ACL y prevención de agotamiento TCAM de QoS en los Catalyst 4500 Switch

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 diversos tipos de TCAM que el uso del Catalyst 4500 y del Catalyst 4948
- Cómo el Catalyst 4500 programa los TCAM
- Cómo configurar óptimo los ACL y el TCAM en el Switch para evitar el agotamiento de TCAM

prerrequisitos

Requisitos

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 se aplica solamente al Switches basado en software de Cisco IOS® y no se aplica al Catalyst OS (CatOS) - los switches basados.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

Para implementar los diversos tipos de directivas ACL y de QoS en el hardware, las tablas de busqueda de herramienta de los programas del Catalyst 4500 (TCAM) y los diversos registros de hardware en el Supervisor Engine. Cuando llega un paquete, el Switch realiza una búsqueda en la tabla del hardware (búsqueda TCAM) y decide a cualquier permit or deny al paquete.

Tipos de los soportes del Catalyst 4500 los diversos de ACL. El cuadro 1 delinea estos tipos de ACL.

Cuadro 1 – Teclea de los ACL que se soportan en los Catalyst 4500 Switch

Tipo ACL	Donde está aplicado	Tráfico controlado	Dirección:
RACL 1	Puerto L3[2], canal L3, o SVI3 (VLAN)	Tráfico IP ruteado	Entrante o saliente
VACL 4	VLA N (vía el **comando vlan filter**)	Todos los paquetes los cuales se rutea en o fuera de un VLA N o los cuales se interliga dentro de un VLA N	Directionless
PACL 5	Puerto L2[6] o canal L2	Todo el tráfico IP y tráfico non-IPv4[7] (vía MAC ACL)	Entrante o saliente

[1] RACL = router ACL

2 Nivel 3 = Capa 3

[3] SVI = Switched Virtual Interface

[4] VACL = VLA N ACL

[5] PACL = puerto ACL

[6] L2 = capa 2

[7] IPv4 = versión IP 4

Catalyst 4500 ACL y arquitectura programada del hardware de calidad de servicio

El Catalyst 4500 TCAM tiene el número siguiente de entradas:

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

Para el ACL de seguridad y QoS ACL, las entradas se dedican así:

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

El cuadro 3 muestra el esmero de la entrada TCAM. Vea los tipos de sección TCAM para más información sobre los TCAM.

El cuadro 2 muestra a los recursos de ACL que están disponibles para los diversos motores y Switches del supervisor del Catalyst 4500.

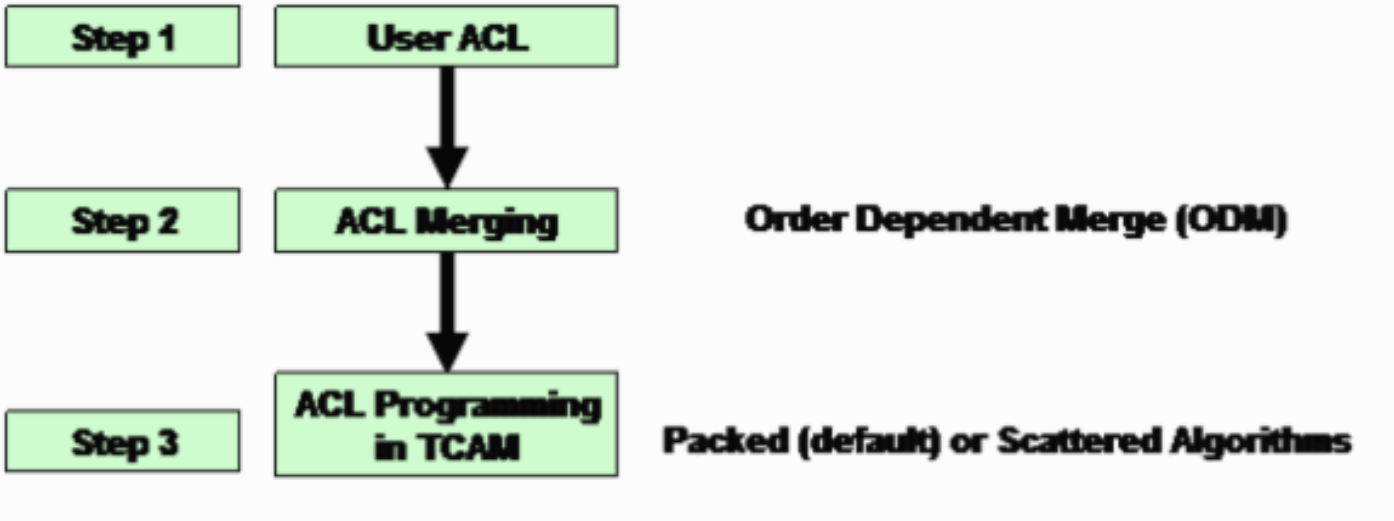
Cuadro 2 – Recursos de ACL del Catalyst 4500 en los diversos motores y Switches del supervisor

Producto	Versiones de TCAM	Característica TCAM (por la dirección)	QoS TCAM (por la 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
V-10GE del Supervisor Engine y WS-C4948-10GE	3	16,000 entradas, 16,000 máscaras	16,000 entradas, 16,000 máscaras

Las aplicaciones del Catalyst 4500 separan, dedicaron los TCAM para la unidifusión IP y el ruteo multicast. El Catalyst 4500 puede tener hasta 128,000 entradas de la ruta que el unicast y las rutas de Multicast compartan. Sin embargo, estos detalles están fuera del ámbito de este documento. Este documento discute solamente los problemas de la Seguridad y del agotamiento de TCAM de QoS.

El cuadro 1 muestra los pasos para programar los ACL en las tablas del hardware en el Catalyst 4500.

Cuadro 1 - Pasos para programar los ACL en los Catalyst 4500 Switch



Paso 1

Este paso implica una de estas acciones:

- Configuración y aplicación de un ACL o política de calidad de servicio (QoS) a una interfaz o a un VLA NLa creación de ACL puede ocurrir dinámicamente. Un ejemplo es el caso de la característica de la Protección de origen IP (IPSG). Con esta característica, el Switch crea automáticamente un PACL para los IP Addresses que se asocia al puerto.
- Modificación de un ACL que existe ya

Nota: La configuración solamente de un ACL no da lugar a la programación TCAM. El ACL (política de calidad de servicio (QoS)) debe aplicado a una interfaz para programar el ACL en el TCAM.

Paso 2

El ACL debe ser combinado antes de que pueda ser programado en las tablas del hardware (TCAM). Los programas de fusión ACL múltiples (PACL, VACL, o RACL) en el hardware en una moda combinada. De esta manera, solamente una sola busqueda de herramienta es necesaria marcar contra todos los ACL aplicables en el trayecto de reenvío lógico del paquete.

Por ejemplo, en el cuadro 2, un paquete que se rutea del PC-A a la PCC potencialmente puede tener estos ACL:

- Una entrada PACL en el puerto PC-A
- Un VACL en el VLAN1
- Un RACL de entrada en la interfaz del VLAN1 en la dirección de la entrada

Se combinan estos tres ACL de modo que las solas operaciones de búsqueda en la entrada TCAM sean bastantes para tomar la decisión de reenvío al permit or deny. Semejantemente, solamente las operaciones de búsqueda de salida única son necesarias porque el TCAM se programa con el resultado combinado de estos tres ACL:

- La salida RACL en la interfaz VLAN2

- El VLAN2 VACL
- La salida PACL en el puerto PCC

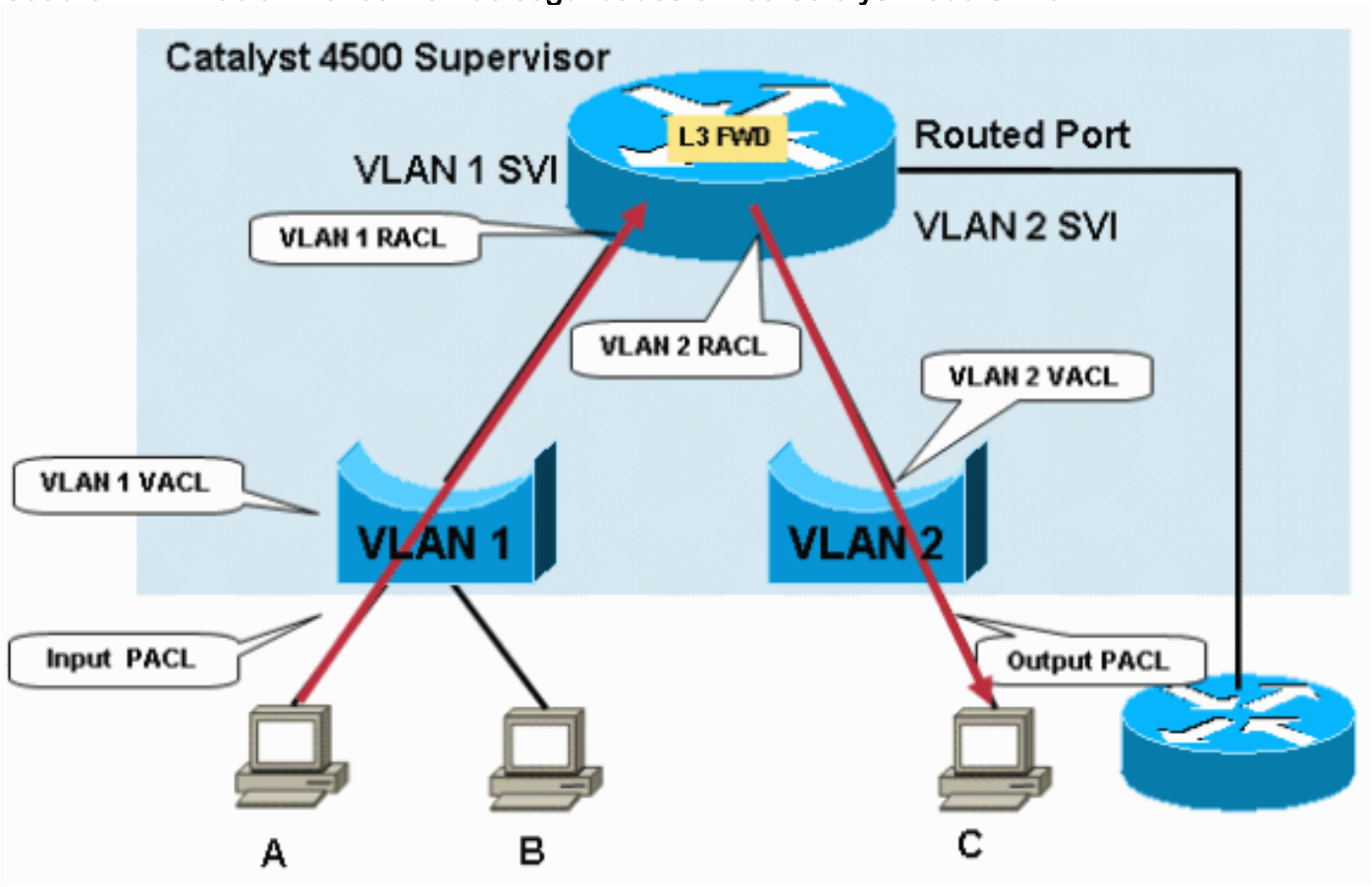
Con las solas operaciones de búsqueda para la entrada y una para la salida, no hay hardware que reenvía de la pena de los paquetes cuando cualquiera o todo el de estos ACL esté en la trayectoria del reenvío de paquete.

Nota: Las búsquedas TCAM entradas y salidas ocurren al mismo tiempo en hardware. Un concepto erróneo común es que la búsqueda TCAM de la salida ocurre después de la búsqueda TCAM de la entrada, pues el flujo de paquetes lógico sugiere. Esta información es importante entender porque la política de resultado del Catalyst 4500 no puede hacer juego en los parámetros de QoS modificados política de entrada. En el caso del ACL de seguridad, la mayoría de la acción severa ocurre. El paquete se cae en cualquiera de estas situaciones:

- Si es el resultado de búsqueda de la entrada el descenso y el resultado de búsqueda de la salida es permiso
- Si es el resultado de búsqueda de la entrada el permiso y el resultado de búsqueda de la salida es descenso

Nota: Se permite el paquete si ambos los resultados de búsqueda entrada y salida son permiso.

Cuadro 2 – Filtración vía los ACL de seguridades en los Catalyst 4500 Switch



La fusión ACL en el Catalyst 4500 es dependiente de la orden. El proceso también se conoce como Order Dependent Merge (ODM). Con el ODM, las entradas ACL se programan en la orden en la cual aparecen en el ACL. Por ejemplo, si un ACL contiene dos entradas de control de acceso (ACE), el Switch programa ACE 1 primero y en seguida programa ACE 2. Sin embargo, la dependencia de la orden está solamente entre los ACE dentro de un ACL específico. Por ejemplo, los ACE en ACL 120 pueden comenzar antes de los ACE en el ACL 100 en el TCAM.

Paso 3

El ACL combinado se programa en el TCAM. La entrada o la salida TCAM para el ACL o QoS está partida más a fondo en dos regiones, PortAndVlan y PortOrVlan. El ACL combinado se programa en la región PortAndVlan del TCAM si una configuración tiene *ambos* ACL en el mismo trayecto de paquete:

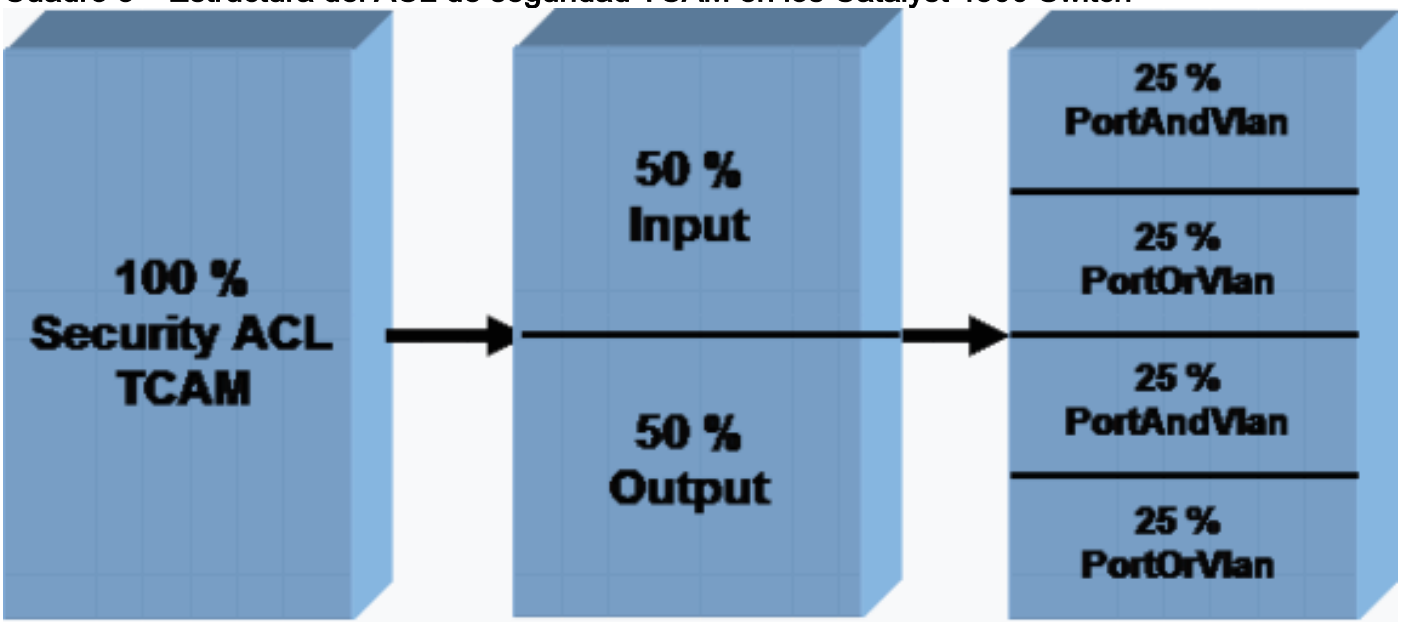
- UN PACL**Nota:** El PACL es un ACL de filtración normal o ACL dinámico IPSG-creado.
- Un VACL o un RACL

Un ACL se programa en la región PortOrVlan del TCAM si un trayecto determinado del paquete tiene solamente un PACL o un VACL o un RACL. El cuadro 3 muestra el ACL de seguridad TCAM que talla para los diversos tipos de ACL. QoS tiene un TCAM semejantemente tallado, separado, dedicado.

Actualmente, usted no puede modificar la asignación de TCAM predeterminada. Sin embargo, hay planes para proporcionar la capacidad de cambiar la asignación de TCAM que está disponible para el PortAndVlan y las regiones PortOrVlanes en las versiones de software futuro. Este cambio permitirá que usted aumente o que disminuya el espacio para el PortAndVlan y el PortOrVlan en la entrada o la salida TCAM.

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

Cuadro 3 – Estructura del ACL de seguridad TCAM en los Catalyst 4500 Switch



El comando show platform hardware ACL statistics utilization brief visualiza esta utilización de TCAM por región para ACL y QoS TCAM. La salida de comando muestra las máscaras y las entradas disponibles y las divide por la región, como en el cuadro 3. Esta salida de muestra es de un Supervisor Engine II+ del Catalyst 4500:

Nota: Vea los tipos de sección TCAM de este documento para 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 demostraciones del cuadro 2. Esta sección presenta la diferencia entre las dos versiones de TCAM de modo que usted pueda seleccionar el producto apropiado para su red y configuración.

El TCAM2 utiliza una estructura en la cual ocho entradas compartan una máscara. Un ejemplo es ocho IP Addresses en los ACE. Las entradas deben tener la misma máscara que la máscara que comparten. Si los ACE tienen diversas máscaras, las entradas deben utilizar las máscaras separadas cuanto sea necesario. Este uso de las máscaras separadas puede llevar para enmascarar el agotamiento. El agotamiento de la máscara en el TCAM es una de las razones comunes para el agotamiento de TCAM.

TCAM3 no tiene tal restricción. Cada entrada puede tener su propia máscara única en el TCAM. El total utilización de todas las entradas que están disponibles en hardware es posible, sin importar la máscara de esas entradas.

Para demostrar esta arquitectura de hardware, el ejemplo en esta sección muestra cómo un TCAM2 y TCAM3 un programa 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 muestra ACL tiene dos entradas que tengan dos diversas máscaras. ACE 1 es una entrada de host y así que tiene una máscara de /32. ACE 2 es una entrada de subred con una máscara de /24. Porque la segunda entrada tiene una diversa máscara, las entradas vacías en la máscara 1 no pueden ser utilizadas y una máscara separada se utiliza en el caso del TCAM2.

Esta tabla muestra cómo este ACL se programa en el TCAM2:

Máscaras	Entradas
Coincidencia de la **máscara 1**: los 32 bits del “sin importancia” de la dirección IP de origen: todos los bits restantes	Fuente IP= 8.1.1.1
	Entry 2 vacío
	Entry 3 vacío
	Entrada vacía 4
	Entrada vacía 5

	Entrada vacía 6
	Entrada vacía 7
	Entrada vacía 8
Coincidencia de la **máscara 2**: la mayoría de los 24 bits significativos del “sin importancia” de la dirección IP de origen: todos los bits restantes	Fuente IP= 8.1.1.0
	Entry 2 vacío
	Entry 3 vacío
	Entrada vacía 4
	Entrada vacía 5
	Entrada vacía 6
	Entrada vacía 7
	Entrada vacía 8

Aunque hay entradas libres disponibles como parte de la máscara 1, la estructura TCAM2 previene la población de ACE 2 en el entry2 vacío para la máscara 1. El uso de esta máscara no es permitido porque la máscara de ACE 2 no hace juego la máscara de /32 de ACE que 1. TCAM2 deben programar ACE 2 con el uso de una máscara separada, una máscara de /24.

Este uso de una máscara separada puede dar lugar a un agotamiento más rápido de los recursos disponibles, como demostraciones del cuadro 2. Otros ACL pueden todavía utilizar las entradas

restantes en la máscara 1. Sin embargo, en la mayoría de los casos, la eficacia del TCAM2 es alta pero no es el 100 por ciento. La eficacia varía con cada escenario de configuración.

Esta tabla muestra que el mismo ACL programado en el TCAM 3. TCAM3 afecta un aparato una máscara para cada entrada:

Máscaras	Entradas
Bits de la máscara 32 para la dirección IP 1	Fuente IP= 8.1.1.1
Bits de la máscara 24 para la dirección IP 2	Fuente IP= 8.1.1.0
Máscara vacía 3	Entry3 vacío
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 cada uno tienen entradas con diversas máscaras, sin las restricciones. Por lo tanto, TCAM3 es mucho más eficiente que el TCAM2. Este ejemplo se simplifica excesivamente para ilustrar la diferencia entre las versiones de TCAM. El software del Catalyst 4500 tiene variadas optimizaciones para aumentar la eficacia de la programación en el TCAM2 para un escenario de configuración práctico. El algoritmo de programación subóptima de TCAM para la sección TCAM2 de este documento discute estas optimizaciones.

Para el TCAM2 y TCAM3 en el Catalyst 4500, se comparten las entradas TCAM si el mismo ACL se aplica en diversas interfaces. Esta optimización guarda el espacio TCAM.

Agotamiento de TCAM del Troubleshooting

Cuando el agotamiento de TCAM ocurre en los Catalyst 4500 Switch durante la programación de un ACL de seguridad, una aplicación parcial del ACL ocurre vía el trayecto por software. Los

paquetes que hacen juego a los aces que no se aplican en el TCAM se procesan en el software. Esto que procesa en el software causa CPU elevada la utilización. Porque la programación del Catalyst 4500 ACL es dependiente de la orden, el ACL se programa siempre de arriba hacia abajo. Si un ACL específico no cabe totalmente en el TCAM, no programan a los aces en la porción inferior del ACL muy probablemente en el TCAM.

Un mensaje de advertencia aparece cuando sucede un desbordamiento 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.
```

Usted puede también ver este mensaje de error en el **comando show logging** hecho salir si usted ha habilitado el Syslog. La presencia de este mensaje indica concluyente que ocurrirá un cierto proceso del software. Por lo tanto, puede haber CPU elevada utilización. El ACL que se ha programado ya en los restos TCAM programó en el TCAM si el agotamiento de la capacidad TCAM ocurre durante la aplicación del nuevo ACL. Los paquetes que hacen juego los ACL que se han programado ya continúan siendo procesados y siendo remitidos en hardware.

Nota: Si usted realiza los cambios a un ACL grande, el mensaje TCAM-excedido puede ser visualizado. El Switch intenta reprogramar el ACL en el TCAM. En la mayoría de los casos, el ACL nuevo, modificado se puede reprogramar completamente en hardware. Si el Switch puede reprogramar con éxito el ACL en la totalidad en el TCAM, este mensaje aparece:

```
*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 el ACL está programado completamente en hardware.

Esta salida muestra la configuración del ACL 101 al VLAN1 y a la verificación que el ACL está programado completamente en hardware:

Nota: Si el ACL no se programa completamente, un mensaje de error del agotamiento de TCAM puede visualizar.

```
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 de los `indicadores` (`L3DenyToCpu`) indica que, si un paquete se niega debido al ACL, el paquete está llevado en batea al CPU. El Switch entonces envía un mensaje inalcanzable del Protocolo de mensaje de control de Internet (ICMP). Este comportamiento es el valor por defecto. Cuando los paquetes se llevan en batea al CPU, CPU elevada la utilización puede ocurrir en el Switch. Sin embargo, en el Cisco IOS Software Release 12.1(13)EW y Posterior, estos paquetes son tarifa limitada al CPU. En la mayoría de los casos, Cisco recomienda que usted apaga la característica que envía los mensajes inalcanzables de ICMP.

Esta salida muestra la configuración del Switch para no enviar los mensajes inalcanzables de ICMP y la verificación del TCAM que programa después del cambio. El estado del ACL 101 ahora

es `FullyLoaded`, como la salida de comando muestra. El tráfico denegado no va al 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 el QoS TCAM se excede durante la aplicación de un seguro política de calidad de servicio (QoS), esa directiva específica no se aplica a la interfaz o al VLA N. El Catalyst 4500 no implementa política de calidad de servicio (QoS) adentro el trayecto por software. Por lo tanto, la utilización de la CPU no clava cuando se excede QoS TCAM.

```
*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.
```

Publique el **comando show platform cpu packet statistics**. Determine si el `interruptor ACL que procesa la` cola recibe un número alto de paquetes. Un número alto de paquetes indica el agotamiento de la Seguridad TCAM. Este agotamiento de TCAM hace los paquetes ser enviado al CPU para la expedición 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
```

Si usted encuentra que el `interruptor ACL que procesa la` cola no recibe una cantidad excesiva de tráfico, refiera CPU elevada a la utilización en los Catalyst 4500 Switch basados en software del Cisco IOS para otras posibles causas. El documento proporciona la información sobre cómo resolver problemas otros CPU elevada Escenarios de utilización.

El Catalyst 4500 TCAM puede desbordar por estas razones:

- Un algoritmo de programación subóptima de TCAM para el TCAM2
- El uso excesivo de las operaciones de la capa 4 (L4Ops) en un ACL
- ACL excesivos para el Supervisor Engine o el tipo de switch

Algoritmo de programación subóptima de TCAM para el TCAM2

Pues los tipos de la sección de TCAM discuten, la eficacia TCAM2 es más bajo debido al hecho de que ocho entradas comparten una máscara. El software del Catalyst 4500 permite dos tipos de algoritmos programados TCAM para el TCAM2 que mejoren la eficacia del TCAM2:

- Pila de discos — Conveniente para la mayoría de los escenarios del ACL de seguridad**Nota:** Este es el valor predeterminado.
- Dispersado — Utilizado en el escenario IPSG

Usted puede cambiar el algoritmo a un algoritmo dispersado, pero éste no ayuda típicamente si usted ha configurado solamente los ACL de seguridades, tales como RACL. El algoritmo dispersado es solamente eficaz en los escenarios donde lo mismo o un ACL similar, pequeño se relanza en los puertos numerosos. Este escenario es el caso con un IPSG que se habilita en las interfaces múltiples. En el escenario IPSG, cada ACL dinámico:

- Tiene una pequeña cantidad de entradasEsto incluye los permisos para los IP Addresses permitidos y una negación en el extremo para prevenir el acceso del puerto por los IP Addresses desautorizados.
- Se relanza para todos los puertos de acceso configuradoEl ACL se relanza para hasta 240 puertos en un Catalyst 4507R.

Nota: TCAM3 utiliza el algoritmo pila de discos valor por defecto. Porque la estructura TCAM es una máscara por la entrada, el algoritmo pila de discos es el algoritmo mejor. Por lo tanto, la opción dispersada del algoritmo no se habilita en este Switches.

Este ejemplo está en un Supervisor Engine II+ que se configura para la característica del IPSG. La salida muestra que, aunque el solamente 49 por ciento de las entradas se utilice, el 89 por ciento de las máscaras está consumido:

```
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 programado del valor por defecto pila de discos el algoritmo a las ayudas dispersadas del algoritmo. El algoritmo dispersado reduce el uso total de la máscara a partir del 89 por ciento al 49 por ciento.

```
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 la información sobre las mejores prácticas para las funciones de seguridad en los Catalyst 4500 Switch, refiera a las mejores prácticas de las funciones de seguridad del Catalyst 4500 para los supervisores.

Uso excesivo del L4Ops en un ACL

El L4Ops del término refiere al uso del **gt**, del **lt**, del **neq**, y de las palabras claves del **rango** en la configuración ACL. El Catalyst 4500 tiene límites en el número de estas palabras claves que usted pueda utilizar en un solo ACL. La limitación, que varía por el Supervisor Engine y el Switch, es seis u ocho L4Ops por el ACL. El cuadro 3 muestra el límite por el Supervisor Engine y por el

ACL.

Cuadro 3 – Límite del L4Op por el ACL en los diversos motores y Switches del supervisor del Catalyst 4500

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

Si el límite del L4Op por el ACL se excede, un mensaje de advertencia se visualiza 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.
```

También, si se excede el límite del L4Op, el específico ACE se amplía en el TCAM. Resultados adicionales de la utilización de TCAM. Este ACE sirve como un ejemplo:

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

Con este ACE en un ACL, el Switch utiliza solamente una entrada y un L4Op. Sin embargo, si seis L4Ops se utilizan ya en este ACL, este ACE se amplía a 10 entradas en el hardware. Tal extensión puede potencialmente utilizar encima de muchas entradas en el TCAM. El uso cuidadoso de este L4Ops previene el desbordamiento TCAM.

Nota: Si este caso implica el V-10GE del Supervisor Engine y WS-C4948-10GE, ocho L4Ops previamente usados en el ACL dan lugar a la extensión de ACE.

Tenga estos elementos presente cuando usted utiliza el L4Op en los Catalyst 4500 Switch:

- Las operaciones L4 se consideran diferentes si diferencia el operador o el operando.Por ejemplo, este ACL contiene tres diversas operaciones L4 porque el **gt 10** y el **gt 11** se consideran dos diversas operaciones 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**`
- Las operaciones L4 se consideran diferentes si el mismo par del operador/del operando se aplica una vez a un puerto de origen y una vez a un puerto 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 Catalyst 4500 Switch comparten el L4Ops cuando son posibles.En este ejemplo, las líneas en los ***itálicos negrita*** demuestran este escenario:Uso del L4Op para el ACL 101 = 5Uso del L4Op para el ACL 102 = 4 **Nota:** La palabra clave del **eq** no consume al Recurso de hardware un de los del L4Op.Uso total del L4Op = **8Nota:** ACL 101 y 102 L4Op de la parte una.**Nota:** Se comparte el L4Op incluso si el protocolo, tal como TCP o User Datagram Protocol (UDP), no hace juego o el permiso/niega la acción no hace juego.

ACL excesivos para el Supervisor Engine o el tipo de switch

Como cuadro 2 muestra, TCAM es un recurso limitado. Usted puede exceder al Recurso TCAM de cualquier Supervisor Engine si usted configura los ACL excesivos o las características como el IPSG con un número alto de entradas del IPSG.

Si usted excede el espacio TCAM para su Supervisor Engine, tome estas medidas:

- Si usted tiene un Supervisor Engine II+ y usted funciona con una versión de Cisco IOS Software que sea *anterior* que el Cisco IOS Software Release 12.2(18)EW, actualice a la última versión de mantenimiento del Cisco IOS Software Release 12.2(25)EWA.La capacidad TCAM se ha aumentado de las versiones posteriores.
- Si usted utiliza el snooping y el IPSG del DHCP y usted comienza a ejecutarse del TCAM, a utilizar la última versión de mantenimiento del Cisco IOS Software Release 12.2(25)EWA y a utilizar el algoritmo dispersado en el caso de los Productos TCAM2.**Nota:** El algoritmo dispersado está disponible en el Cisco IOS Software Release 12.2(20)EW y Posterior.La última versión también tiene mejoras para una mejor utilización de TCAM con el snooping DCHP y las características del examen del Address Resolution Protocol (ARP) dinámico (DAI).
- Si usted comienza a ejecutarse del TCAM porque se excede el límite del L4Op, intente reducir el uso del L4Op en el ACL para prevenir el desbordamiento TCAM.
- Si usted utiliza muchos ACL o directivas similares en los diversos puertos en el mismo VLA N, agregue los en un solo ACL o la directiva en la interfaz VLAN.Esta agregación guarda un cierto espacio TCAM. Por ejemplo, cuando usted aplica las directivas Voz-basadas, el acceso basado predeterminado QoS se utiliza para la clasificación. Este valor por defecto QoS puede causar la capacidad TCAM de ser excedido. Si usted conmuta el QoS a VLAN basado, usted reduce el uso TCAM.
- Si usted todavía tiene los problemas con el TCAM espacian, consideran un Supervisor Engine de gama alta, tal como el V-10GE o el Catalyst 4948-10GE del Supervisor Engine.Estos Productos utilizan TCAM3 el hardware más eficiente.

Resumen

El Catalyst 4500 programa los ACL configurados con el uso del TCAM. El TCAM permite la aplicación de los ACL en la trayectoria del hardware que reenvía sin el impacto en el funcionamiento del Switch. El funcionamiento es constante a pesar del tamaño del ACL porque el funcionamiento de las búsquedas ACL está en la línea tarifa. Sin embargo, el TCAM es un recurso limitado. Por lo tanto, si usted configura una cantidad excesiva de entradas ACL, usted excede la capacidad TCAM. El Catalyst 4500 ha implementado las variadas optimizaciones y con tal que los comandos de variar el algoritmo programado del TCAM para alcanzar la máxima eficiencia. TCAM3 los Productos tales como el V-10GE del Supervisor Engine y el Catalyst 4948-10GE ofrecen a la mayoría de los Recursos TCAM para el ACL de seguridad y las directivas de QoS.

Información Relacionada

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