Catalyst 4500 스위치에서 ACL 및 QoS TCAM 소모 방지

목차

소개

Cisco Catalyst 4500 및 Catalyst 4948 시리즈 스위치는 TCAM(Ternary Content Addressable Memory)을 사용하여 유선 속도 ACL(Access Control List) 및 QoS 기능을 지원합니다. ACL과 정책을 활성화해도 TCAM에 ACL이 완전히 로드되는 한 스위치의 스위칭 또는 라우팅 성능이 저하되지 않습니다. TCAM이 모두 사용되면 CPU 경로를 통해 패킷을 전달할 수 있으므로 해당 패킷의 성능이 저하될 수 있습니다. 이 문서에서는 다음에 대한 세부 정보를 제공합니다.

- Catalyst 4500 및 Catalyst 4948에서 사용하는 다양한 유형의 TCAM
- Catalyst 4500에서 TCAM을 프로그래밍하는 방법
- TCAM 소모를 피하기 위해 스위치에서 ACL 및 TCAM을 최적으로 구성하는 방법

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 4500 시리즈 스위치
- Catalyst 4948 시리즈 스위치

참고: 이 문서는 Cisco IOS® 소프트웨어 기반 스위치에만 적용되며 Catalyst OS(CatOS) 기반 스위치에는 적용되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

하드웨어에서 다양한 유형의 ACL 및 QoS 정책을 구현하기 위해 Catalyst 4500은 TCAM(하드웨어 조회 테이블)과 다양한 하드웨어 레지스터를 Supervisor Engine에 프로그래밍합니다. 패킷이 도착하면 스위치에서 하드웨어 테이블 조회(TCAM 조회)를 수행하고 패킷을 허용하거나 거부합니다.

Catalyst 4500은 다양한 유형의 ACL을 지원합니다. 표 1에는 이러한 유형의 ACL이 요약되어 있습니다.

표 1 - Catalyst 4500 스위치에서 지원되는 ACL 유형

ACL 유형	적용 위치	제어 트래픽	방향
RACL[1]	L3[2] 포트, L3 채널 또는 SVI[3](VLAN)	라우팅된 IP 트래픽	인바운드 또는 아웃바운드
VACL[4]	VLAN(vlan **filter** 명령을 통해)	VLAN으로 라우팅되거나 VLAN 내에 브리징된 모든 패킷	방향 없음
PACL[5]	L2[6] 포트 또는 L2 채널	모든 IP 트래픽 및 비 IPv4[7] 트래픽(MAC ACL을 통해)	인바운드 또는 아웃바운드

[1] RACL = 라우터 ACL

[2] L3 = 레이어 3

[3] SVI = 스위치 가상 인터페이스

[4] VACL = VLAN ACL

[5] PACL = 포트 ACL

[6] L2 = 레이어 2

[7] IPv4 = IP 버전 4

Catalyst 4500 ACL 및 QoS 하드웨어 프로그래밍 아키텍처

Catalyst 4500 TCAM에는 다음과 같은 항목이 있습니다.

- 보안 ACL에 대한 32,000개의 항목(기능 ACL이라고도 함)
- QoS ACL에 대한 32,000개 항목

보안 ACL과 QoS ACL의 경우 항목은 다음과 같은 방법으로 전용됩니다.

- 입력 방향에 대한 16,000개 항목
- 출력 방향에 대한 16,000개 항목

그림 3은 TCAM 진입 방식을 보여줍니다. TCAM에 대한 자세한 내용은 TCAM의 유형 섹션을 참조하십시오.

표 2는 다양한 Catalyst 4500 Supervisor Engine 및 스위치에 사용할 수 있는 ACL 리소스를 보여줍니다.

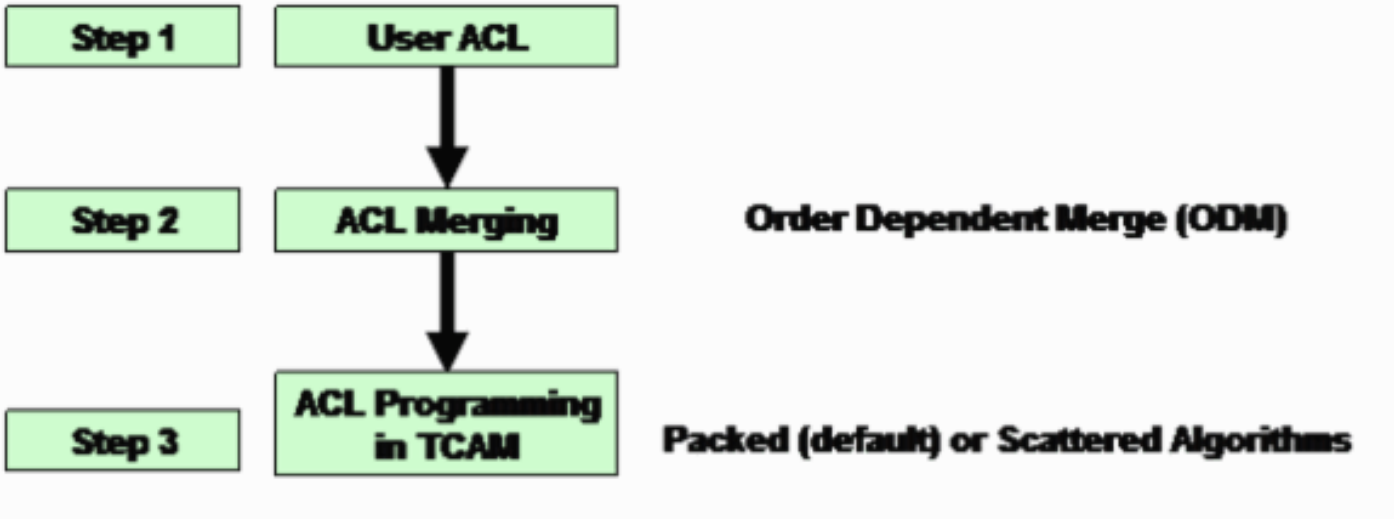
표 2 - 다양한 수퍼바이저 엔진 및 스위치의 Catalyst 4500 ACL 리소스

제품	TCAM 버전	기능 TCAM(방향별)	QoS TCAM(방향별)
Supervisor Engine II+	2	8,000개 항목, 1,000개 마스크	8,000개 항목, 1,000개 마스크
Supervisor Engine II+TS/III/IV/V 및 WS-C4948	2	16,000개 항목, 2,000개 마스크	16,000개 항목, 2,000개 마스크
Supervisor Engine V-10GE 및 WS-C4948-10GE	3	16,000개 항목, 16,000개 마스크	16,000개 항목, 16,000개 마스크

Catalyst 4500은 IP 유니캐스트 및 멀티캐스트 라우팅에 별도의 전용 TCAM을 사용합니다. Catalyst 4500은 유니캐스트 및 멀티캐스트 경로가 공유하는 최대 128,000개의 경로 항목을 가질 수 있습니다. 그러나 이러한 세부사항은 이 문서의 범위를 벗어납니다. 이 문서에서는 보안 및 QoS TCAM 소모 문제에 대해서만 설명합니다.

그림 1은 Catalyst 4500의 하드웨어 테이블에서 ACL을 프로그래밍하는 단계를 보여줍니다.

그림 1 - Catalyst 4500 스위치에서 ACL 프로그램 단계



1단계

이 단계에는 다음 작업 중 하나가 포함됩니다.

- 인터페이스 또는 VLAN에 대한 ACL 또는 QoS 정책의 구성 및 적용ACL을 동적으로 생성할 수 있습니다. 예를 들면 IP Source Guard(IPSG) 기능의 예입니다. 이 기능을 사용하면 스위치가 포트와 연결된 IP 주소에 대한 PACL을 자동으로 생성합니다.
- 이미 존재하는 ACL 수정

참고: ACL의 컨피그레이션만으로 TCAM 프로그래밍이 발생하지 않습니다. TCAM에서 ACL을 프로그래밍하려면 인터페이스에 ACL(QoS 정책)을 적용해야 합니다.

2단계

ACL은 TCAM(하드웨어 테이블)에서 프로그래밍하려면 먼저 병합해야 합니다. 병합은 하드웨어에서 여러 ACL(PACL, VACL 또는 RACL)을 결합된 방식으로 프로그래밍합니다. 이러한 방법으로 패킷 논리적 포워딩 경로의 모든 적용 가능한 ACL을 확인하려면 단일 하드웨어 조회만 필요합니다.

예를 들어 그림 2에서 PC-A에서 PC-C로 라우팅된 패킷은 잠재적으로 다음 ACL을 가질 수 있습니다.

- PC-A 포트의 입력 PACL
- VLAN 1의 VACL
- 입력 방향의 VLAN 1 인터페이스에 대한 입력 RACL

이러한 3개의 ACL은 병합되어 입력 TCAM의 단일 조회가 허용 또는 거부를 결정하는 데 충분합니다. 마찬가지로, TCAM이 다음 세 ACL의 병합 결과와 함께 프로그래밍되므로 단일 출력 조회만 필요합니다.

- VLAN 2 인터페이스의 출력 RACL
- VLAN 2 VACL
- PC-C 포트의 출력 PACL

입력 및 출력에 대한 단일 조회를 통해 이러한 ACL 중 하나 또는 모두가 패킷 전달 경로에 있는 경우 패킷의 페널티 하드웨어 포워딩이 없습니다.

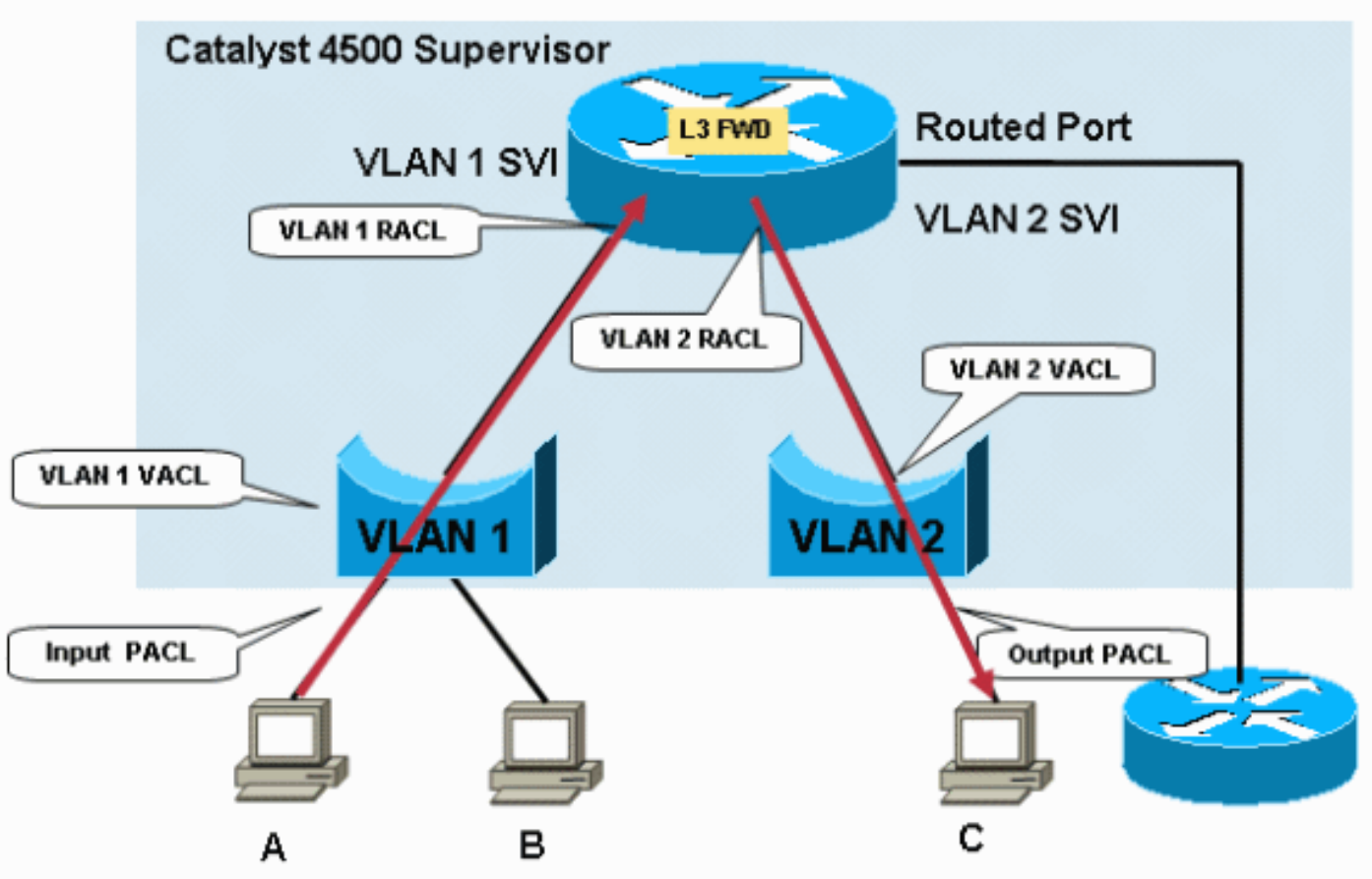
참고: 입력 및 출력 TCAM 조회는 하드웨어에서 동시에 발생합니다. 일반적으로 잘못된 생각으로는 출력 TCAM 조회가 입력 TCAM 조회 후에 일어나며, 이는 논리적 패킷 흐름에서 알 수 있습니다. Catalyst 4500 출력 정책은 입력 정책 수정 QoS 매개변수에서 확인할 수 없으므로 이 정보를 이해

하는 것이 중요합니다. 보안 ACL의 경우 가장 심각한 작업이 발생합니다. 다음 상황 중 하나에서 패킷이 삭제됩니다.

- 입력 조회 결과가 삭제되고 출력 조회 결과가 permit인 경우
- 입력 조회 결과가 허용이고 출력 조회 결과가 삭제되는 경우

참고: 입력 및 출력 조회 결과가 모두 허용되는 경우 패킷이 허용됩니다.

그림 2 - Catalyst 4500 스위치에서 보안 ACL을 통한 필터링



Catalyst 4500의 ACL 병합은 주문에 따라 다릅니다. 이 프로세스를 ODM(주문 종속 병합)이라고도 합니다. ODM을 사용하면 ACL 항목이 ACL에 나타나는 순서대로 프로그래밍됩니다. 예를 들어, ACL에 ACE(액세스 제어 항목)가 두 개 포함된 경우, 스위치 프로그램은 ACE 1을 먼저 프로그래밍한 다음 ACE 2를 프로그래밍합니다. 그러나 주문 의존성은 특정 ACL 내의 ACE에만 적용됩니다. 예를 들어 ACL 120의 ACE는 TCAM의 ACL 100에서 ACE보다 먼저 시작할 수 있습니다.

3단계

병합된 ACL은 TCAM에 프로그래밍됩니다. ACL 또는 QoS용 입력 또는 출력 TCAM은 PortAndVlan 및 PortOrVlan이라는 두 영역으로 추가로 분할됩니다. 컨피그레이션에 동일한 패킷 경로에 이러한 ACL이 *모두* 있는 경우 병합된 ACL은 TCAM의 PortAndVlan 영역에 프로그래밍됩니다.

- PACL**참고:** PACL은 일반적인 필터링 ACL 또는 IPSG에서 생성한 동적 ACL입니다.
- VACL 또는 RACL

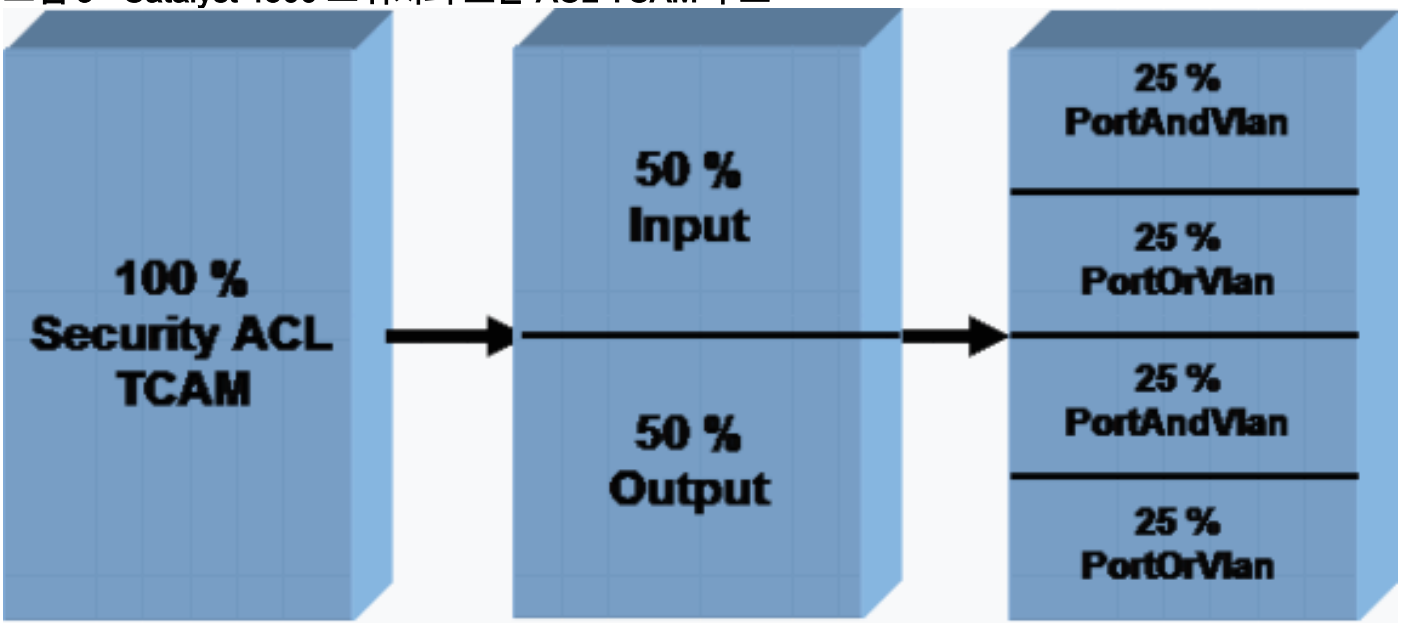
패킷의 특정 경로에 PACL, VACL 또는 RACL만 있는 경우 TCAM의 PortOrVlan 영역에서 ACL이 프로그래밍됩니다. 그림 3은 다양한 유형의 ACL에 대한 보안 ACL TCAM 조각을 보여줍니다. QoS에는 이와 비슷하게 조각화된 전용 TCAM이 있습니다.

현재 TCAM 기본 할당을 수정할 수 없습니다. 그러나 향후 소프트웨어 릴리스에서 PortAndVlan 및

PortOrVlan 영역에 사용할 수 있는 TCAM 할당을 변경할 수 있는 기능을 제공할 계획입니다. 이 변경을 통해 입력 또는 출력 TCAM에서 PortAndVlan 및 PortOrVlan의 공간을 늘리거나 줄일 수 있습니다.

참고: PortAndVlan 영역에 대한 할당이 증가하면 입력 또는 출력 TCAM의 PortOrVlan 영역에 대해 동일한 감소가 발생합니다.

그림 3 - Catalyst 4500 스위치의 보안 ACL TCAM 구조



show **platform hardware ACL statistics utilization brief** 명령은 ACL 및 QoS TCAM에 대해 영역별 이 TCAM 사용률을 표시합니다. 명령 출력은 그림 3과 같이 사용 가능한 마스크와 항목을 표시하고 영역으로 나눕니다. 이 샘플 출력은 Catalyst 4500 Supervisor Engine II+에서 가져온 것입니다.

참고: 마스크 및 항목에 대한 자세한 내용은 이 문서의 TCAM 유형 섹션을 참조하십시오.

```
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
```

TCAM 유형

Catalyst 4500은 표 2에 나와 있는 것처럼 두 가지 유형의 TCAM을 사용합니다. 이 섹션에서는 네트워크와 구성에 적합한 제품을 선택할 수 있도록 두 TCAM 버전 간의 차이를 보여줍니다.

TCAM 2는 8개의 항목이 하나의 마스크를 공유하는 구조를 사용합니다. 예를 들어 ACE에 8개의 IP 주소가 있습니다. 항목은 공유되는 마스크와 동일한 마스크를 가져야 합니다. ACE에 다른 마스크가 있는 경우, 항목은 필요에 따라 별도의 마스크를 사용해야 합니다. 이러한 별도의 마스크를 사용하면 마스크 용해가 발생할 수 있습니다. TCAM의 마스크 소모는 TCAM이 고갈되는 일반적인 이유 중 하나입니다.

TCAM 3에는 그러한 제한이 없습니다. 각 항목은 TCAM에 고유한 마스크를 가질 수 있습니다. 해당 항목의 마스크와 상관없이 하드웨어에서 사용 가능한 모든 항목의 전체 사용률이 가능합니다.

이 하드웨어 아키텍처를 시연하기 위해 이 섹션의 예에는 하드웨어에서 TCAM 2 및 TCAM 3 프로그램 ACL이 어떻게 표시되는지 나와 있습니다.

```
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
```

이 샘플 ACL에는 두 개의 다른 마스크가 있는 두 개의 항목이 있습니다. ACE 1은 호스트 항목이므로 /32 마스크가 있습니다. ACE 2는 /24 마스크가 있는 서브넷 항목입니다. 두 번째 엔트리에 마스크가 다르므로 마스크 1의 빈 엔트리를 사용할 수 없으며 TCAM 2의 경우에는 별도의 마스크를 사용합니다.

다음 표는 TCAM 2에서 이 ACL을 프로그래밍하는 방법을 보여줍니다.

마스크	**항목**
마스크 1 일치: 소스 IP 주소의 모든 32비트 "Don't care": 모든 나머지 비트	소스 IP = 8.1.1.1
	빈 항목 2
	빈 항목 3
	빈 항목 4
	빈 항목 5
	빈 항목 6
	빈 항목 7
	빈 항목 8
마스크 2 일치: 소스 IP 주소 "Don't care"의 가장 중요한 24비트: 모든 나머지 비트	소스 IP = 8.1.1.0
	빈 항목 2
	빈 항목 3
	빈 항목 4
	빈 항목 5
	빈 항목 6
	빈 항목 7
	빈 항목 8

마스크 1의 일부로 사용 가능한 항목이 있지만 TCAM 2 구조에서는 마스크 1의 빈 항목 2에 ACE 2를 채우는 것을 방지합니다. ACE 2의 마스크가 ACE 1의 /32 마스크와 일치하지 않으므로 이 마스크를 사용할 수 없습니다. TCAM 2는 별도의 마스크인 /24 마스크를 사용하여 ACE 2를 프로그래밍해야 합니다.

이렇게 별도의 마스크를 사용하면 표 2에서 볼 수 있듯이 사용 가능한 리소스를 더 빠르게 소모할 수 있습니다. 다른 ACL은 여전히 마스크 1의 나머지 항목을 사용할 수 있습니다. 그러나 대부분의 경우 TCAM 2의 효율성은 높지만 100%는 아닙니다. 효율성은 각 컨피그레이션 시나리오에 따라 달라집니다.

이 표는 TCAM 3에서 프로그래밍된 것과 동일한 ACL을 보여줍니다. TCAM 3은 각 항목에 대해 마스크를 할당합니다.

마스크	항목
IP 주소 1의 마스크 32비트	소스 IP = 8.1.1.1
IP 주소 2의 마스크 24비트	소스 IP = 8.1.1.0
빈 마스크 3	빈 항목 3
빈 마스크 4	빈 항목 4
빈 마스크 5	빈 항목 5
빈 마스크 6	빈 항목 6
빈 마스크 7	빈 항목 7
빈 마스크 8	빈 항목 8
빈 마스크 9	빈 항목 9
빈 마스크 10	빈 항목 10
빈 마스크 11	빈 항목 11
빈 마스크 12	빈 항목 12
빈 마스크 13	빈 항목 13
빈 마스크 14	빈 항목 14
빈 마스크 15	빈 항목 15
빈 마스크 16	빈 항목 16

이 예에서 나머지 14개의 항목은 각각 다른 마스크와 제한 없이 항목을 가질 수 있습니다. 따라서 TCAM 3은 TCAM 2보다 훨씬 효율적입니다. 이 예제는 TCAM 버전 간의 차이를 설명하기 위해 너무 단순합니다. Catalyst 4500 소프트웨어는 TCAM 2에서 실제 구성 시나리오에 대한 프로그래밍 효율성을 높이기 위한 여러 가지 최적화를 갖추고 있습니다. 이 문서의 TCAM 2 섹션에 대한 Suboptimal TCAM 프로그래밍 알고리즘에서는 이러한 최적화에 대해 설명합니다.

Catalyst 4500의 TCAM 2 및 TCAM 3에 대해 동일한 ACL이 다른 인터페이스에 적용되는 경우 TCAM 항목이 공유됩니다. 이 최적화를 통해 TCAM 공간이 절약됩니다.

TCAM 소모 문제 해결

보안 ACL을 프로그래밍하는 동안 Catalyst 4500 스위치에서 TCAM 소모가 발생하는 경우 소프트웨어 경로를 통해 ACL의 부분 애플리케이션이 발생합니다. TCAM에 적용되지 않은 ACE와 일치하는 패킷은 소프트웨어에서 처리됩니다. 소프트웨어에서 이 프로세싱을 수행하면 CPU 사용률이 높습니다. Catalyst 4500 ACL 프로그래밍은 순서에 따라 다르므로 ACL은 항상 위에서 아래로 프로그래밍됩니다. 특정 ACL이 TCAM에 완전히 맞지 않을 경우 ACL의 하단 부분에 있는 ACE는 TCAM에 프로그래밍되지 않습니다.

TCAM 오버플로가 발생하면 경고 메시지가 나타납니다. 예를 들면 다음과 같습니다.

```
%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.
```

syslog를 활성화한 경우 **show logging** 명령 출력에서도 이 오류 메시지를 볼 수 있습니다. 이 메시지가 있으면 일부 소프트웨어 처리가 발생함을 명확하게 나타냅니다. 따라서 CPU 사용률이 높을 수 있습니다. TCAM에서 이미 프로그래밍된 ACL은 새 ACL을 적용하는 동안 TCAM 용량 소모가 발생할 경우 TCAM에서 프로그래밍된 상태로 유지됩니다. 이미 프로그래밍된 ACL과 일치하는 패킷은 하드웨어에서 계속 처리되고 전달됩니다.

참고: 대규모 ACL을 변경하면 TCAM 초과 메시지가 표시될 수 있습니다. 스위치는 TCAM에서 ACL을 다시 프로그래밍하려고 시도합니다. 대부분의 경우, 새로운 수정된 ACL은 하드웨어에서 완전히 재프로그래밍될 수 있습니다. 스위치가 ACL을 완전히 TCAM으로 다시 프로그래밍할 수 있는 경우 다음 메시지가 나타납니다.

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

ACL이 하드웨어에서 완전히 프로그래밍되었는지 확인하려면 **show platform software acl input summary interface *interface-id*** 명령을 사용합니다.

이 출력은 ACL 101을 VLAN 1에 대한 컨피그레이션과 ACL이 하드웨어에서 완전히 프로그래밍되었는지 확인하는 것을 보여줍니다.

참고: ACL이 완전히 프로그래밍되지 않은 경우 TCAM 소모 오류 메시지가 표시될 수 있습니다.

```
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
```

Flags(Flags) 필드(L3DenyToCpu)는 ACL로 인해 패킷이 거부된 경우 패킷이 CPU에 펀딩됨을 나타냅니다. 그런 다음 스위치는 ICMP(Internet Control Message Protocol) 연결 불가 메시지를 전송합니다. 이 동작이 기본값입니다. 패킷이 CPU에 펀딩되면 스위치에서 높은 CPU 사용률이 발생할 수 있습니다. 그러나 Cisco IOS Software 릴리스 12.1(13)EW 이상에서는 이러한 패킷의 속도가 CPU로 제한됩니다. 대부분의 경우 Cisco에서는 ICMP 연결 불가 메시지를 전송하는 기능을 끄는 것이 좋습니다.

이 출력은 ICMP 연결 불가 메시지를 보내지 않도록 스위치의 컨피그레이션 및 변경 후 TCAM 프로그래밍의 확인을 보여줍니다. ACL 101의 상태가 명령 출력에 표시된 대로 FullyLoaded로 변경되었습니다. 거부된 트래픽은 CPU로 이동하지 않습니다.

```
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
```

참고: 특정 QoS 정책을 적용하는 동안 QoS TCAM이 초과되면 해당 특정 정책이 인터페이스 또는 VLAN에 적용되지 *않습니다*. Catalyst 4500은 소프트웨어 경로에 QoS 정책을 구현하지 않습니다. 따라서 QoS TCAM을 초과할 경우 CPU 사용률이 증가하지 않습니다.

```
*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.
```

show platform cpu packet statistics 명령어를 실행합니다. ACL 큐가 많은 패킷을 수신하는지 확인합니다. 패킷이 많을수록 보안 TCAM의 소모가 나타납니다. 이 TCAM 소모 때문에 소프트웨어 전달을 위해 패킷이 CPU로 전송됩니다.

```
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
```

ACL 대기열에서 과도한 양의 트래픽이 수신되지 않는 경우 Cisco IOS Software-Based Catalyst 4500 스위치에서 높은 CPU 사용률을 참조하여 가능한 다른 원인을 확인하십시오. 이 문서에서는 다른 높은 CPU 사용률 시나리오를 해결하는 방법에 대한 정보를 제공합니다.

Catalyst 4500 TCAM은 다음과 같은 이유로 오버플로가 발생할 수 있습니다.

- TCAM 2를 위한 최적 이하의 TCAM 프로그래밍 알고리즘
- ACL에서 레이어 4 작업(L4Ops)을 과도하게 사용하는 경우
- 수퍼바이저 엔진 또는 스위치 유형에 대한 과도한 ACL

TCAM 2를 위한 비최적 TCAM 프로그래밍 알고리즘

TCAM의 유형에 대해 설명하면 8개의 항목이 하나의 마스크를 공유하므로 TCAM 2의 효율성이 낮아집니다. Catalyst 4500 소프트웨어는 TCAM 2의 효율성을 개선하는 두 가지 유형의 TCAM 프로그래밍 알고리즘을 지원합니다.

- 패키지—대부분의 보안 ACL 시나리오에 적합**참고:** 이것이 기본값입니다.

- 분산형 - IPSG 시나리오에서 사용됩니다.

알고리즘을 산발적 알고리즘으로 변경할 수 있지만, 일반적으로 RACL과 같은 보안 ACL만 구성한 경우에는 이 방법이 도움이 되지 않습니다. 산발적인 알고리즘은 여러 포트에서 동일하거나 유사한 소규모 ACL이 반복되는 경우에만 효과적입니다. 이 시나리오는 여러 인터페이스에서 활성화된 IPSG의 경우입니다. IPSG 시나리오에서 각 동적 ACL은 다음과 같습니다.

- 항목 수가 적음여기에는 허용되는 IP 주소에 대한 허가와 무단 IP 주소에 의한 포트 액세스를 방지하기 위한 엔드 투 엔드 거부가 포함됩니다.
- 구성된 모든 액세스 포트에 대해 반복됩니다.Catalyst 4507R에서 최대 240개의 포트에 대해 ACL이 반복됩니다.

참고: TCAM 3은 기본 압축 알고리즘을 사용합니다. TCAM 구조는 엔트리당 하나의 마스크이기 때문에 압축 알고리즘이 최상의 알고리즘입니다. 따라서 이러한 스위치에서는 분산형 알고리즘 옵션이 활성화되지 않습니다.

이 예는 IPSG 기능에 대해 구성된 Supervisor Engine II+에 있습니다. 이 출력에 따르면 항목의 49%만 사용되지만 마스크 중 89%가 소비됩니다.

```
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
```

이 경우 기본 압축 알고리즘에서 분산 알고리즘으로 프로그래밍 알고리즘을 변경하면 도움이 됩니다. 분산된 알고리즘은 총 마스크 사용량을 89%에서 49%로 줄입니다.

```
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
```

Catalyst 4500 스위치의 보안 기능에 대한 모범 사례에 대한 자세한 내용은 Catalyst 4500 Security Features Best Practices for Supervisor를 참조하십시오.

ACL에서 L4Ops의 과도한 사용

L4Ops라는 용어는 ACL 컨피그레이션에서 **gt**, **lt**, neq 및 **range** 키워드를 사용하는 것을 의미합니다. Catalyst 4500에는 단일 ACL에서 사용할 수 있는 이러한 키워드의 수에 대한 제한이 있습니다. Supervisor Engine과 스위치에 따라 달라지는 제한 사항은 ACL당 6개 또는 8개의 L4Ops입니다. 표 3에는 Supervisor Engine별 및 ACL별 제한이 나와 있습니다.

표 3 - 다른 Catalyst 4500 Supervisor Engine 및 스위치의 ACL당 L4Op 제한

제품	L4Op
수퍼바이저 엔진 II+/ II+TS	32(ACL당 6개)
Supervisor Engine III/IV/V 및 WS-C4948	32(ACL당 6개)
Supervisor Engine V-10GE 및 WS-C4948-10GE	64(ACL당 8개)

ACL당 L4Op 제한을 초과하면 콘솔에 경고 메시지가 표시됩니다. 메시지는 다음과 유사합니다.

```
%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.
```

또한 L4Op 제한을 초과하면 TCAM에서 특정 ACE가 확장됩니다. 추가 TCAM 사용률 결과. 이 ACE는 다음과 같은 예입니다.

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

ACL에서 이 ACE를 사용하면 스위치는 하나의 엔트리와 하나의 L4Op만 사용합니다. 그러나 이 ACL에서 6개의 L4Ops가 이미 사용되고 있으면 이 ACE는 하드웨어에서 10개의 항목으로 확장됩니다. 이러한 확장은 TCAM의 많은 항목을 사용할 수 있습니다. 이러한 L4Ops를 신중하게 사용하면 TCAM 오버플로가 방지됩니다.

참고: 이 경우 Supervisor Engine V-10GE 및 WS-C4948-10GE가 포함되며, ACL에서 이전에 8개의 L4Ops를 사용한 경우 ACE가 확장됩니다.

Catalyst 4500 스위치에서 L4Op를 사용할 경우 다음 사항에 유의하십시오.

- 연산자나 피연산자가 다른 경우 L4 연산은 서로 다른 것으로 간주됩니다.예를 들어 이 ACL에는 세 가지 다른 L4 작업이 포함되어 있습니다. **gt 10** 및 **gt 11**은 두 개의 서로 다른 L4 작업으로 간주되기 때문입니다.
  ```
  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
  ```
- 동일한 연산자/피연산자 쌍이 소스 포트에 한 번 그리고 목적지 포트에 한 번 적용되는 경우 L4 연산은 다른 것으로 간주됩니다.예를 들면 다음과 같습니다.
  ```
  access-list 101 permit tcp host 8.1.1.1 gt 10 any
  access-list 101 permit tcp host 8.1.1.2 any gt 10
  ```
- Catalyst 4500 스위치는 가능한 경우 L4Ops를 공유합니다.이 예에서 굵은 글꼴의 줄은 다음 시나리오*를 보여줍니다.*ACL 101에 대한 L4Op 사용량 = 5ACL 102에 대한 L4Op 사용량 = 4 **참고**: eq 키워드는 L4Op 하드웨어 리소스를 사용하지 않습니다.총 L4Op 사용량 = **8참고:** ACL 101 및 102는 하나의 L4Op를 공유합니다.**참고:** TCP 또는 UDP(User Datagram Protocol)와 같은 프로토콜이 일치하지 않거나 허용/거부 작업이 일치하지 않는 경우에도 L4Op가 공유됩니다.

수퍼바이저 엔진 또는 스위치 유형에 대한 과도한 ACL

표 2에 나와 있듯이 TCAM은 제한된 리소스입니다. IPSG 항목 수가 많은 IPSG와 같은 과도한 ACL 또는 기능을 구성하는 경우 Supervisor Engine의 TCAM 리소스를 초과할 수 있습니다.

Supervisor Engine의 TCAM 공간을 초과할 경우 다음 단계를 수행하십시오.

- Supervisor Engine II+가 있고 Cisco IOS Software 릴리스 12.2(18)EW *이전*의 Cisco IOS Software 릴리스를 실행하는 경우 최신 Cisco IOS Software 릴리스 12.2(25)EWA 유지 관리 릴리스로 업그레이드하십시오.TCAM 용량은 이후 릴리스에서 증가했습니다.
- DHCP 스누핑 및 IPSG를 사용하는 경우 TCAM이 부족하기 시작하면 최신 Cisco IOS Software 릴리스 12.2(25)EWA 유지 관리 릴리스를 사용하고 TCAM 2 제품의 경우 분산된 알고리즘을 사용합니다.**참고:** Cisco IOS Software Release 12.2(20)EW 이상에서 산발적인 알고리즘을 사용할 수 있습니다.또한 최신 릴리스에서는 DCHP 스누핑 및 DAI(Dynamic Address Resolution Protocol) 검사 기능을 통해 TCAM 활용도를 높일 수 있습니다.
- L4Op 제한이 초과되어 TCAM이 부족하기 시작하면 TCAM 오버플로를 방지하기 위해 ACL에서 L4Op 사용량을 줄여 보십시오.
- 동일한 VLAN의 여러 포트에서 유사한 ACL 또는 정책을 많이 사용하는 경우 이를 VLAN 인터페이스의 단일 ACL 또는 정책에 합산합니다.이 집계는 일부 TCAM 공간을 절약합니다. 예를 들어 음성 기반 정책을 적용할 때 기본 포트 기반 QoS가 분류에 사용됩니다. 이 기본 QoS로 인해 TCAM 용량이 초과될 수 있습니다. QoS를 VLAN 기반으로 전환하면 TCAM 사용량이 줄어듭니다.
- TCAM 공간에 문제가 있는 경우에는 Supervisor Engine V-10GE 또는 Catalyst 4948-10GE와 같은 하이엔드 Supervisor Engine을 고려해 보십시오.이러한 제품은 가장 효율적인 TCAM 3 하드웨어를 사용합니다.

요약

Catalyst 4500은 TCAM을 사용하여 구성된 ACL을 프로그래밍합니다. TCAM을 사용하면 스위치 성능에 영향을 주지 않고 하드웨어 포워딩 경로에서 ACL을 적용할 수 있습니다. ACL 조회의 성능은 회선 속도이므로 ACL의 크기에도 불구하고 성능은 일정합니다. 그러나 TCAM은 한정된 리소스입니다. 따라서 ACL 항목을 지나치게 많이 구성하는 경우 TCAM 용량을 초과하게 됩니다. Catalyst 4500은 여러 최적화를 구현했으며 최대 효율성을 달성하기 위해 TCAM의 프로그래밍 알고리즘을 다르게 하는 명령을 제공했습니다. Supervisor Engine V-10GE 및 Catalyst 4948-10GE와 같은 TCAM 3 제품은 보안 ACL 및 QoS 정책을 위한 TCAM 리소스를 가장 많이 제공합니다.

관련 정보

- LAN 제품 지원 페이지
- LAN 스위칭 지원 페이지
- 기술 지원 및 문서 – Cisco Systems