ACL y QoS TCAM Exhaustion Avoidance en Catalyst 4500 Switches

Contenido

Introducción

Los switches Cisco Catalyst 4500 y Catalyst 4948 Series soportan ACL (Access Control List) tarifa del alambre y la función de Calidad de Servicio (QoS) con el uso de TCAM (Ternary Content Addressable Memory). La habilitación de las ACL y las políticas no disminuye el rendimiento del ruteo o el switching del switch mientras las ACL se carguen completamente en el TCAM. Si se agota el TCAM, los paquetes se pueden remitir a través del trayecto de la CPU, que puede disminuir el rendimiento de esos paquetes. Este documento proporciona detalles sobre:

- Los diferentes tipos de TCAM que utilizan Catalyst 4500 y Catalyst 4948
- Cómo el Catalyst 4500 programa las TCAM
- Cómo configurar de manera óptima las ACL y TCAM en el switch para evitar el agotamiento de TCAM

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 4500 Series Switch
- Catalyst 4948 Series Switch

Nota: Este documento sólo se aplica a los switches basados en el software Cisco IOS® y no se aplica a los switches basados en 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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Para implementar los diversos tipos de ACL y políticas de QoS en hardware, Catalyst 4500 programa tablas de búsqueda de hardware (TCAM) y varios registros de hardware en Supervisor Engine. Cuando llega un paquete, el switch realiza una búsqueda de tabla de hardware (búsqueda TCAM) y decide permitir o denegar el paquete.

El Catalyst 4500 admite diferentes tipos de ACL. La tabla 1 describe estos tipos de ACL.

Tabla 1: Tipos de ACL Soportados en Catalyst 4500 Switches

Tipo de ACL	Donde se aplica	Tráfico controlado	Dirección:
RACL[1]	Puerto L3[2], canal L3 o SVI[3] (VLAN)	Tráfico IP enrutado	Entrante o saliente
VACL[4]	VLAN (a través del comando **vlan filter**)	Todos los paquetes que se rutean dentro o fuera de una VLAN o que se puentean dentro de una VLAN	Sin dirección
PACL[5]	Puerto L2[6] o canal L2	Todo el tráfico IP y el tráfico que no es IPv4[7] (a través de MAC ACL)	Entrante o saliente

[1] RACL = ACL del router

2 Nivel 3 = Capa 3

[3] SVI = interfaz virtual conmutada

[4] VACL = VLAN ACL

[5] PACL = ACL de puerto

[6] L2 = Capa 2

[7] IPv4 = IP versión 4

Arquitectura de programación de hardware de QoS y ACL de Catalyst 4500

El TCAM Catalyst 4500 tiene el siguiente número de entradas:

- 32 000 entradas para ACL de seguridad, que también se conoce como ACL de función
- 32 000 entradas para QoS ACL

Tanto para la ACL de seguridad como para la ACL de QoS, las entradas están dedicadas de la siguiente manera:

- 16 000 entradas para la dirección de entrada
- 16 000 entradas para la dirección de salida

La figura 3 muestra la dedicación de la entrada TCAM. Consulte la sección Tipos de TCAM para obtener más información sobre las TCAM.

La Tabla 2 muestra los recursos de ACL disponibles para diversos Catalyst 4500 Supervisor Engines y switches.

Tabla 2 - Recursos de ACL de Catalyst 4500 en diversos motores y switches de supervisor

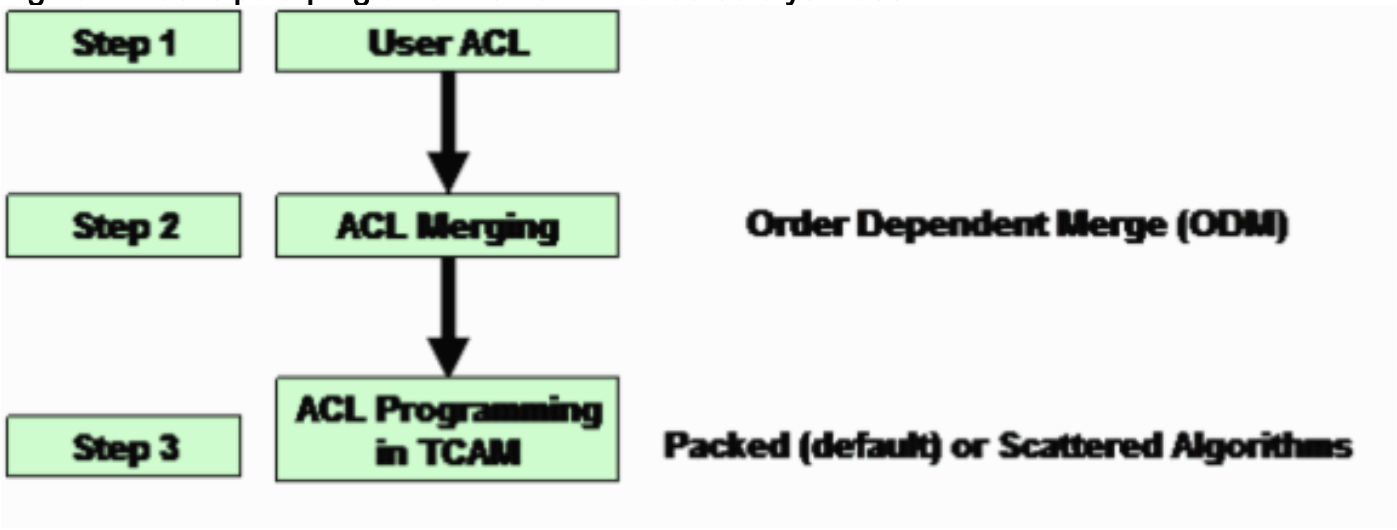
Producto	Versión TCAM	TCAM de funciones (por dirección)	TCAM de QoS (por dirección)
Supervisor Engine II+	2	8000 entradas, 1000 máscaras	8000 entradas, 1000 máscaras
Supervisor Engine II+TS/III/IV/V y WS-C4948	2	16 000 entradas, 2000 máscaras	16 000 entradas, 2000 máscaras
Supervisor Engine V-10GE y WS-C4948-10GE	3	16 000 entradas, 16 000 máscaras	16 000 entradas, 16 000 máscaras

El Catalyst 4500 utiliza TCAM independientes y dedicados para el routing de unidifusión y multidifusión IP. El Catalyst 4500 puede tener hasta 128.000 entradas de ruta que comparten las rutas de unidifusión y multidifusión. Sin embargo, estos detalles están fuera del alcance de este documento. Este documento sólo trata los problemas de seguridad y de agotamiento de la TCAM

de QoS.

La Figura 1 muestra los pasos para programar las ACL en las tablas de hardware en el Catalyst 4500.

Figura 1: Pasos para programar ACL en switches Catalyst 4500



Paso 1

Este paso implica una de estas acciones:

- Configuración y aplicación de una política de ACL o QoS a una interfaz o VLANLa creación de ACL puede producirse dinámicamente. Un ejemplo es el caso de la función IP Source Guard (IPSG). Con esta función, el switch crea automáticamente una PACL para las direcciones IP asociadas con el puerto.
- Modificación de una ACL que ya existe

Nota: La configuración sola de una ACL no da como resultado la programación TCAM. La ACL (política de QoS) debe aplicarse a una interfaz para programar la ACL en la TCAM.

Paso 2

La ACL se debe combinar antes de que se pueda programar en las tablas de hardware (TCAM). La combinación programa varias ACL (PACL, VACL o RACL) en el hardware de forma combinada. De esta manera, sólo es necesaria una única búsqueda de hardware para comparar todas las ACL aplicables en la trayectoria de reenvío lógico de paquetes.

Por ejemplo, en la Figura 2, un paquete que se enruta de PC-A a PC-C potencialmente puede tener estas ACL:

- PACL de entrada en el puerto PC-A
- VACL en VLAN 1
- Una RACL de entrada en la interfaz VLAN 1 en la dirección de entrada

Estas tres ACL se combinan para que una sola búsqueda en el TCAM de entrada sea suficiente para tomar la decisión de reenvío para permitir o denegar. De manera similar, sólo se necesita una única búsqueda de salida porque el TCAM se programa con el resultado combinado de estas tres ACL:

- El resultado RACL en la interfaz VLAN 2
- VLAN 2 VACL
- La salida PACL en el puerto PC-C

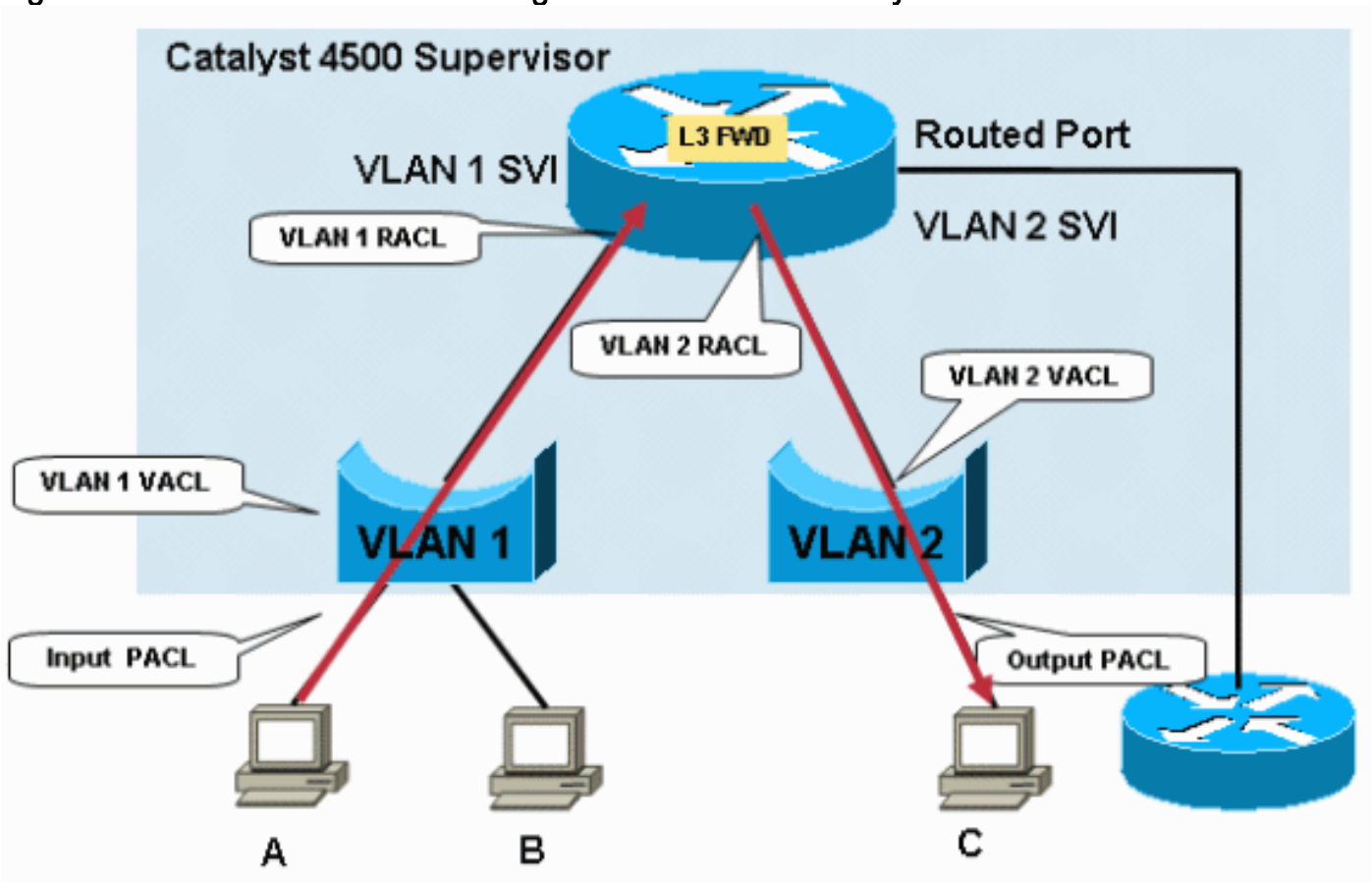
Con una única búsqueda de entrada y una para salida, no hay reenvío de hardware de penalización de los paquetes cuando alguna o todas estas ACL están en el trayecto de reenvío de paquetes.

Nota: Las búsquedas TCAM de entrada y salida se producen al mismo tiempo en el hardware. Un error común es que la búsqueda TCAM de salida ocurre después de la búsqueda TCAM de entrada, como sugiere el flujo de paquetes lógico. Esta información es importante para comprender porque la política de salida de Catalyst 4500 no puede coincidir con los parámetros QoS modificados de la política de entrada. En el caso de ACL de seguridad, se produce la acción más grave. El paquete se descarta en cualquiera de estas situaciones:

- Si el resultado de la búsqueda de entrada es drop y el resultado de la búsqueda de salida es permit
- Si el resultado de la búsqueda de entrada es permit y el resultado de la búsqueda de salida es drop

Nota: El paquete se permite si se permiten los resultados de la búsqueda de entrada y salida.

Figura 2: Filtrado mediante ACL de seguridad en switches Catalyst 4500



La combinación de ACL en el Catalyst 4500 depende del orden. El proceso también se conoce como fusión dependiente de pedidos (ODM). Con el ODM, las entradas de ACL se programan en el orden en que aparecen en la ACL. Por ejemplo, si una ACL contiene dos entradas de control de acceso (ACE), el switch programa primero ACE 1 y luego ACE 2. Sin embargo, la dependencia del orden sólo se produce entre las ACE dentro de una ACL específica. Por ejemplo, las ACE en la ACL 120 pueden comenzar antes de las ACE en la ACL 100 en la TCAM.

Paso 3

La ACL fusionada se programa en el TCAM. El TCAM de entrada o salida para ACL o QoS se divide en dos regiones, PortAndVlan y PortOrVlan. La ACL combinada se programa en la región PortAndVlan del TCAM si una configuración tiene *ambas* de estas ACL en el mismo trayecto de paquete:

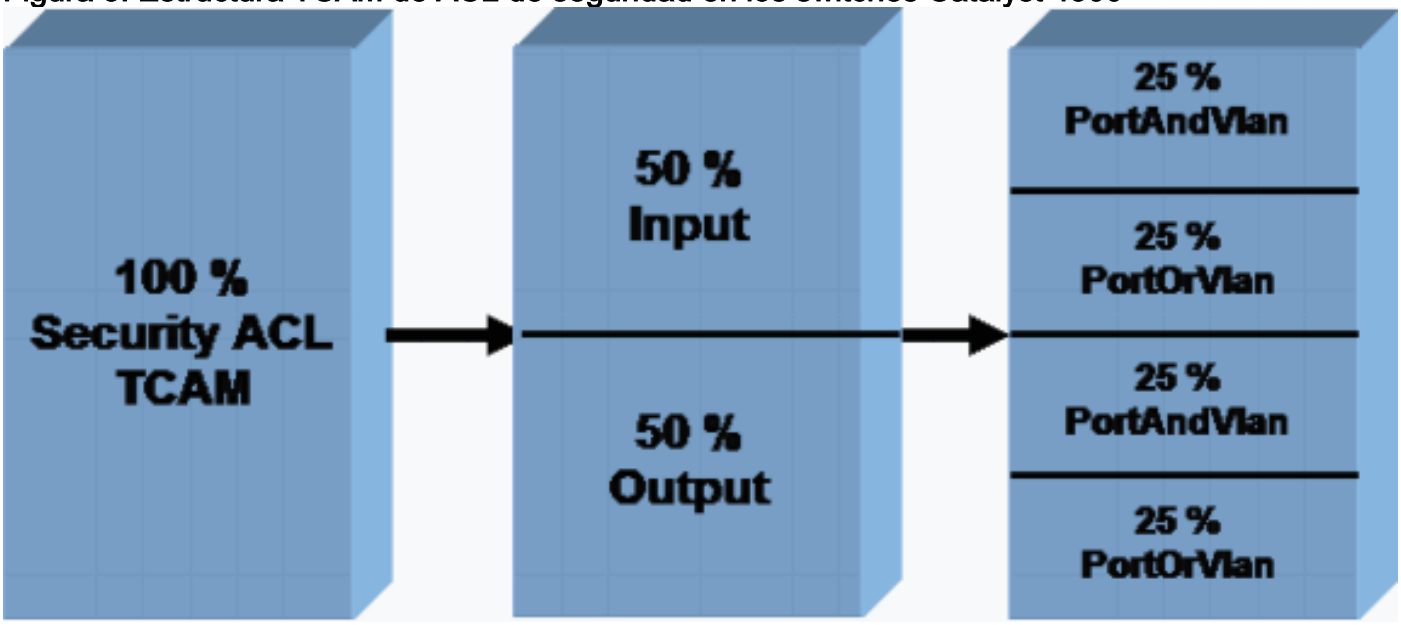
- UN PACL**Nota:** PACL es una ACL de filtrado normal o una ACL dinámica creada por IPSG.
- Una VACL o RACL

Una ACL se programa en la región PortOrVlan del TCAM si una trayectoria determinada del paquete tiene solamente una PACL o una VACL o una RACL. La figura 3 muestra la seguridad ACL TCAM tallando para varios tipos de ACL. QoS tiene una TCAM dedicada, separada y dividida de forma similar.

Actualmente, no puede modificar la asignación predeterminada de TCAM. Sin embargo, hay planes para proporcionar la capacidad de cambiar la asignación TCAM disponible para las regiones PortAndVlan y PortOrVlan en futuras versiones de software. Este cambio le permitirá aumentar o disminuir el espacio para PortAndVlan y PortOrVlan en las TCAM de entrada o salida.

Nota: Cualquier aumento en la asignación para la región PortAndVlan dará como resultado una disminución equivalente para la región PortOrVlan en la TCAM de entrada o salida.

Figura 3: Estructura TCAM de ACL de seguridad en los switches Catalyst 4500



El comando **show platform hardware ACL statistics usage brief** muestra esta utilización de TCAM por región tanto para las TCAM de ACL como de QoS. El resultado del comando muestra las máscaras y entradas disponibles y las divide por región, como en la Figura 3. Este ejemplo de resultado proviene de un Catalyst 4500 Supervisor Engine II+:

Nota: Vea la sección Tipos de TCAM de este documento para obtener más información sobre las máscaras y las entradas.

```
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
```

Tipos de TCAM

El Catalyst 4500 utiliza dos tipos de TCAM, como se muestra en la Tabla 2. Esta sección presenta la diferencia entre las dos versiones de TCAM para que pueda seleccionar el producto adecuado para su red y configuración.

TCAM 2 utiliza una estructura en la que ocho entradas comparten una máscara. Un ejemplo es ocho direcciones IP en ACE. Las entradas deben tener la misma máscara que la que comparten. Si los ACE tienen máscaras diferentes, las entradas deben utilizar máscaras separadas según sea necesario. Este uso de máscaras separadas puede llevar al agotamiento de las máscaras. El agotamiento de la máscara en la TCAM es una de las razones comunes para el agotamiento de la TCAM.

La TCAM 3 no tiene ninguna restricción de este tipo. Cada entrada puede tener su propia máscara única en el TCAM. Es posible la utilización completa de todas las entradas disponibles en el hardware, independientemente de la máscara de esas entradas.

Para demostrar esta arquitectura de hardware, el ejemplo de esta sección muestra cómo un TCAM 2 y un TCAM 3 programan ACL en 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
```

Esta ACL de muestra tiene dos entradas que tienen dos máscaras diferentes. ACE 1 es una entrada de host y por lo tanto tiene una máscara /32. ACE 2 es una entrada de subred con una máscara /24. Debido a que la segunda entrada tiene una máscara diferente, no se pueden utilizar entradas vacías en la máscara 1 y se utiliza una máscara independiente en el caso de TCAM 2.

Esta tabla muestra cómo se programa esta ACL en TCAM 2:

Máscaras	Entradas
Máscara 1 Coincidencia: los 32 bits de la dirección IP de origen "No importa": todos los bits restantes	IP de origen = 8.1.1.1
	Entrada vacía 2
	Entrada vacía 3
	Entrada vacía 4
	Entrada vacía 5
	Entrada

	vacía 6
	Entrada vacía 7
	Entrada vacía 8
Coincidencia **Mask 2**: 24 bits más significativos de la dirección IP de origen "No importa": todos los bits restantes	IP de origen = 8.1.1.0
	Entrada vacía 2
	Entrada vacía 3
	Entrada vacía 4
	Entrada vacía 5
	Entrada vacía 6
	Entrada vacía 7
	Entrada vacía 8

Aunque hay entradas gratuitas disponibles como parte de la Máscara 1, la estructura TCAM 2 evita la población de ACE 2 en la entrada vacía 2 para la Máscara 1. El uso de esta máscara no está permitido porque la máscara de ACE 2 no coincide con la máscara /32 de ACE 1. TCAM 2 debe programar la ACE 2 con el uso de una máscara independiente, una máscara /24.

Este uso de una máscara independiente puede dar lugar a un agotamiento más rápido de los recursos disponibles, como muestra la tabla 2. Otras ACL todavía pueden utilizar las entradas restantes en la Máscara 1. Sin embargo, en la mayoría de los casos, la eficiencia de TCAM 2 es alta, pero no es del 100%. La eficiencia varía según cada escenario de configuración.

Esta tabla muestra la misma ACL programada en el TCAM 3. TCAM 3 asigna una máscara para cada entrada:

Máscaras	**Entradas**
Máscara 32 bits para la dirección IP 1	IP de origen = 8.1.1.1
Máscara 24 bits para la dirección IP 2	IP de origen = 8.1.1.0
Máscara vacía 3	Entrada vacía 3
Máscara vacía 4	Entrada vacía 4
Máscara vacía 5	Entrada vacía 5
Máscara vacía 6	Entrada vacía 6
Máscara vacía 7	Entrada vacía 7
Máscara vacía 8	Entrada vacía 8
Máscara vacía 9	Entrada vacía 9

Máscara vacía 10	Entrada vacía 10
Máscara vacía 11	Entrada vacía 11
Máscara vacía 12	Entrada vacía 12
Máscara vacía 13	Entrada vacía 13
Máscara vacía 14	Entrada vacía 14
Máscara vacía 15	Entrada vacía 15
Máscara vacía 16	Entrada vacía 16

En este ejemplo, las 14 entradas restantes pueden tener entradas con diferentes máscaras, sin restricciones. Por lo tanto, el TCAM 3 es mucho más eficiente que el TCAM 2. Este ejemplo se simplifica excesivamente para ilustrar la diferencia entre las versiones TCAM. El software Catalyst 4500 tiene numerosas optimizaciones para aumentar la eficiencia de la programación en TCAM 2 para un escenario de configuración práctico. La sección Algoritmo de Programación TCAM Subóptimo para TCAM 2 de este documento analiza estas optimizaciones.

Para TCAM 2 y TCAM 3 en el Catalyst 4500, las entradas TCAM se comparten si se aplica la misma ACL en diferentes interfaces. Esta optimización ahorra espacio TCAM.

Resolución de problemas de agotamiento de TCAM

Cuando se produce el agotamiento de TCAM en los switches Catalyst 4500 durante la programación de una ACL de seguridad, una aplicación parcial de la ACL ocurre a través de la trayectoria de software. Los paquetes que coinciden con las ACE que no se aplican en el TCAM se procesan en el software. Este procesamiento en el software causa una alta utilización de la CPU. Debido a que la programación de ACL de Catalyst 4500 depende del orden, la ACL siempre se programa desde arriba hacia abajo. Si una ACL específica no encaja completamente en la TCAM, las ACE en la parte inferior de la ACL probablemente no se programen en la TCAM.

Aparece un mensaje de advertencia cuando se produce un desbordamiento de TCAM. Aquí tiene un ejemplo:

```
%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.
```

También puede ver este mensaje de error en el resultado del comando **show logging** si ha habilitado syslog. La presencia de este mensaje indica de manera concluyente que se llevará a cabo cierto procesamiento de software. En consecuencia, puede haber una alta utilización de la CPU. La ACL que ya se ha programado en el TCAM permanece programada en el TCAM si se agota la capacidad TCAM durante la aplicación de la nueva ACL. Los paquetes que coinciden con las ACL que ya se han programado continúan siendo procesados y reenviados en hardware.

Nota: Si realiza cambios en una ACL grande, se puede mostrar el mensaje TCAM-overs. El switch intenta reprogramar la ACL en TCAM. En la mayoría de los casos, la nueva ACL modificada se puede reprogramar completamente en hardware. Si el switch puede reprogramar correctamente la ACL en su totalidad en el TCAM, aparece este mensaje:

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

Utilice el comando **show platform software acl input summary interface *interface-id*** para verificar que la ACL esté completamente programada en el hardware.

Este resultado muestra la configuración de ACL 101 a VLAN 1 y la verificación de que la ACL está completamente programada en el hardware:

Nota: Si la ACL no está completamente programada, puede aparecer un mensaje de error TCAM-agottion.

```
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
```

El campo `Flags` (`L3DenyToCpu`) indica que, si se niega un paquete debido a la ACL, el paquete se envía a la CPU. A continuación, el switch envía un mensaje de protocolo de mensajes de control de Internet (ICMP) inalcanzable. Este comportamiento es el predeterminado. Cuando los paquetes son impulsados a la CPU, puede producirse una alta utilización de la CPU en el switch. Sin embargo, en Cisco IOS Software Release 12.1(13)EW y posteriores, estos paquetes se limitan a la velocidad de la CPU. En la mayoría de los casos, Cisco recomienda desactivar la función que envía mensajes de ICMP inalcanzable.

Este resultado muestra la configuración del switch para no enviar mensajes ICMP inalcanzables y la verificación de la programación TCAM después del cambio. El estado de ACL 101 está ahora `Totalmente cargado`, como muestra el resultado del comando. El tráfico denegado no va a la 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: Si se excede la TCAM de QoS durante la aplicación de una política de QoS determinada, esa política específica *no* se aplica a la interfaz o VLAN. El Catalyst 4500 no implementa la política de QoS en la trayectoria de software. Por lo tanto, la utilización de la CPU no aumenta cuando se excede la TCAM de 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.
```

Ejecute el comando **show platform cpu packet statistics**. Determine si la cola de `procesamiento de ACL Sw` recibe un número elevado de paquetes. Un número elevado de paquetes indica el agotamiento de la TCAM de seguridad. Este agotamiento de TCAM hace que los paquetes se envíen a la CPU para el reenvío de 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
```

Si encuentra que la cola de procesamiento `ACL sw` no recibe una cantidad excesiva de tráfico, consulte Uso Excesivo de CPU en Switches Catalyst 4500 Basados en Cisco IOS Software para conocer otras causas posibles. El documento proporciona información sobre cómo resolver otros escenarios de uso elevado de la CPU.

El TCAM Catalyst 4500 puede desbordarse por estas razones:

- Un algoritmo de programación TCAM subóptimo para TCAM 2
- Uso excesivo de las operaciones de capa 4 (L4Ops) en una ACL
- ACL excesivas para el motor supervisor o tipo de switch

Algoritmo de programación TCAM subóptimo para TCAM 2

Como discute la sección Tipos de TCAM, la eficiencia de TCAM 2 es menor debido al hecho de que ocho entradas comparten una máscara. El software Catalyst 4500 permite dos tipos de algoritmos de programación TCAM para TCAM 2 que mejoran la eficiencia de TCAM 2:

- Paquetes: adecuados para la mayoría de los escenarios de ACL de seguridad**Nota:** Este es el valor predeterminado.
- disperso: se utiliza en el escenario IPSG

Puede cambiar el algoritmo a un algoritmo disperso, pero esto no suele ayudar si ha configurado sólo ACL de seguridad, como las RACL. El algoritmo disperso sólo es efectivo en escenarios donde se repite la misma o similar ACL pequeña en numerosos puertos. Este escenario es el caso de un IPSG habilitado en varias interfaces. En el escenario IPSG, cada ACL dinámica:

- Tiene un pequeño número de entradasEsto incluye permisos para direcciones IP permitidas y una denegación al final para evitar el acceso del puerto por direcciones IP no autorizadas.
- Se repite para todos los puertos de acceso configuradosLa ACL se repite para hasta 240 puertos en un Catalyst 4507R.

Nota: TCAM 3 utiliza el algoritmo empaquetado predeterminado. Debido a que la estructura TCAM es una máscara por entrada, el algoritmo empaquetado es el mejor algoritmo posible. Por lo tanto, la opción del algoritmo disperso no está habilitada en estos switches.

Este ejemplo se encuentra en un Supervisor Engine II+ configurado para la función IPSG. El resultado muestra que, aunque sólo se utiliza el 49% de las entradas, el 89% de las máscaras se consumen:

```
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
```

En este caso, un cambio en el algoritmo de programación del algoritmo empaquetado predeterminado al algoritmo disperso ayuda. El algoritmo disperso reduce el uso total de la máscara del 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
```

Para obtener información sobre las prácticas recomendadas para las funciones de seguridad en los switches Catalyst 4500, consulte Prácticas Recomendadas de las Funciones de Seguridad de Catalyst 4500 para Supervisores.

Uso Excesivo de L4Ops en una ACL

El término L4Ops hace referencia al uso de las palabras clave **gt**, **lt**, **neq** y **range** en la configuración ACL. El Catalyst 4500 tiene límites en el número de estas palabras clave que puede utilizar en una única ACL. La limitación, que varía según el Supervisor Engine y el switch, es de seis u ocho L4Ops por ACL. La tabla 3 muestra el límite por Supervisor Engine y por ACL.

Tabla 3 - Límite de L4Op por ACL en Diferentes Motores y Switches Supervisor Catalyst 4500

Producto	L4Op
Supervisor Engine II+/ II+TS	32 (6 por ACL)
Supervisor Engine III/IV/V y WS-C4948	32 (6 por ACL)
Supervisor Engine V-10GE y WS-C4948-10GE	64 (8 por ACL)

Si se excede el límite L4Op por ACL, se muestra un mensaje de advertencia en la consola. El mensaje es similar a esto:

```
%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.
```

Además, si se excede el límite L4Op, la ACE específica se expande en la TCAM. Resultados adicionales de utilización de TCAM. Esta ACE sirve como ejemplo:

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

Con esta ACE en una ACL, el switch utiliza sólo una entrada y una L4Op. Sin embargo, si ya se utilizan seis L4Ops en esta ACL, esta ACE se expande a 10 entradas en el hardware. Esta expansión puede potencialmente utilizar muchas entradas en el TCAM. El uso cuidadoso de estos L4Ops evita el desbordamiento de TCAM.

Nota: Si este caso involucra a Supervisor Engine V-10GE y WS-C4948-10GE, ocho L4Ops usadas previamente en la ACL resultan en la expansión ACE.

Tenga en cuenta estos elementos cuando utilice L4Op en los switches Catalyst 4500:

- Las operaciones L4 se consideran diferentes si el operador u operando difieren.Por ejemplo, esta ACL contiene tres operaciones L4 diferentes porque **gt 10** y **gt 11** se consideran dos operaciones L4 diferentes:
  ```
  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
  ```
- Las operaciones L4 se consideran diferentes si la misma pareja de operando/operador se aplica una vez a un puerto de origen y una vez a un puerto de destino.Aquí tiene un ejemplo:
  ```
  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
  ```
- Los switches Catalyst 4500 comparten L4Ops cuando es posible.En este ejemplo, las líneas en cursiva de ***negrita*** muestran este escenario:Uso de L4Op para ACL 101 = 5Uso de L4Op para ACL 102 = 4 **Nota:** La palabra clave **eq** no consume ninguno de los recursos de

hardware de L4Op.Uso total de L4Op = 8**Nota:** Las ACL 101 y 102 comparten un L4Op.**Nota:** L4Op se comparte incluso si el protocolo, como TCP o el protocolo de datagramas de usuario (UDP), no coincide o la acción permit/deny no coincide.

ACL excesivas para el motor supervisor o el tipo de switch

Como muestra la tabla 2, TCAM es un recurso limitado. Puede exceder el recurso TCAM de cualquier Supervisor Engine si configura ACL excesivas o funciones como IPSG con un alto número de entradas IPSG.

Si excede el espacio TCAM para su Supervisor Engine, siga estos pasos:

- Si tiene un Supervisor Engine II+ y ejecuta una versión del software Cisco IOS *anterior* a la versión 12.2(18)EW del software Cisco IOS, actualice a la última versión de mantenimiento 12.2(25)EWA del software Cisco IOS.La capacidad de TCAM se ha incrementado en las versiones posteriores.
- Si utiliza la indagación DHCP e IPSG y comienza a quedarse sin TCAM, utilice la última versión de mantenimiento 12.2(25)EWA del software del IOS de Cisco y utilice el algoritmo disperso en el caso de los productos TCAM 2.**Nota:** El algoritmo disperso está disponible en Cisco IOS Software Release 12.2(20)EW y posteriores.La última versión también cuenta con mejoras para una mejor utilización de TCAM con las funciones de detección de DCHP y de inspección dinámica de protocolo de resolución de direcciones (ARP) (DAI).
- Si comienza a quedarse sin TCAM porque se excede el límite de L4Op, intente reducir el uso de L4Op en la ACL para evitar el desbordamiento de TCAM.
- Si utiliza muchas ACL o políticas similares en varios puertos en la misma VLAN, agréguelas en una única ACL o política en la interfaz VLAN.Esta agregación ahorra algo de espacio TCAM. Por ejemplo, cuando se aplican políticas basadas en voz, se utiliza la QoS predeterminada basada en puerto para la clasificación. Esta QoS predeterminada puede hacer que se exceda la capacidad TCAM. Si cambia la QoS a basada en VLAN, reducirá el uso de TCAM.
- Si todavía tiene problemas con el espacio TCAM, considere un motor supervisor de gama alta, como el Supervisor Engine V-10GE o Catalyst 4948-10GE.Estos productos utilizan el hardware TCAM 3 más eficiente.

Summary

El Catalyst 4500 programa las ACL configuradas con el uso de TCAM. TCAM permite la aplicación de las ACL en la trayectoria de reenvío de hardware sin impacto en el rendimiento del switch. El rendimiento es constante a pesar del tamaño de la ACL porque el rendimiento de las búsquedas de ACL es a velocidad de línea. Sin embargo, TCAM es un recurso finito. Por lo tanto, si configura un número excesivo de entradas de ACL, excede la capacidad de TCAM. El Catalyst 4500 ha implementado numerosas optimizaciones y ha proporcionado comandos para variar el algoritmo de programación de TCAM a fin de lograr la máxima eficiencia. Los productos TCAM 3, como Supervisor Engine V-10GE y Catalyst 4948-10GE, ofrecen la mayoría de los recursos TCAM para las políticas de seguridad de ACL y QoS.

Información Relacionada

- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems