigenze. L'utilizzo di maschere separate può causare l'esaurimento delle maschere. L'esaurimento della maschera nel TCAM è uno dei motivi più comuni per l'esaurimento del TCAM.

Il CAM 3 non presenta tali limitazioni. Ciascuna voce può avere una maschera univoca nella TCAM. È possibile utilizzare tutte le voci disponibili nell'hardware, indipendentemente dalla maschera di tali voci.

Per dimostrare questa architettura hardware, l'esempio in questa sezione mostra come un TCAM 2 e un TCAM 3 programmano gli ACL nell'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
```

Questo ACL di esempio ha due voci con due maschere diverse. ACE 1 è una voce host e quindi ha una maschera /32. ACE 2 è una voce di subnet con una maschera /24. Poiché la seconda voce ha una maschera diversa, non è possibile utilizzare voci vuote nella Maschera 1 e nel caso di TCAM 2 viene utilizzata una maschera separata.

Nella tabella viene mostrato come questo ACL viene programmato in TCAM 2:

Maschere	Voci
Corrispondenza **maschera 1**: tutti i 32 bit dell'indirizzo IP di origine "Don't care": tutti i bit rimanenti	IP origine = 8.1.1.1
	Voce vuota 2
	Voce vuota 3
	Voce vuota 4
	Voce vuota 5
	Voce vuota 6
	Voce vuota 7
	Voce vuota 8
Corrispondenza **maschera 2**: i 24 bit più significativi dell'indirizzo IP di origine "Don't Care": tutti i bit rimanenti	IP origine = 8.1.1.0

	Voce vuota 2
	Voce vuota 3
	Voce vuota 4
	Voce vuota 5
	Voce vuota 6
	Voce vuota 7
	Voce vuota 8

Anche se sono disponibili voci libere come parte della Maschera 1, la struttura TCAM 2 impedisce la popolazione di ACE 2 nella voce vuota 2 per la Maschera 1. L'uso di questa maschera non è consentito perché la maschera di ACE 2 non corrisponde alla maschera /32 di ACE 1. TCAM 2 deve programmare ACE 2 con l'uso di una maschera separata, una maschera /24.

L'utilizzo di una maschera separata può determinare un più rapido esaurimento delle risorse disponibili, come illustrato nella tabella 2. Gli altri ACL possono ancora usare le voci restanti nella maschera 1. Tuttavia, nella maggior parte dei casi, l'efficienza di TCAM 2 è elevata, ma non è del 100%. L'efficienza varia a seconda dello scenario di configurazione.

Nella tabella viene mostrato lo stesso ACL programmato in TCAM 3. TCAM 3 alloca una maschera per ciascuna voce:

Maschere	Voci
Maschera a 32 bit per l'indirizzo IP 1	IP origine = 8.1.1.1
Maschera 24 bit per l'indirizzo IP 2	IP origine = 8.1.1.0
Maschera vuota 3	Voce vuota 3
Maschera vuota 4	Voce vuota 4
Maschera vuota 5	Voce vuota 5
Maschera vuota 6	Voce vuota 6
Maschera vuota 7	Voce vuota 7
Maschera vuota 8	Voce vuota 8
Maschera vuota 9	Voce vuota 9
Maschera vuota 10	Voce vuota 10
Maschera vuota 11	Voce vuota 11
Maschera vuota 12	Voce vuota 12
Maschera vuota 13	Voce vuota 13
Maschera vuota 14	Voce vuota 14
Maschera vuota 15	Voce vuota 15
Maschera vuota 16	Voce vuota 16

In questo esempio, le 14 voci rimanenti possono avere voci con maschere diverse, senza

restrizioni. Pertanto, il TCAM 3 è molto più efficiente del TCAM 2. Questo esempio è eccessivamente semplificato per illustrare la differenza tra le versioni TCAM. Il software Catalyst 4500 è dotato di numerose ottimizzazioni per aumentare l'efficienza della programmazione in TCAM 2 per uno scenario di configurazione pratico. Nella sezione Algoritmo di programmazione TCAM non ottimale per TCAM 2 di questo documento vengono descritte queste ottimizzazioni.

Sia per TCAM 2 che per TCAM 3 su Catalyst 4500, le voci TCAM vengono condivise se lo stesso ACL viene applicato a interfacce diverse. Questa ottimizzazione consente di risparmiare spazio TCAM.

Risoluzione dei problemi di esaurimento TCAM

Quando si verifica l'esaurimento del TCAM sugli switch Catalyst 4500 durante la programmazione di un ACL di sicurezza, si verifica un'applicazione parziale dell'ACL tramite il percorso software. I pacchetti che corrispondono agli ACE non applicati nel TCAM vengono elaborati nel software. Questa elaborazione nel software causa un elevato utilizzo della CPU. Poiché la programmazione degli ACL di Catalyst 4500 dipende dall'ordine, gli ACL vengono sempre programmati dall'alto verso il basso. Se un ACL specifico non può essere inserito completamente nel TCAM, gli ACE nella parte inferiore dell'ACL molto probabilmente non sono programmati nel TCAM.

Quando si verifica un overflow TCAM, viene visualizzato un messaggio di avvertenza. Di seguito è riportato un esempio:

```
%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.
```

èpossibile visualizzare questo messaggio di errore anche nell'output del comando **show logging** se è stato abilitato syslog. La presenza di questo messaggio indica in modo definitivo che verrà eseguita un'elaborazione del software. Di conseguenza, l'utilizzo della CPU può essere elevato. L'ACL già programmato nel TCAM rimane programmato nel TCAM se la capacità del TCAM si esaurisce durante l'applicazione del nuovo ACL. I pacchetti che corrispondono agli ACL già programmati continuano ad essere elaborati e inoltrati nell'hardware.

Nota: se si apportano modifiche a un ACL di grandi dimensioni, è possibile che venga visualizzato il messaggio TCAM-exceeded (TCAM-exceeded) (TCAM-exceeded) (spazio vuoto). Lo switch cerca di riprogrammare l'ACL in TCAM. Nella maggior parte dei casi, il nuovo ACL modificato può essere riprogrammato completamente nell'hardware. Se lo switch può riprogrammare l'ACL interamente nel TCAM, viene visualizzato questo messaggio:

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

Per verificare che l'ACL sia completamente programmato nell'hardware, usare il comando **show platform software acl input summary interface** *id-interfaccia*.

Questo output mostra la configurazione di ACL 101 sulla VLAN 1 e la verifica che l'ACL sia interamente programmato nell'hardware:

Nota: se l'ACL non è completamente programmato, potrebbe essere visualizzato un messaggio di errore di esaurimento TCAM.

```
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
```

Il campo `Flags` (`L3DenyToCpu`) indica che, se un pacchetto viene rifiutato a causa dell'ACL, il pacchetto viene indirizzato alla CPU. Lo switch invia quindi un messaggio ICMP (Internet Control Message Protocol) non raggiungibile. Questo è il comportamento predefinito. Quando i pacchetti vengono inviati alla CPU, sullo switch può verificarsi un elevato utilizzo della CPU. Tuttavia, nel software Cisco IOS versione 12.1(13)EW e successive, questi pacchetti hanno una velocità limitata alla CPU. Nella maggior parte dei casi, Cisco consiglia di disattivare la funzione che invia messaggi ICMP "destinazione irraggiungibile".

Questo output mostra la configurazione dello switch per non inviare messaggi ICMP "destinazione irraggiungibile" e la verifica della programmazione TCAM dopo la modifica. Lo stato dell'ACL 101 è ora `FullyLoaded`, come mostrato nell'output del comando. Il traffico negato non viene indirizzato alla 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
```

Nota: se si supera il TCAM QoS durante l'applicazione di una determinata policy QoS, tale policy *non* viene applicata all'interfaccia o alla VLAN. Catalyst 4500 non implementa il criterio QoS nel percorso software. Pertanto, l'utilizzo della CPU non aumenta quando si supera il TCAM QoS.

```
*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.

Eseguire il comando **show platform cpu packet statistics**. Determinare se la coda di `elaborazione del software ACL` riceve un numero elevato di pacchetti. Un numero elevato di pacchetti indica l'esaurimento del TCAM di sicurezza. L'esaurimento del TCAM determina l'invio dei pacchetti alla CPU per l'inoltro del software.

```
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
```

Se la coda di `elaborazione del software ACL` non riceve una quantità eccessiva di traffico, fare riferimento all'utilizzo elevato della CPU sugli switch Catalyst 4500 con software Cisco IOS per altre possibili cause. Il documento fornisce informazioni su come risolvere i problemi relativi ad altri scenari di utilizzo elevato della CPU.

Il TCAM Catalyst 4500 può causare un overflow per i seguenti motivi:

- Un algoritmo di programmazione TCAM non ottimale per TCAM 2
- Uso eccessivo di operazioni di livello 4 (L4Ops) in un ACL
- ACL eccessivi per il Supervisor Engine o il tipo di switch

Algoritmo di programmazione TCAM non ottimale per TCAM 2

Come illustrato nella sezione Tipi di TCAM, l'efficienza di TCAM 2 è inferiore in quanto otto voci condividono una maschera. Il software Catalyst 4500 consente due tipi di algoritmi di programmazione TCAM per TCAM 2 che migliorano l'efficienza di TCAM 2:

- Pacchetto: adatto alla maggior parte degli scenari ACL di sicurezza**Nota:** questa è l'impostazione predefinita.
- Dispersa: utilizzata nello scenario IPSG

Èpossibile modificare l'algoritmo in un algoritmo a dispersione, ma questa operazione in genere non è utile se sono stati configurati solo ACL di sicurezza, ad esempio ACL. L'algoritmo a dispersione è efficace solo in scenari in cui lo stesso ACL o un ACL piccolo simile viene ripetuto su più porte. Questo scenario si verifica con un IPSG abilitato su più interfacce. Nello scenario IPSG, ogni ACL dinamico:

- Ha un numero ridotto di vociCiò include i permessi per gli indirizzi IP consentiti e una negazione alla fine per impedire l'accesso alla porta da parte di indirizzi IP non autorizzati.

- Ripetuto per tutte le porte di accesso configurateL'ACL viene ripetuto per un massimo di 240 porte su uno switch Catalyst 4507R.

Nota: TCAM 3 utilizza l'algoritmo compresso di default. Poiché la struttura TCAM è una maschera per ogni voce, l'algoritmo compresso è il migliore algoritmo possibile. Pertanto, l'opzione scattered algorithm non è abilitata su questi switch.

L'esempio si riferisce a un Supervisor Engine II+ configurato per la funzionalità IPSG. L'output mostra che, sebbene venga utilizzato solo il 49% delle voci, viene utilizzato l'89% delle maschere:

```
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 questo caso, è utile modificare l'algoritmo di programmazione dall'algoritmo compresso di default all'algoritmo sparso. L'algoritmo a dispersione riduce l'utilizzo totale della maschera dall'89% al 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
```

Per informazioni sulle best practice per le funzioni di sicurezza sugli switch Catalyst 4500, fare riferimento alle best practice per le funzioni di sicurezza degli switch Catalyst 4500 per i supervisori.

Uso eccessivo di L4Ops in un ACL

Il termine L4Ops si riferisce all'uso delle parole chiave **gt**, **lt**, **neq** e **range** nella configurazione degli ACL. Catalyst 4500 ha dei limiti sul numero di parole chiave che è possibile usare in un singolo ACL. Il limite, che varia a seconda del Supervisor Engine e dello switch, è sei o otto L4Ops per ACL. La tabella 3 mostra il limite per Supervisor Engine e per ACL.

Tabella 3 - Limite L4Op per ACL su diversi Supervisor Engine e switch Catalyst 4500

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

Se si supera il limite L4Op per ACL, sulla console viene visualizzato un messaggio di avviso. Il messaggio è simile al seguente:

```
%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.
```

Inoltre, se il limite L4Op viene superato, la voce ACE specifica viene espansa nella TCAM. Ulteriori risultati sull'utilizzo di TCAM. La voce ACE rappresenta un esempio:

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

Con questa voce ACE in un ACL, lo switch usa solo una voce e un L4Op. Tuttavia, se in questo ACL sono già in uso sei ACL, l'ACE viene espansa a 10 voci nell'hardware. Una tale espansione può potenzialmente utilizzare un sacco di voci nel TCAM. L'uso accorto di questi L4Ops impedisce l'overflow TCAM.

Nota: se questo caso coinvolge Supervisor Engine V-10GE e WS-C4948-10GE, otto ACL precedentemente utilizzati da L4Ops danno luogo all'espansione ACE.

Tenere presenti questi elementi quando si usa L4Op sugli switch Catalyst 4500:

- Le operazioni L4 sono considerate diverse se l'operatore o l'operando differiscono.Ad esempio, questo ACL contiene tre diverse operazioni L4 perché **gt 10** e **gt 11** sono considerate due diverse operazioni L4:
  ```
  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
  ```

- Le operazioni L4 sono considerate diverse se la stessa coppia operatore/operando si applica una volta a una porta di origine e una volta a una porta di destinazione.Di seguito è riportato un esempio:
  ```
  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
  ```

- Ove possibile, gli switch Catalyst 4500 condividono gli switch L4Ops.Nell'esempio, le righe in ***corsivo grassetto*** illustrano questo scenario:Uso L4Op per ACL 101 = 5Uso L4Op per ACL 102 = 4 **Nota:** la parola chiave **eq** non utilizza alcuna risorsa hardware L4Op.Totale utilizzo L4Op = **8Nota:** gli ACL 101 e 102 condividono un L4Op.**Nota:** L4Op viene condiviso anche se il protocollo, ad esempio TCP o UDP (User Datagram Protocol), non corrisponde o l'azione di autorizzazione/rifiuto non corrisponde.

ACL eccessivi per il Supervisor Engine o il tipo di switch

Come mostra la Tabella 2, TCAM è una risorsa limitata. È possibile eccedere la risorsa TCAM di qualsiasi Supervisor Engine se si configurano ACL o funzionalità eccessive, come IPSG, con un numero elevato di voci IPSG.

Se si supera lo spazio TCAM per il Supervisor Engine, eseguire la procedura seguente:

- Se si dispone di un Supervisor Engine II+ e si esegue una versione software Cisco IOS *precedente* alla versione 12.2(18)EW, aggiornare il software Cisco IOS alla versione 12.2(25)EWA.La capacità di TCAM è stata aumentata nelle versioni successive.
- Se si utilizza lo snooping DHCP e IPSG e si inizia a non utilizzare più TCAM, usare la versione più recente del software Cisco IOS versione 12.2(25)EWA per la manutenzione e usare l'algoritmo a dispersione nel caso di prodotti TCAM 2.**Nota:** l'algoritmo a dispersione è disponibile a partire da Cisco IOS versione 12.2(20)EW.L'ultima release presenta miglioramenti per un migliore utilizzo del TCAM con snooping DCHP e funzioni DAI (Dynamic Address Resolution Protocol).
- Se si inizia ad avere un TCAM insufficiente perché viene superato il limite L4Op, provare a ridurre l'uso di L4Op nell'ACL in modo da evitare l'overflow TCAM.
- Se si usano molti ACL o policy simili su diverse porte della stessa VLAN, aggregarli in un unico ACL o policy sull'interfaccia VLAN.Questa aggregazione consente di risparmiare spazio TCAM. Ad esempio, quando si applicano policy basate sulla voce, per la classificazione viene utilizzata la QoS predefinita basata sulla porta. Questa QoS predefinita può causare il superamento della capacità TCAM. Se si passa QoS a VLAN, l'utilizzo di TCAM viene ridotto.
- Se i problemi con lo spazio TCAM persistono, prendere in considerazione un Supervisor Engine di fascia alta, come il Supervisor Engine V-10GE o Catalyst 4948-10GE.Questi prodotti utilizzano l'hardware TCAM 3 più efficiente.

Riepilogo

Catalyst 4500 usa il software TCAM per programmare gli ACL configurati. TCAM consente l'applicazione degli ACL nel percorso di inoltro hardware senza alcun impatto sulle prestazioni dello switch. Le prestazioni rimangono costanti nonostante le dimensioni dell'ACL, in quanto le prestazioni delle ricerche ACL avvengono alla velocità della linea. Tuttavia, TCAM è una risorsa limitata. Pertanto, se si configura un numero eccessivo di voci ACL, si supera la capacità TCAM. Catalyst 4500 ha implementato numerose ottimizzazioni e fornito comandi per variare l'algoritmo di programmazione di TCAM al fine di ottenere la massima efficienza. I prodotti TCAM 3, come Supervisor Engine V-10GE e Catalyst 4948-10GE, offrono la maggior parte delle risorse TCAM per le policy di sicurezza ACL e QoS.

Informazioni correlate

- Pagine di supporto dei prodotti LAN
- Pagina di supporto dello switching LAN
- Documentazione e supporto tecnico – Cisco Systems