12000 Series 인터넷 라우터에 액세스 목록 구현

목차

소개

이 문서에서는 Cisco 12000 Series Internet Router의 ACL(Access Control List) 지원에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco 라우터에서 ACL이 작동하는 방법에 대한 기본 지식을 얻을 것을 권장합니다.

ACL 및 해당 애플리케이션에 대한 일반적인 정보는 다음 문서를 참조하십시오.

- 액세스 제어 목록:개요 및 지침

- IP 서비스 구성:IP 패킷 필터링

사용되는 구성 요소

이 문서의 정보는 Cisco 12000 Series 인터넷 라우터를 기반으로 합니다.

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.

Cisco 12000 Series 인터넷 라우터의 ACL 지원 개요

Cisco 12000 Series 인터넷 라우터에서 ACL은 하드웨어(ASIC(Application-Specific Integrated Circuit), 소프트웨어(라인 카드의 CPU) 또는 하드웨어 지원을 사용하여 소프트웨어에서 처리되는 하이브리드 기능으로 처리할 수 있습니다.ACL이 하드웨어나 소프트웨어에서 처리되는지 여부는 ACL 애플리케이션, 라인 카드 엔진 유형 및 다른 라인 카드의 ACL에서의 상호 작용에 따라 달라집니다.

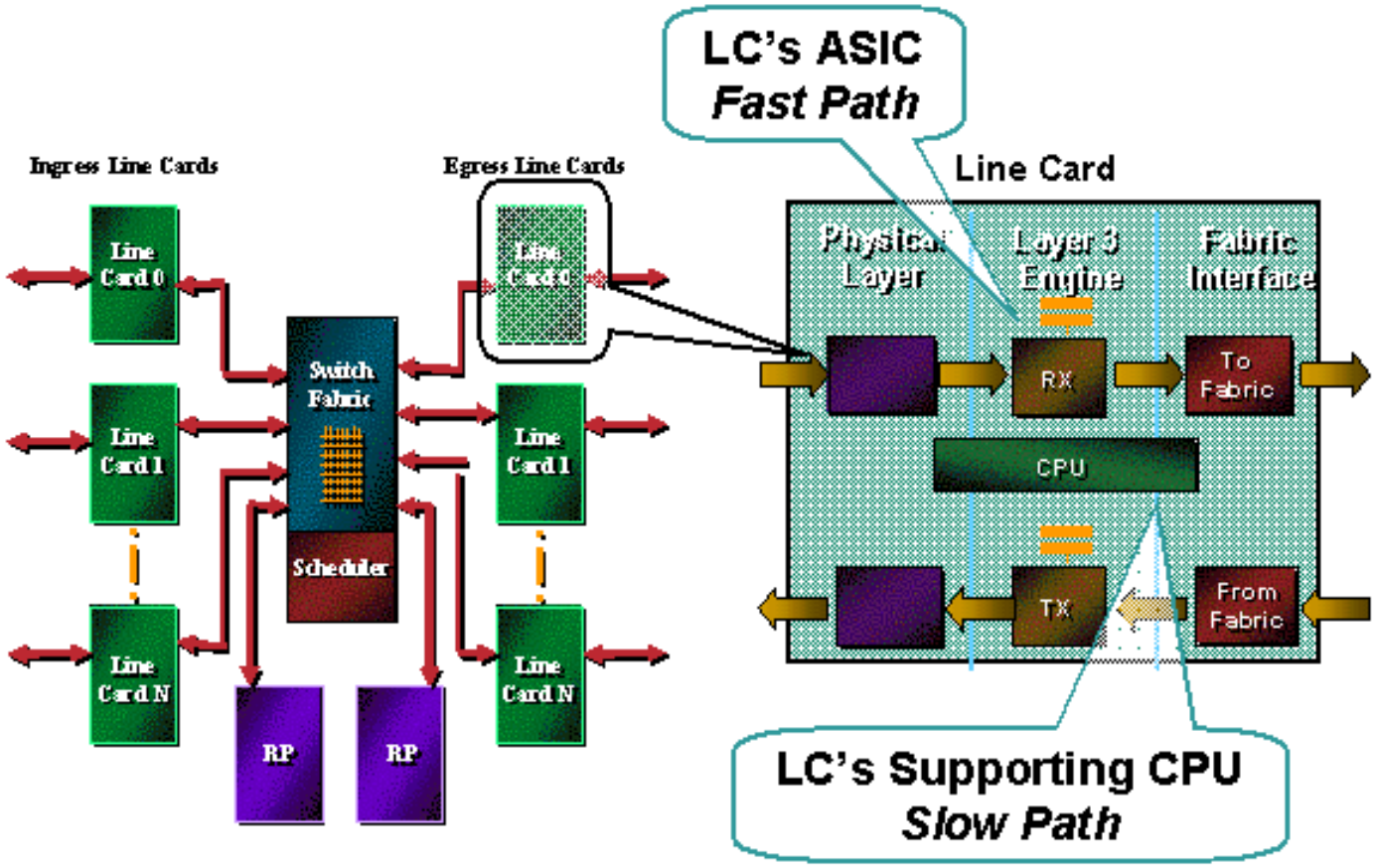
Cisco 12000 Series 라인 카드 엔진은 다양한 ACL 기능을 제공합니다.특정 라인 카드 엔진에 대한 ACL 지원 정보를 보려면 이 문서의 해당 섹션으로 이동하십시오.

참고: IP 멀티캐스트 ACL은 Cisco IOS® 소프트웨어 릴리스 12.0S에서 지원되지 않습니다.멀티캐스트 필터링이 필요한 경우 IP 멀티캐스트 경계 기능을 사용할 수 있습니다.자세한 내용은 Cisco 12000 Series Engine 2 및 ISE 라인 카드의 빠른 경로 멀티캐스트 포워딩을 참조하십시오.

ASIC 기반 ACL과 CPU 기반 ACL 비교

Cisco 12000은 모든 세대의 ACL 처리를 지원합니다.이러한 각 처리 모드가 어떻게 작동, 상호 작용 및 지원되는지를 운영 적으로 파악하는 것은 Cisco 12000에서 효과적인 ACL을 사용하는 데 필수적입니다.

초기 세대의 ACL 프로세싱에서는 프로그래밍 가능한 CPU를 사용하여 ACL을 처리했습니다.시간이 지남에 따라 PPS(Packet per second) 처리 요구 사항은 새로운 CPU의 처리 능력을 초과했습니다.ASIC는 라우터 포워딩 및 기능 기능을 위해 더 높은 PPS 속도를 제공하도록 설계되었습니다.LC(Line Card) CPU에 로드된 ACL이 LC ASIC에 로드되었습니다.ASIC는 더 높은 PPS 속도를 처리하기 위해 급조되었습니다.이러한 2세대 ASIC는 이전 세대의 선구적인 작업을 기반으로 구축되었으며 더 많은 ASIC 기능을 제공합니다.Cisco 12000은 분산형 라우팅 플랫폼이므로 다양한 세대의 ACL 처리 간의 상호 작용으로 운영 혼란이 발생할 수 있습니다.



ASIC 기반 ACL, CPU 기반 ACL, 빠른 경로, 느린 경로 및 ASIC 펀트와 같은 용어는 이 문서 전체에서 ACL 처리 시 발생하는 사항을 설명하는 데 사용됩니다.다음은 이러한 용어에 대한 설명입니다.

- ASIC 기반 ACL(빠른 경로) - ACL이 ASIC 하드웨어에서 로드되고 처리됩니다.ASIC의 성능 범위는 ACL 깊이, 성능 및 기능을 결정합니다.빠른 경로는 LC 지원 CPU에서 ASIC 기반 처리와 처리 사이의 차이를 설명하기 위해 경로에 사용되었습니다.보다 일반적인 용어인 ASIC 기반 용어가 이 문서에서 사용됩니다.
- CPU 기반 ACL(Slow Path) - ACL은 라인 카드 CPU의 소프트웨어에서 처리됩니다.초기 세대 카드(엔진 0 및 경우에 따라 엔진 1)의 경우 모든 처리가 LC CPU에서 수행됩니다.ASIC 기반 LC는 ASIC에서 펀팅된 패킷에 대해 ACL 처리를 수행합니다.과거 Slow Path(슬로우 경로)는 LC CPU에 대한 펀트가 ASIC보다 느리다는 것을 설명하기 위해 사용되었습니다.이 문서에서는 CPU 기반의 보다 일반적인 용어를 사용합니다.
- ASIC Punts(ASIC 펀트) - ASIC에는 엄격한 설계 봉투가 있습니다.패킷이 설계된 엔벨로프를 초과하면 ASIC에서 펀딩되어 CPU를 지원하는 LC에서 처리되거나 RP(Route Processor)로 전송됩니다.ASIC 기반 ACL은 ASIC의 설계 외부에 있는 패킷을 펀트합니다.예를 들면 log 또는 log-input 키워드와 함께 ACE가 있는 ACL이 있습니다.패킷을 로깅하는 데 필요한 정보는 ASIC 외부에서 처리되어야 합니다. 따라서 패킷은 ASIC에서 자동으로 펀딩되어 LC CPU에 추가되며 일반 CPU 기반 ACL처럼 처리됩니다.

참고: ACL과 일치하도록 match 문으로 PBR(정책 기반 라우팅)을 구성할 때 ACL은 소스 포트와 일치하지 않아야 합니다.GSR(기가비트 스위치 라우터)은 소스 포트와 일치하는 ACL이 있는 PBR에 대한 하드웨어 스위칭을 지원하지 않습니다.프로세스 스위칭과 GSR 성능 저하를 트리거합니다.

제어 및 관리 평면 필터링

라우터 프로세서는 Cisco 12000 Series의 분산 아키텍처에서 제어 및 관리 플레인 서비스를 제공합니다.수신 경로 ACL(rACL)은 RP로 향하는 제어 및 관리 트래픽을 위한 간단한 분산 필터링 기능을

제공합니다.논리적으로 분산된 아키텍처의 장점을 활용하는 추가적인 보안 계층으로 간주할 수 있습니다.

IP 수신 경로 ACL 구성

rACL은 Cisco IOS® Software Release 12.0(21)S2의 유지 보수 스로틀(maintenance throttle)에 대한 특별 포기를 통해 도입되었습니다. Cisco IOS Software Release 12.0(22)S에서 공식적으로 지원됩니다.자세한 내용은 IP 수신 ACL을 참조하십시오.

라우터 프로세서는 Cisco 12000 Series의 분산 아키텍처에서 컨트롤 플레인 서비스를 제공합니다.Receive ACL은 라우팅 업데이트 및 SNMP(Simple Network Management Protocol) 쿼리 등 RP로 향하는 트래픽을 제어하는 필터링 기능을 제공합니다.

rACL은 플레인 트래픽의 제어 및 관리에 새로운 보호를 추가하기 위한 다단계 노력의 1단계로 간주됩니다.소프트웨어 업데이트를 통해 새로운 속도 제한 개선 사항이 추가됩니다.

라인 카드 유형별 IPv4 ACL 지원

12000 Series 라인 카드는 엔진 유형별로 다른 ACL 기능을 제공합니다.이 섹션에서는 서로 다른 라인 카드 엔진의 ACL 기능에 대해 설명합니다.특정 라인 카드 엔진에 대한 ACL 지원 정보는 이 문서의 해당 섹션을 참조하십시오.

모든 ACL에는 몇 가지 일반적인 특성이 있습니다(ASIC 및 CPU 기반).

- 각 방향에 대해 하나의 인터페이스에 하나의 ACL만 적용할 수 있습니다.예를 들어, 인터페이스 POS 0/0에는 입력 ACL과 출력 ACL이 하나만 있을 수 있습니다.
- ACL에 대한 패킷 테스트는 일치하는 항목이 발견된 후 중지됩니다.300개 항목의 ACL이 ACE(Access-list Entry) #45의 패킷과 일치하면 패킷이 처리되고 ACL 처리가 중지됩니다.
- 모든 ACL의 끝에 암시적 **거부** 항목이 있습니다.따라서 ACL에 일치하는 항목이 없으면 패킷이 삭제됩니다.Cisco ACL은 *명시적 허용* ACL 아키텍처로 생성됩니다.즉, 패킷이 처리 및 전달되도록 하려면 패킷과 일치하는 ACE가 있어야 합니다.
- 새로 추가된 ACE는 항상 ACL의 끝에 추가됩니다.ACL에 업데이트가 필요할 때마다 ACL을 제거하고(no access-**list** 명령 사용) 새 ACL을 다시 추가하는 것이 좋습니다.
- 초기가 아닌 IP 프래그먼트는 IP 헤더에 레이어 4 프로토콜 정보를 포함하지 않으므로 초기가 아닌 프래그먼트에 대해서는 표준 일치 기준만 지원됩니다.Cisco ACL이 IP 프래그먼트 필터링을 준수하는 방법에 대한 자세한 내용은 Access Control Lists and IP Fragments(액세스 제어 목록 및 IP 프래그먼트)에서 확인할 수 있습니다.
- 번호가 지정된 ACL은 CLI(Command Line Interface)를 통해 입력되는 즉시 처리 및 적용됩니다. 대규모 ACL을 사용하면 RP 또는 LC CPU에서 CPU가 급증할 수 있습니다.

엔진 0 - ACL 처리

엔진 0은 Cisco 12000에 대해 제공되는 첫 번째 라인 카드입니다. 모든 CPU 기반 처리 및 포워딩입니다.따라서 엔진 0 라인 카드는 LC CPU에서 ACL을 처리합니다.

이러한 라인 카드는 엔진 0을 기반으로 합니다.

라인 카드 유형	인터페이스 유형	연결
DS3 12 개	동축	중소기업

DS3 12 개	동축	중소기업
E3 12개	동축	중소기업
1xCHOC12->DS3		IR
1xCHOC12/STM4 ->OC3/STM1	POS	IR
4xOC3c/STM1c	POS	SR
4xOC3c/STM1c	POS	LR
4xOC3c/STM1c	POS	MM
1xOC12c/STM4c	POS	IR
1xOC12c/STM4c	POS	MM
6xCT3->DS1		중소기업
2xCHOC3/STM1- >DS1/E1		IR
4xOC3c/STM1c	ATM	IR
4xOC3c/STM1c	ATM	MM
1xOC12c/STM4c	ATM	IR
1xOC12c/STM4c	ATM	MM

지원되는 일치 기준

모든 Cisco IOS 소프트웨어 릴리스 12.0S 표준, 확장 ACL 및 터보 ACL은 엔진 0에서 지원됩니다.

지원되는 ACE 수

ACL 크기는 성능 요구 사항 및 사용 가능한 메모리 리소스로만 제한됩니다.

출력 ACL 처리

출력 ACL은 시스템에 있는 다른 라인 카드의 인그레스 기능 경로에서 처리됩니다.출력 ACL을 다른 LC의 인그레스 쪽에 푸시하면 후면판이 삭제될 패킷을 전달하는 것을 방지할 수 있습니다.이는 Cisco 7500의 분산 아키텍처에서 상속된 기능입니다.자세한 설명, 이유 및 운영 지침은 IPv4 출력 ACL - 라인 카드 상호 운용 매트릭스에 나와 있습니다.

라인 카드별 명령

None.

운영 지침 및 라인 카드 상호 작용

- NetFlow가 Engine 0 라인 카드에 구성되어 있고 출력 ACL이 이그레스 엔진 3 또는 4+ 라인 카드에 구성되어 있는 경우, NetFlow가 ACL에서 거부된 패킷과 전달된 패킷을 고려하도록 하기 위해 인그레스 및 이그레스 라인 카드 모두에서 출력 ACL을 처리합니다.

권장 사항

Cisco에서는 대형 ACL에 엔진 0에서 터보 ACL을 사용하는 것이 좋습니다.소형 선형 ACL은 Turbo

ACL에 추가 메모리가 필요하므로 더 작은 ACL에 더 효율적입니다.

엔진 1 - ACL 처리

개요

엔진 1 라인 카드는 엔진 0의 CPU 기반 처리와 엔진 2의 1세대 포워딩/기능 ASIC 간의 브리지입니다. 엔진 1 라인 카드는 기본적으로 소프트웨어에서 ACL을 처리합니다.Cisco IOS Software Release 12.0(10)S 이상에서 Engine 1은 Salsa ASIC 버전 4 또는 5가 장착된 카드에 대한 하드웨어 ACL을 제공합니다(특정 카드가 장착된 Salsa 버전을 확인하려면 아래 라인 카드 명령 참조 참조).

이러한 라인 카드는 엔진 1을 기반으로 합니다.

라인 카드 유형	인터페이스 유형	연결
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100베이스F
8xFE	(RJ45)	100BaseT
8xFE	(MM)	100베이스F
1xGE	SX,	GBIC:
1xGE	SX,	GBIC:
2xOC12c/STM4c	DPT	IR
2xOC12c/STM4c	DPT	LR
2xOC12c/STM4 c	DPT	XLR
2xOC12c/STM4c	DPT	MM
2xOC12c/STM4c	DPT	IR
2xOC12c/STM4c	DPT	LR
2cOC12c/STM4c	DPT	XLR
2xOC12c/STM4c	DPT	MM

지원되는 일치 기준

모든 Cisco IOS Software Release 12.0S 지원 표준, 확장 및 터보 ACL은 LC CPU(저속 경로)에서 지원됩니다. 또한 엔진 1은 Salsa ASIC에서 입력 ACL을 처리할 수 있습니다.Salsa ASIC는 경로 조회와 함께 입력 ACL 처리를 처리하므로 기존 선형 ACL 처리 및 터보 ACL 처리와 비교할 때 성능이 향상됩니다.Salsa ASIC는 출력 ACL 또는 하위 인터페이스 ACL을 처리할 수 없습니다.

지원되는 ACE 수

ACL 크기는 성능 요구 사항 및 사용 가능한 메모리 리소스로만 제한됩니다.

출력 ACL 처리

출력 ACL은 시스템에 있는 다른 라인 카드의 인그레스 기능 경로에서 처리됩니다.자세한 내용은 IPv4 출력 ACL - 라인 카드 상호 작동 매트릭스 섹션을 참조하십시오.

라인 카드별 명령

- **access-list 하드웨어 salsa**
- **컨트롤러 l3 표시 | ASIC 포함**

운영 지침 및 라인 카드 상호 작용

- Salsa ASIC와 PSA ASIC는 동시에 작동할 수 없습니다.access-**list hardware** 명령은 PSA(Engine 2) 또는 Salsa(Engine 1)만 허용하지만 둘 다 허용하지는 않습니다.
- NetFlow가 Engine 1 라인 카드에 구성되어 있고 출력 ACL이 이그레스 엔진 3 또는 4+ 라인 카드에 구성되어 있는 경우, NetFlow가 ACL에서 거부된 패킷과 전달된 패킷을 고려하도록 하기 위해 인그레스 및 이그레스 라인 카드 모두에서 출력 ACL을 처리합니다.

권장 사항

하드웨어 ACL을 지원하지 않는 엔진 1 라인 카드 버전의 경우 대규모 ACL에 Turbo ACL을 사용하는 것이 좋습니다.작은 ACL(20줄 미만)을 선형 ACL로 구현하여 메모리를 절약할 수 있습니다.

엔진 2 - ACL 처리

개요

Engine 2는 포워딩/기능 ASIC가 있는 첫 번째 라인 카드였습니다.Cisco IOS Software Release 12.0(10)S 이상에서는 Engine 2 라인 카드가 고성능 PSA(Packet Switching ASIC)에서 하드웨어 ACL 기능을 제공합니다. 모든 포워딩/기능 ASIC와 마찬가지로 엄격한 성능 봉투는 ASIC 기능에 경계를 배치합니다.엔진 2 ACL의 주요 성능 포락선은 PSA ASIC의 메모리 제한 때문입니다.

엔진 2에서 패킷 전달은 PSA ASIC에 의해 수행됩니다.PSA에는 3가지 주요 외부 메모리가 있습니다.

- PLU(Path-lookup) - 다중 노드를 저장하는 데 사용됩니다.
- TLU(Table Lookup) - FIB leaf 및 loadbalance 구조를 저장하는 데 사용됩니다.또한 PSA ACL 데이터 구조 중 많은 부분을 유지하는 데 사용됨
- SRAM - 로드 공유 구조를 위한 기본 위치입니다.

PSA ACL 기능은 마이크로코드 기반 ACL 검사 구현입니다.기본 ACL 확인을 허용하는 특수 지침 세트가 PSA 칩에 로드됩니다.이 기능에는 구축 전에 신중하게 이해해야 하는 여러 가지 제한 사항이 있습니다.PSA ACL의 주요 단점은 필요한 대용량 하드웨어 포워딩 메모리입니다.

PSA ACL 기능을 사용하려면 접두사 수 등에 관계없이 PLU/TLU 메모리 블록이 미리 할당되어야 합니다.이러한 할당은 주로 TLU 영역에서 이루어지므로 PSA ACL을 구성할 때 이러한 카드에 유지 관리할 수 있는 경로 수에 큰 영향을 미칩니다.

PLU/TLU 메모리의 초기 출력 외에 TLU 메모리에 저장된 각 접두사에는 훨씬 더 많은 메모리가 필요합니다.각 접두사에 필요한 메모리의 양은 적용된 ACL의 방향(인그레스 대 이그레스)과 라인 카드 유형에 따라 달라집니다.일반적으로 이그레스 ACL은 인그레스(ingress)보다 더 많은 메모리가 필요하고, 물리적 포트가 더 많은 라인 카드에는 더 적은 수의 포트가 있는 ACL보다 더 많은 메모리가 필요합니다.

엔진 2 라인 카드가 ACL을 사용하지 않는 경우 ACL에 대한 데이터 구조는 구성된 실제 ACL에 관계없이 작성됩니다.더 작은 비 ACL 구조로 변경하려면 라우터에 **no access-list 하드웨어 psa**를 구성해야 합니다.이 명령은 모든 Engine2 라인 카드에서 모든 방향의 모든 ACL 처리를 비활성화합니다

.Cisco는 이를 매우 신중하게 사용하는 것이 좋습니다.

개요

매치 깊이와 독립적인 ACL 처리 성능을 제공하기 위해 Engine 2 ACL은 하드웨어 포워딩 테이블에 통합됩니다.접두사 확장성에 어떤 영향을 미칠 수 있는지에 대한 설명은 아래를 참조하십시오.

이러한 라인 카드는 엔진 3을 기반으로 합니다.

라인 카드 유형	인터페이스 유형	연결
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR
1xOC192c/STM64c	Enabler	SR
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xOC12c/STM4c	ATM	IR
4xOC12c/STM4c	ATM	MM
8xOC3cSTM1c	ATM/TS	IR
8xOC3c/STM1c	ATM/TS	MM
3xGE	SX	GBIC:
3xGE	CWDM	GBIC:
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR
1xOC48c/STM16c	DPT	SR
1xOC48c/STM16c	DPT	LR

지원되는 일치 기준

레이어 4 소스 포트를 제외한 모든 Cisco IOS Software Release 12.0S에서 표준 및 확장 ACL 일치 기준을 지원합니다.비연속 마스크, IP 우선 순위 필드 및 레이어 4 소스 포트는 PSA ASIC에서 펀칭되고 LC CPU에서 처리됩니다.

지원되는 ACE 수

PSA에서 최대 5개의 448라인 입력 ACL입니다.포트당 하나의 ACL을 구성할 수 있습니다.추가 ACL은 라인 카드 CPU에서 관리합니다.출력 ACL에 대한 제한 사항은 아래의 "제한" 섹션을 참조하십시오.

출력 ACL 처리

이 라인 카드에 구성된 출력 ACL은 시스템의 다른 라인 카드의 인그레스 기능 경로에서 수행됩니다.자세한 내용은 IPv4 출력 ACL - 라인 카드 상호 운영 매트릭스를 참조하십시오.

라인 카드별 명령

- **access-list hardware psa limit 128**
- **액세스 목록 하드웨어 psa 없음**
- **psa 우회**
- **show access-list psa 세부 정보**
- **show access-list psa 요약**
- **컨트롤러 psa 기능 표시**

운영 지침 및 라인 카드 상호 작용

- 빠른 경로 ACL 처리를 위해서는 다음 조건을 충족해야 합니다.적용된 ACL은 128 또는 448-ACE 제한 내에 있습니다.**access-list hardware psa limit 128** 명령이 구성된 경우 길이는 128ACE보다 작아야 합니다.448 라인 ACL 마이크로코드 번들이 필요한 경우 길이는 448 ACE보다 작아야 합니다.입력 및 출력 ACL은 카드당 함께 구성되지 않습니다.*라우터*에 최대 5개의 출력 ACL을 구성할 수 있습니다.
- 8포트 및 16포트 OC-3/STM-1 POS 라인 카드에서는 128회선 ACL만 지원됩니다.4-port OC-12/STM-4 POS, 1-port OC-48/STM-16 POS 및 3-port Gigabit Ethernet 라인 카드에서 448 라인 ACL이 지원됩니다.
- 입력 ACL은 두 ACL이 동일한 카드에 동시에 구성된 경우 출력 ACL보다 빠른 경로에서 우선 순위를 갖습니다(출력 ACL은 느린 경로에서 처리됨).
- 출력 ACL이 Engine 2 카드에 구성되어 있고 인그레스 라인 카드가 Engine 0/1/2/4이면 출력 ACL이 인그레스 카드에서 처리됩니다.다른 엔진 유형의 경우 출력 ACL은 엔진 2 이그레스 저속 경로에서 처리됩니다.
- 출력 ACL은 IP-to-MPLS 트래픽에 대해 지원되지 않습니다(첫 번째 MPLS 레이블은 IP 패킷에 "Pushed").
- ACL 처리 정보는 하드웨어 FIB에 통합되며 접두사 확장성에 영향을 줄 수 있습니다.접두사 메모리 소모는 메모리 할당 실패에 의해 보고되며, 함께 제공되는 로그 메시지에 "exmem=1" 서명이 있습니다.

권장 사항

- ACL 처리 정보는 CEF 포워딩 테이블에 통합되어 접두사 확장성을 줄입니다.ACL을 사용하지 않는 애플리케이션은 CEF 테이블에서 ACL 지원을 비활성화하여 no access-**list hardware psa** 명령을 실행하여 사용 가능한 접두사 메모리를 늘릴 수 있습니다.
- **no access-list hardware psa** 명령의 컨피그레이션에서는 ACL에 대한 PSA 지원을 비활성화하

는 것 외에도 Engine 2 카드에 의한 모든 ACL 프로세싱을 비활성화합니다.ACL의 소프트웨어 실행을 강제하지 않습니다.이그레스 라인 카드에 출력 ACL이 구성된 경우에도 이 조건이 적용됩니다.

- access-list **hardware psa** 명령을 실행한 후 **access-list 컴파일된** 명령의 컨피그레이션은 PSA 용량을 초과하는 ACE를 터보 ACL로 변환합니다.이는 448개 이상의 ACE에 대한 최적의 ACL 성능을 제공합니다.기본 ACL 마이크로코드는 128입니다(Cisco IOS Software 릴리스 12.0(14)S/ST와 동일). 더 작은 ACL을 사용 중이고 448줄 기능이 필요하지 않은 경우 **access-list hardware psa limit 128** TLU(command conserve forwarding) 메모리를 구성하여 접두사 확장성을 향상시킵니다.Turbo ACL 프로세싱은 access-list **hardware psa limit 128** 명령과 함께 129**개** 이상의 ACL에 대해 access-list compiled 명령을 사용하여 활성화해야 합니다.이 조합은 PSA ASIC의 첫 128개 행과 나머지 행을 Turbo ACL로 처리하여 포워딩 메모리를 절약하면서 성능을 최적화합니다.
- 4포트 OC12 ATM 라인 카드는 입력 ACL을 지원하지 않지만, 마이크로코드에서 출력 ACL 탐지를 제공하므로 느린 경로에서 출력 ACL을 처리할 수 있습니다.
- 8xOC3 ATM 라인 카드는 Cisco IOS Software Release 12.0(23)S 이상에서 per-vc 128 line ACL을 지원합니다.빠른 경로에 최대 16개의 고유한 입력 ACL을 구성할 수 있습니다.448 입력 ACL은 저속 경로에서만 VC별로 지원됩니다.출력 ACL은 지원되지 않습니다.

ISE(IP Services Engine) 엔진 3 - ACL 처리

개요

Engine 3은 첫 번째 듀얼 스테이지 포워딩 라인 카드입니다.엔진 3에는 인그레스 및 이그레스 경로에 포워딩/기능 ASIC이 있습니다.이를 통해 ACL은 인그레스 및 이그레스 경로 모두에서 ASIC에 배치할 수 있습니다.또한 Engine 3 ASIC 구조는 하이브리드 파이프라인/병렬 배열입니다.ASIC 구조에서는 ACL 처리를 병렬 고속 TCAM(Ternary Content Addressable Memory)으로 구현하며, 인그레스 당 최대 20K ACE와 이그레스 당 20K ACE의 라인 속도 처리를 제공합니다.

이러한 라인 카드는 엔진 3을 기반으로 합니다.

라인 카드 유형	인터페이스 유형	연결
4xOC12c/STM4c	POS	IR
4xOC12c/STM4c	POS	MM
4xCHOC12/STM4->OC3/STM1->DS3/E3	POS	IR
16xOC3c/STM1c	POS	IR
16xOC3c/STM1c	POS	MM
8xOC3/STM1c	POS	IR
8xOC3c/STM1c	POS	MM
4xOC3c/STM1c	POS	IR
4xOC3c/STM1c	POS	MM
4xOC3c/STM1c	POS	LR
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	LR

1xCHOC48/STM1 6->STM4- >OC3/STM1- >DS3/E3	POS	SR
4xOC12c/STM4c	ATM/IP	IR
4xOC12c/STM4c	ATM/IP	MM
4xGE	GE	
4xOC12c/STM4c	DPT	IR
4xOC12c/STM4c	DPT	XLR

지원되는 일치 기준

모든 Cisco IOS Software Release 12.0S Standard 및 Extended 일치 기준은 라인 카드 CPU에서 처리되는 로그 ACE를 제외하고 빠른 경로에서 지원됩니다.

지원되는 ACE 수

- 포트당, VLAN별, 프레임 릴레이 하위 인터페이스별, ATM 하위 인터페이스당 인그레스 및 이그레스 방향 모두에서 라인 레이트 처리방향과 카드당 최대 20,000개의 확장 ACE가 지원됩니다.
- TCP/UDP 소스/대상 포트 "범위", "lt" 및 "gt"에 대한 일치 기준은 모두 하드웨어에서 "L4 운영자" 리소스를 사용하여 처리됩니다.
- 전체 라인 카드의 고유 L4 피연산자 수는 32개로 제한됩니다.소스 포트 연산자는 최대 6개로 제한됩니다.

출력 ACL 처리

Transmit-path Packet Processing ASIC에서 회선 속도 출력 ACL 처리를 위한 네이티브 빠른 경로 지원.자세한 내용은 IPv4 출력 ACL - 라인 카드 상호 운영 매트릭스를 참조하십시오.

라인 카드별 명령

- **hw-module <*slot #*> tcam compile no-merge*!—12.0(21)S3***
- **show-access-list 하드웨어 인터페이스 <*interface name*>**
- **show cef int pos[*x/y*] | inc if_number**

운영 지침 및 라인 카드 상호 작용

- 로깅 ACE와 일치하는 패킷은 느린 경로에서 처리됩니다.
- 거부 ACE와 일치하는 패킷(시스템 중단에 대비하여 제한됨)은 느린 경로에서 처리됩니다.
- ACL에 주소 범위가 포함된 경우 하드웨어는 최대 3개의 ACE가 필요한 "Range ACEs"라는 특수한 ACE를 사용합니다.
- ACL 병합은 개별 ACL 간에 공통 ACE를 공유하여 TCAM 리소스를 보존할 수 있습니다.ACL의 병합 여부를 확인하려면 **show-access-list hardware interface** 명령을 사용합니다.
- 병합된 ACL에는 ACL 카운터가 지원되지 않습니다.Cisco IOS Software Release 12.0(21)S3 이상에서 ACL 병합은 hw-**module <slot #> tcam compile no-merge** 명령과 함께 비활성화할 수 있습니다.ACL의 병합 여부를 확인하려면 **show-access-list hardware interface** 명령을 사용합니다.

- NetFlow가 엔진 0/1 라인 카드에 구성되어 있고 출력 ACL이 이그레스 엔진 3 또는 4+ 라인 카드에 구성되어 있는 경우 NetFlow가 ACL에서 거부된 패킷 및 전달된 패킷을 고려하도록 하기 위해 인그레스 라인 카드와 이그레스 라인 카드 모두에서 출력 ACL을 처리합니다.

ACL 카운터 지원

	Per-ACE	Per-ACE (hardware counters)	Aggregate
21S3/ST3		X	
22S		X	X
23S	X	X	X

정의:

- Per-ACE—일반 Cisco IOS 소프트웨어 지원, RP/LC의 **show access-list <*number*>** 명령은 각 ACE와 연결된 ACL 및 카운터를 표시합니다.ACL을 구성하기 전에 **병합**이 비활성화된 경우에만 사용할 수 있습니다.이 작업은 다음 컨피그레이션 명령을 사용하여 수행할 수 있습니다.
  ```
  Router(config)#hw-module slot <number> tcam compile acl no-merge
  ```
  이 옵션을 활성화하면 일부 TCAM 병합 최적화가 해제되고 확장성에 영향을 줍니다.정확한 효과는 개별 ACL에 따라 달라집니다.또한 정책 기반 라우팅이 해당 인터페이스에 적용되는 경우에는 카운터가 정확하지 않습니다.이 경우 집계 카운터를 사용해야 합니다.
- TCAM(Per-ACE) - 각 TCAM 항목과 연결된 하드웨어 카운터입니다.구성이 필요하지 않으며 성능/확장성에 영향을 미치지 않습니다.이 CLI를 사용하는 라인 카드에서만 사용할 수 있습니다.이 카운터는 소프트웨어에서 지울 수 없습니다.
  ```
  LC-Slot4#show contr tofab alpha acl <if-number> vmr2ace
  ```
  이 명령에 대한 새로운 일반 CLI는 Cisco IOS Software 릴리스 22S에서 사용할 수 있습니다.
  ```
  LC-Slot4#show access-list hardware interface p0:1 in
  ```
  ACE당 카운터와 마찬가지로 TCAM 카운터는 ACL이 있는 해당 인터페이스에서 PBR을 사용하지 않는 경우에만 유효합니다.
- Aggregate(집계) - 각 ACL은 요약 허용/거부 카운터를 표시합니다.모든 개별 ACE 카운터의 합계입니다.구성이 필요하지 않으며 성능이나 확장성에 영향을 미치지 않습니다.

권장 사항

현재 없음

엔진 4(POS) - ACL 처리

개요

엔진 4는 Cisco IOS Software 릴리스 12.0(18)S 이상에서 이 ACL 지원을 제공합니다.

- 엔진 4 라인 카드가 인그레스 카드인 경우 출력 ACL은 E0/1/2 라인 카드에서 지원됩니다.이 컨피그레이션에서는 출력 ACL이 이그레스 라인 카드 CPU에 의해 처리됩니다.

이러한 라인 카드는 엔진 4를 기반으로 합니다.

라인 카드 유형	인터페이스 유형	엔진 유형	연결
4xOC48c/STM16c	POS	E4	
4xOC48c/STM16c	POS	E4	LR
1xOC192c/STM64c	POS	E4	IR
1xOC192c/STM64c	POS	E4	SR
1xOC192c/STM64c	POS	E4	VSR-1
10xGE	SFP	E4	

엔진 4+(POS 및 DPT) - ACL 처리

개요

Engine 4+는 Cisco 12000 Series 10기가비트 포트폴리오에 ACL 기능을 도입했습니다.

각 인그레스 및 이그레스 경로에서 최대 1,024개의 ACE가 지원됩니다.입력 및 출력 ACL은 모두 최대 96개의 ACE에 대해 라인 레이트로 처리됩니다.더 긴 일치를 위한 성능은 일치 깊이에 따라 달라집니다.

이러한 POS 라인 카드는 Engine 4+를 기반으로 합니다.

라인 카드 유형	인터페이스 유형	연결
4xOC48c/STM16c	POS	SR
4xOC48c/STM16c	POS	LR
1xOC192c/STM64c	POS	IR
1xOC192c/STM64c	POS	SR
1xOC192c/STM64c	POS	VSR-1
1xOC192/STM64c	POS	LR
4xOC48c/STM16c	DPT	SFP:
1xOC192c/STM64c	DPT	IR
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1

1xOC192c/STM64c	DPT	LR

지원되는 일치 기준

모든 Cisco IOS Software Release 12.0S 지원 표준 및 확장 ACL 기준은 로그 또는 프래그먼트 ACE를 제외하고 빠른 경로에서 지원됩니다.

지원되는 ACE 수

빠른 경로에서 방향당 최대 1,024개의 ACE가 지원됩니다.

참고: ACE 1021을 구성할 수 있습니다.ACE의 암시적 **permit ip any any**, deny ip any any, **send to CPU** 명령에 대해 **세 항목이 예약됩니다**.

지원되는 ACE 수에 대한 상한선은 없습니다.1021 제한을 초과하는 모든 ACE는 라인 카드 느린 경로에서 수행됩니다.

출력 ACL 처리

출력 ACL은 전송 측 빠른 경로에서 처리됩니다.자세한 내용은 IPv4 출력 ACL - 라인 카드 상호 운영 매트릭스를 참조하십시오.

라인 카드별 명령

- **show tcam appl [*acl-in*] | *acl-out*] tcam <*label-no*>**
- **show tcam appl [*acl-in*] | *acl-out*] memory <*port*> <*항목 수*>**

운영 지침 및 라인 카드 상호 작용

- 하위 인터페이스 ACL은 지원되지 않습니다.
- 성능은 일치 깊이에 따라 달라집니다.
- 범위 엔트리는 두 개의 ACL 규칙(두 엔트리가 경계를 넘는 경우 3개)을 사용합니다.
- 물리적 인터페이스당 하나의 ACL이 지원됩니다.
- 빠른 경로에서 최대 1,024개의 ACE(방향당)가 지원됩니다.
- 1024 빠른 경로 ACE는 포트 간에 공유할 수 있습니다.
- fragment 키워드를 사용하는 ACE는 느린 경로에서 필터링됩니다.
- 거부된 패킷은 느린 경로에서 처리되는 ACE에 대해 계산되지 않습니다.
- NetFlow가 Engine 0 라인 카드에 구성되어 있고 출력 ACL이 이그레스 엔진 3 또는 4+ 라인 카드에 구성되어 있는 경우, 출력 ACL은 인그레스 및 이그레스 라인 카드 모두에서 처리되어 NetFlow가 ACL에서 거부한 패킷과 전달된 패킷을 고려하도록 합니다.

권장 사항

현재 없음

엔진 4+(이더넷) - ACL 처리

개요

Engine 4+ 이더넷 라인 카드는 Cisco 12000 10기가비트 이더넷 포트폴리오에 하드웨어별 VLAN 입력 ACL 기능을 도입합니다.다음은 몇 가지 특성입니다.

- 입출력 ACL은 성능에 영향을 주지 않고 단일 포트에서 동시에 적용할 수 있습니다.
- ACL은 VLAN당 또는 포트별로 적용할 수 있습니다.
- 최대 15K ACE의 입력 ACL 성능이 일치 깊이로 저하되지 않습니다.
- 출력 ACL은 최대 96개의 ACE에 대해 라인 레이트로 처리됩니다.더 긴 일치를 위한 성능은 일치 깊이에 따라 달라집니다.

이러한 이더넷 라인 카드는 Engine 4+를 기반으로 합니다.

라인 카드 유형	인터페이스 유형	엔진 유형
10xGE Rev B("X-B")	SFP:	E4+
모듈형	SFP:	E4+
10GE 1개	10G	E4+
10GE 1개	10G	E4+

지원되는 일치 기준

모든 Cisco IOS Software Release 12.0S 지원 표준 및 확장 ACL 기준은 로그 또는 프래그먼트 ACE를 제외하고 빠른 경로에서 지원됩니다.

지원되는 ACE 수

- 포트당 또는 VLAN별로 구성할 수 있는 최대 15,000개의 입력 ACL입니다.
- 포트별로 적용할 수 있는 카드당 1024 출력 ACE**참고:** ACE 1021을 구성할 수 있습니다.ACE의 암시적 **permit ip any any**, deny ip any any, **send to CPU** 명령**에** 대해 **세** 항목**이 예약됩니다**.

출력 ACL 처리

출력 ACL은 전송 측 빠른 경로에서 기본적으로 처리됩니다.자세한 내용은 IPv4 출력 ACL - 라인 카드 상호 작동 매트릭스를 참조하십시오.

라인 카드별 명령

- **hw-module slot <*number*> ip acl merge**

운영 지침 및 라인 카드 상호 작용

- fragment 키워드를 포함하는 ACE는 느린 경로에서 처리됩니다.
- ACL 카운터는 다른 기능과 결합된 ACL에 대해 지원되지 않습니다.
- 병합된 ACL에는 ACL 카운터가 지원되지 않습니다.병합된 ACL은 hw-**module slot <slot number> ip acl merge** 명령**으로** 구성할 수 있습니다.
- 라인 카드당 최대 168개의 L4 운영이 지원됩니다.이 값을 초과하면 ACL이 느린 경로에서 실행됩니다.

- 엔진 1 라인 카드가 NetFlow를 샘플링했으며 이그레스 엔진 3 또는 4+ 라인 카드에서 출력 ACL이 활성화된 경우 NetFlow가 ACL에서 거부된 패킷과 전달된 패킷을 고려하도록 하기 위해 인그레스 및 이그레스 라인 카드 모두에서 출력 ACL을 처리합니다.

권장 사항

현재 없음

ACL 로깅

Cisco IOS Software Release 12.0(21)S 이전에는 MBUS(Maintenance Bus)를 통해서만 RP에 ACL 로깅 정보가 전송되었습니다. 높은 수준의 ACL 로깅 작업 동안 MBUS의 용량을 초과할 수 있었습니다.Cisco IOS Software 릴리스 12.0(21)S는 이 시나리오를 방지하는 몇 가지 최적화를 도입합니다.

MBUS 오버로드 상황은 Cisco IOS Software에서 다음과 같은 오류 메시지와 함께 보고됩니다.

```
LCLOG-3-INVSTATE

MBUS_SYS-3-SEQUENCE
```

Cisco IOS Software 릴리스 12.0(21)S 이상에서는 높은 심각도(심각도 0-4) 로깅 메시지가 MBUS를 통해 RP에 전달되고, 낮은 심각도(심각도 5-7) 로그 메시지는 고용량 스위칭 패브릭을 통해 RP에 전달됩니다.ACL 로그 메시지는 심각도가 높으므로 이제 스위칭 패브릭을 통해 RP에 전달됩니다.

이 추가된 로깅 기능은 다음 명령을 사용하여 구성할 수 있습니다.

- **logging method mbus [*severity*]** - 심각도별로 MBUS를 사용하여 RP로 전송할 메시지를 결정합니다.심각도가 높은 메시지는 스위치 패브릭을 통해 전송됩니다.
- **show logging method** - 모든 메시지 심각도 수준에 대한 현재 로깅 방법을 표시합니다.
- **logging sequence-nums**—이 명령을 사용하면 RP에서 메시지를 올바르게 다시 정렬할 수 있도록 전송 라인 카드가 번호 로그 메시지의 순서를 지정할 수 있습니다.이 명령을 사용하지 않으면 로그 메시지가 비순차적 순서로 RP에 전달될 수 있습니다.

IPv4 출력 ACL - 라인 카드 상호 작동 매트릭스

Engine 3 및 Engine 4+ 릴리스로 이그레스 ACL 프로세싱이 도입되기 전에 출력 ACL은 인그레스 라인 카드에서 처리되었습니다.출력 ACL은 고성능 엔진 3 및 엔진 4+ 출력 ACL 처리 기능을 활용하도록 업데이트되었습니다.

이 차트에서는 서로 다른 라인 카드 조합에 대해 출력 ACL이 처리되는 위치에 대한 요약을 제공합니다.

	이그레스 라인 카드					
인그레스 라인 카드(멤버 인터페이스에 적용된	**E0**	**E1**	**E2**	**E3**	**E4**	**E4+**

출력 ACL)						
E0	인그레스	인그레스	인그레스	이그레스	해당 없음	이그레스
E1	인그레스	인그레스	인그레스	이그레스	해당 없음	이그레스
E2	인그레스	인그레스	인그레스	이그레스	해당 없음	이그레스
E3	이그레스	이그레스	이그레스	이그레스	해당 없음	이그레스
E4	이그레스	이그레스	이그레스	이그레스	해당 없음	이그레스
E4+	이그레스	이그레스	이그레스	이그레스	해당 없음	이그레스

IPv6 ACL 지원

IPv6 확장 ACL은 Cisco IOS Software 릴리스 12.0(23)S에서 E0, E1, E2, E3 및 E4+의 저속 경로(인그레스 및 이그레스)에서 지원됩니다.

엔진 3에서 IPv6 ACL 기능은 Cisco IOS Software 릴리스 12.0(25)S의 하드웨어에서 지원됩니다.ACL은 특정 인터페이스에 적용되며, 각 액세스 목록의 끝에 암시적 deny 문이 있습니다.IPv6 ACL은 전역 컨피그레이션 모드에서 deny 및 permit 키워드와 함께 **ipv6 access-list** 명령을 사용하여 구성됩니다.Engine 3 기반 카드는 트래픽 기반 IPv6 옵션 헤더, 플로우 레이블 및 선택적으로 상위 레이어 프로토콜 유형 정보의 필터링을 지원합니다.

Cisco 12000 ACL 명령 참조

엔진 1 명령

- access-list 하드웨어 salsa
- 컨트롤러 l3 표시 | ASIC 포함

엔진 2 명령

- access-list hardware psa limit 128
- 액세스 목록 하드웨어 psa 없음
- psa 우회
- show access-list psa 세부 정보
- show access-list psa 요약
- 컨트롤러 psa 기능 표시

Engine 3 명령

- hw-module <*slot #*> tcam compile no-merge*!— Cisco IOS Software 릴리스 12.0(21)S3 기준*
- show-access-list 하드웨어 인터페이스 <*interface name*>
- show contr [*tofab|frfab*] alpha acl <*int*> vmr2ace

Engine 4+ 명령

- show access-list gen7 레이블

- show tcam appl [*acl-in*] | *acl-out*] tcam <*label-no*>
- show tcam appl [*acl-in*] | *acl-out*] 메모리 <*port*><*항목 수*>

Engine 4+ Ethernet 명령

- hw-module slot <*number*> ip acl merge

용어집

이 섹션에서는 관련 용어의 표준 정의를 제공합니다.

- **처리 평면** - 네트워크 디바이스를 세 개의 처리 플레인으로 논리적으로 나눌 수 있습니다.Data Plane(데이터 플레인) - 네트워크 디바이스를 통해 흐르는 패킷에서 처리합니다.Control Plane(제어 평면) - 네트워크 디바이스를 하나로 묶는 데 사용되는 패킷에서 처리합니다.여기에는 Point-to-Point Protocol - PPP 및 High-Level Data Link Control - HDLC), 라우팅 프로토콜(Border Gateway Protocol - BGP, Routing Information Protocol 버전 2 - RIPv2, Open Shortest Path First - OSPF 등), 타이밍 프로토콜(예: Network Time Protocol - NTP)이 포함됩니다 .Management Plane(관리 평면) - 네트워크 디바이스를 관리하는 데 사용되는 패킷에서 처리합니다.여기에는 텔넷, SSH(Secure Shell), FTP(File Transfer Protocol), TFTP(Trivial File Transfer Protocol), SNMP 및 기타 관리 프로토콜이 포함됩니다.
- **표준 ACL**—표준 ACL은 레이어 3에서만 필터링됩니다.
- **확장 ACL**—확장 IP 액세스 목록은 소스 및 대상 주소를 사용하여 매칭 작업을 수행하고 프로토콜 유형 정보(옵션)를 사용하여 더욱 세분화된 제어를 수행합니다.
- **Linear Processed ACLs(선형 처리 ACL)** - 소프트웨어에서 온라인으로 처리됩니다.성능은 일치 수준(일치 여부를 결정하기 전에 확인해야 하는 항목 수)에 따라 달라집니다.
- **Turbo ACL(Compiled)** - Turbo ACL은 소프트웨어 처리 속도를 높이는 최적화된 일련의 조회 테이블로 ACL을 컴파일하여 소프트웨어 ACL 처리를 최적화합니다.Turbo ACL의 성능은 일치 깊이에 따라 다릅니다.
- **Input ACLs(입력 ACL)** - ACL이 적용되는 포트에 유입되는 트래픽에 적용되는 ACL입니다.
- **Output ACLs**(출력 ACLs) - 적용된 포트를 종료하는 트래픽에 적용되는 ACL입니다.일부 예외에서는 출력 ACL이 입력 라인 카드로 처리됩니다.
- **Receive Path ACLs(수신 경로 ACL)** - 수신 경로 ACL은 라우팅 업데이트 및 SNMP 쿼리 등 라우터 자체로 향하는 제어 트래픽에 대한 필터링을 제공합니다.
- **Dual Stage Forwarding Line Card**—인그레스 및 이그레스 경로에 포워딩/기능 ASIC이 있는 라인 카드입니다.이렇게 하면 라인 카드가 LC CPU에 패킷을 펀팅하지 않고도 인그레스 패킷 흐름과 이그레스 패킷 흐름에서 기능을 수행할 수 있습니다.또한 Cisco 12000에서 듀얼 스테이지 포워딩 알고리즘의 새로운 전파를 사용할 수 있습니다. Engine 3 라인 카드는 듀얼 스테이지 포워딩 라인 카드의 예입니다.
- **Single Stage Forwarding Line Card**—인그레스 경로에 포워딩/기능 ASIC이 있는 라인 카드입니다.이러한 라인 카드는 인그레스 경로에서 흐르는 패킷에 대해서만 ASIC 기반 처리를 수행합니다.이그레스(egress) 트래픽은 처리되지 않음(방금 전달), 다른 LC의 인그레스 ASIC에 의해 처리되거나 LC CPU에 의해 관리됩니다.Engine 2, Engine 4 및 Engine 4+는 단일 단계 포워딩 라인 카드의 예입니다.

관련 정보

- Cisco 12000 Series 인터넷 라우터
- 기술 지원 및 문서 – Cisco Systems