Catalyst 6500/Sup2T 및 Catalyst 6880 컨피그레이션의 기본 컨트롤 플레인 정책 예

목차

소개

이 문서에서는 디바이스에 자동으로 구성된 기본 Catalyst 6500 Sup2T/Catalyst 6880 CoPP(Control Plane Policing) 컨피그레이션의 일부인 기본 클래스 맵과 일치하는 트래픽 유형을 자세히 설명합니다.이는 CPU가 오버로드되지 않도록 보호하기 위해 구성됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 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.

구성

CoPP는 Catalyst 6500/SUP2T 및 Catalyst 6880 스위치에서 기본적으로 활성화되며 사전 구성된 템플릿을 기반으로 합니다.일부 클래스 맵 컨피그레이션에는 MAC/IP ACL(Access Control List)에

서 트래픽을 캡처한다는 사실이 아니라 스위치에서 트래픽을 수신하고 포워딩 결정을 내릴 때 포워딩 엔진에서 신호를 보내는 내부 예외 사항으로 인해 해당 match 문이 없습니다.

특정 클래스 맵을 현재 CoPP 정책에서 추가/수정/제거해야 하는 경우 정책 맵 모드의 컨피그레이션 모드에서 수행해야 합니다.정확한 구문은 Catalyst 6500 Release 15.0SY Software Configuration Guide - Control Plane Policing (CoPP)을 참조하십시오.

CoPP 기본 예외 클래스에는 다음 설명이 있습니다.

사례	클래스 맵 이름	설명
MTU(Maximum Transmission Unit) 실패	class cop-mtu-fail	패킷 크기가 나가는 인터페이스 MTU 크기를 초과합니다. Don't Fragment 비트가 설정되지 않은 경우 단편화가 필요합니다. Don't Fragment 비트가 설정된 경우 ICMP(Internet Control Message Protocol) Destination Unreachable 메시지는 "fragmentation needed and DF set"이 생성되어 소스로 다시 전송되어야 함을 나타냅니다. 참조:RFC-791, RFC-1191
TTL(Time To Live) 실패	class cop-ttl-fail	패킷 TTL = 1(IPv4의 경우), Hop Limit = 0 또는 1(IPv6의 경우) TTL이 0으로 감소하면 이전 홉이 패킷을 폐기해야 하므로 TTL = 0(IPv4)을 하드웨어에서 즉시 삭제할 수 있습니다. Hop Limit = 0(IPv6의 경우)은 RFC-2460, 섹션 8.2에 명시되어 있으므로 TTL = 0과 다릅니다. "IPv4와 달리 IPv6 노드는 최대 패킷 수명을 적용하는 데 필요하지 않습니다.따라서 IPv4 Time to Live 필드의 이름이 IPv6"에서 Hop Limit으로 바뀌었습니다. 즉, Hop Limit = 0인 수신 IPv6 패킷이 여전히 유효하며 ICMP 메시지를 다시 보내야 합니다. 참조:RFC-791, RFC-2460
옵션	class cop-options	옵션이 있는 패킷(IPv4), Hop-by-Hop 확장 헤더(IPv6) 예를 들어 라우터 알림 RFC-2113, 엄격한 소스 경로 등이 있습니다. 패킷이 IPv6 헤더의 Destination Address 필드에 식별된 노드(또는 멀티캐스트의 경우 각 노드 집합)에 도달할 때까지 패킷의 전달 경로를 따라 어떤 노드에서도 확장 헤더를 검사하거나 처리하지 않습니다.유일한 예외는 Hop-by-Hop Options 헤더입니다. Hop-by-Hop Options 헤더는 패킷의 전달 경로를 따라 모든 노드에서 검사하고 처리해야 하는 정보를 전달합니다. 여기에는 소스 및 대상 노드가 포함됩니다. 옵션 필드의 하드웨어 처리는 지원되지 않으므로 소프트웨어 처리/스위칭이 필요합니다.

		참조:RFC-791 / RFC-2460 RPF 확인에 실패한 패킷이 필터링됩니다.그러나 하드웨어의 리소스가 제한적이기 때문에 하드웨어에서 RPF 검사를 수행할 수 없는 경우가 있습니다(즉, 하나의 IP에 연결된 RPF 인터페이스가 16개 이상). 이러한 경우 패킷이 소프트웨어로 전송되어 전체 RPF 확인이 수행됩니다.
RPF(Reverse Path Forwarding) 실패(유니캐스트)	class cop-ucast-rpf-fail	PIM(Protocol Independent Multicast) 어설션 프로세스를 시작하기 위해 실패한 첫 번째 RPF 데이터 패킷(멀티캐스트 그룹으로 주소 지정)이 소프트웨어로 전송됩니다.프로세스가 완료되면 지정된 라우터/전달자가 선택됩니다.다음 패킷(동일한 흐름)이 지정된 라우터에서 오지 않으면 RPF 오류가 발생하고 하드웨어가 즉시 이를 삭제할 수 있습니다(DoS(서비스 거부) 공격을 방지하기 위해).
RPF 실패 (멀티캐스트)	class copp-mcast-rpf-fail	PIM-assert 프로세스를 시작하기 위해 실패한 첫 번째 RPF 데이터 패킷(멀티캐스트 그룹으로 주소)이 소프트웨어로 전송됩니다.프로세스가 완료되면 지정된 라우터/전달자가 선택됩니다.다음 패킷(동일한 흐름)이 지정된 라우터에서 오지 않으면 RPF 오류가 발생하고 하드웨어가 즉시 이를 삭제할 수 있습니다(DoS 공격을 방지하기 위해). 그러나 라우팅 테이블이 업데이트되면 PIM-assert를 통해 새로운 지정 라우터를 선택해야 할 수 있습니다. 즉, RPF 실패 패킷이 소프트웨어에 도달해야 합니다(PIM-assert가 다시 시작되려면). 이를 위해 하드웨어에서 RPF 실패 패킷에 대한 소프트웨어 메커니즘(플로우당)으로의 정기적인 누수가 가능합니다.그러나 많은 양의 플로우가 있는 경우 소프트웨어가 처리하기에는 주기적인 누수가 너무 많을 수 있습니다.멀티캐스트 RPF 실패 패킷에 하드웨어 CoPP가 여전히 필요합니다.
하드웨어 패킷 재작성은 지원되지 않습니다.	class cop-unsupp-rewrite	참조:RFC-3704, RFC-2362 하드웨어가 다양한 경우 패킷을 다시 작성할 수 있지만, 일부 경우에는 현재 하드웨어 설계에서 수행할 수 없습니다.이를 위해 하드웨어는 패킷을 소프트웨어로 전송합니다.
ICMP 경로 없음 ICMP acl-drop ICMP 리디렉션	class-cop-icmp-redirect-unreachable	ICMP 메시지 생성을 위해 소프트웨어로 전송된 패킷.ICMP 리디렉션, ICMP 대상에 연결할 수 없음(예:호스트 연결 불가 또는 관리상 금지). 참조:RFC-792 / RFC-2463
Cisco CEF(Express Forwarding) 수신(대상 IP는 라우	클래스 복사 수신	패킷의 목적지 IP가 라우터의 IP 주소 중 하나인 경우(CEF가 수신 인접성에 도달함) 소프트웨어는 콘텐츠를 처리합니다.

터의 IP임)		
CEF glean(대상 IP가 라우터 네트워크 중 하나에 속함)	클래스 코p-glean	패킷의 목적지 IP가 라우터의 네트워크 중 하나에 속하지만 확인되지 않은 경우(즉, FIB(Forwarding Information Base) 테이블에서 적중하지 않은 경우, CEF 편애적 인접성에 도달하고 해결 절차가 시작되는 소프트웨어로 전송됩니다. IPv4의 경우 주소가 해결될 때까지 동일한 흐름이 CEF glean에 계속 적용됩니다 .IPv6의 경우, 확인 중에 대상 IP와 일치하는 임시 FIB 항목(대신 인접성을 삭제하는 지점)이 설치됩니다.지정된 기간 동안 확인할 수 없는 경우 FIB 항목이 제거됩니다(즉, 동일한 흐름이 다시 CEF glean에 도달하기 시작).
멀티캐스트 IP 224.0.0.0/4으로 전송되는 패킷	class copp-mcast-ip-control	제어 패킷은 소프트웨어에서 처리해야 합니다.
멀티캐스트 IP FF로 향하는 패킷::/8	class copp-mcast-ipv6-control	제어 패킷은 소프트웨어에서 처리해야 합니다.
소프트웨어에 복사해야 하는 멀티캐스트 패킷	class copp-멀티캐스트-copy	경우에 따라 상태 업데이트를 위해 멀티캐스트 패킷을 소프트웨어에 복사해야 합니다(패킷은 여전히 동일한 VLAN에 하드웨어 브리징됨). 예를 들어, Dense Mode 항목, dual-rpf SPT 전환의 경우 (*,G/m) hit.
FIB 테이블에서 누락되는 멀티캐스트 패킷	클래스 코프-멀티캐스트-펀트	대상 IP(멀티캐스트 IP)가 FIB 테이블에서 누락되었습니다.패킷은 소프트웨어에 펀딩됩니다.
직접 연결된 소스(IPv4)	class-cop-ip-connected	직접 연결된 소스의 멀티캐스트 트래픽은 멀티캐스트 상태를 생성하고 하드웨어에 설치할 수 있는 소프트웨어로 전송됩니다.
직접 연결된 소스(IPv6)	class-copp-ipv6-connected	직접 연결된 소스의 멀티캐스트 트래픽은 멀티캐스트 상태를 생성하고 하드웨어에 설치할 수 있는 소프트웨어로 전송됩니다.
브로드캐스트 패킷	클래스 코프 방송	브로드캐스트 패킷(예: 브로드캐스트 DMAC이 있는 IP/Non-IP 및 멀티캐스트 DMAC이 있는 IP 유니캐스트)은 소프트웨어로 유출됩니다.
하드웨어 스위칭에 대해 알 수 없는 프로토콜(즉, 에 의해 지원되지 않음)	class-cop-unknown-protocol	IPX(Internetwork Packet Exchange) 등의 비 IP 프로토콜은 하드웨어 스위칭이 되지 않습니다.소프트웨어는 소프트웨어로 전송되며, 여기에 전달됩니다.
PIM이 비활성화된 라우티드 포트를 통해 들어오는 멀티캐스트 데이터 트래픽	class-copp-mcast-v4-data-on-routedPort	라우팅된 포트(PIM이 비활성화된 경우)를 통해 들어오는 멀티캐스트 데이터 트래픽이 소프트웨어로 유출됩니다.그러나 소프트웨어로 보낼 필요가 없으므로 삭제됩니다.
PIM이 비활성화된 라우티드 포트를 통해 들어오는 멀티캐스트 데이	class-copp-mcast-v6-data-on-routedPort	라우팅된 포트(PIM이 비활성화된 경우)를 통해 들어오는 멀티캐스트 데이터 트래픽이 소프트웨어로 유출됩니다.그러나 소프트웨어로 보낼 필요가 없으므로 삭제됩니다.

터 트래픽		
패킷 브리징을 위한 인그레스 ACL 리디렉션	class cop-ucast-ingress-acl-bridged	하드웨어에는 ACL 리디렉션을 통해 소프트웨어에서 설정한 8개의 ACL 관련 예외가 있습니다.이 패킷은 TCAM(Ternary Content Addressable Memory) 관련 이유로 ACL에서 CPU에 브리징된 유니캐스트 패킷과 관련이 있습니다.
패킷을 브리징하는 이그레스 ACL 리디렉션	class cop-ucast-egress-acl-bridged	하드웨어에는 ACL 리디렉션을 통해 소프트웨어에서 설정한 8개의 ACL 관련 예외가 있습니다.이 패킷은 TCAM(Ternary Content Addressable Memory) 관련 이유로 ACL에서 CPU에 브리징된 유니캐스트 패킷과 관련이 있습니다.
패킷을 CPU로 브리징하기 위해 멀티캐스트 ACL 리디렉션	class cop-mcast-acl-bridged	하드웨어에는 ACL 리디렉션을 통해 소프트웨어에서 설정한 8개의 ACL 관련 예외가 있습니다.이는 멀티캐스트 처리와 관련이 있습니다.
서버 로드 밸런싱 처리를 위한 CPU에 대한 ACL 브리지	클래스 코p-slb	하드웨어에는 ACL 리디렉션을 통해 소프트웨어에서 설정한 8개의 ACL 관련 예외가 있습니다.이는 SLB(Server Load Balancing) 결정을 위한 하드웨어 리디렉션과 관련이 있습니다.
ACL VACL 로그 리디렉션	class copp-vacl-log	하드웨어에는 ACL 리디렉션을 통해 소프트웨어에서 설정한 8개의 ACL 관련 예외가 있습니다.이는 VACL(VLAN Access Control List) ACL에서 Cisco IOS의 CPU로 패킷 리디렉션과 관련이 있습니까?로깅 목적
DHCP 스누핑	class cop-dhcp-snooping	DHCP 스누핑된 패킷은 DHCP 처리를 위해 CPU로 리디렉션됩니다.
MAC 정책 기반 전달	클래스 cop-mac-pbf	이 경우 하드웨어가 패킷을 전달할 수 없으므로 CPU에서 정책 기반 전달이 수행됩니다.
IP-Admission Network Admission Control	수업-ip-수락	호스트의 안티바이러스 자격 증명을 기반으로 네트워크 액세스를 제공하기 위해 다음 옵션 중 하나를 통해 상태 검증이 이루어집니다.(1) L2 인터페이스는 LPIP(LAN Port IP)를 사용하며, 여기서 ARP(Address Resolution Protocol) 패킷은 CPU로 리디렉션되고 (2) L3 인터페이스는 GWIP(Gateway IP)를 사용합니다. 검증 후 인증(*)이 있습니다. L2 인터페이스의 경우 HTTP 패킷 가로채기를 수행하고 URL 리디렉션(*)을 수행할 수 있는 WebAuth입니다. L3 인터페이스의 경우 AuthProxy입니다.
동적 ARP 검사	class cop-arp-snooping	ARP 공격(man-in-the-middle) 방지를 위해 동적 ARP 검사(DAI(Dynamic ARP Inspection)라고도 함)는 ARP 요청/응답을 인터셉트할 때 검증한 다음 다음 중 하나에 대해 CPU에서 처리합니다.(1) 사용자가 구성한 ARP ACL(정적으로 구성된 호스트의 경우), (2) 신뢰할 수 있는 데이터베이스에 저장된 IP 주소 바인딩(즉, DHCP 바인딩)에 대한 MAC 주소. 유효한 ARP 패킷만 로컬

		ARP 캐시를 업데이트하거나 포워딩하는 데 사용됩니다. 검증 프로세스에는 ARP 패킷 CPU 개입이 필요합니다. 즉, DoS 공격을 방지하기 위해 하드웨어 CoPP가 필요합니다.
WCCP용 CPU로 ACL 리디렉션	class cop-wccp	WCCP(Web Cache Communication Protocol) 전달 결정을 위해 패킷/흐름을 CPU로 리디렉션해야 하는 경우에 사용됩니다.
SIA(Service Insertion Architecture)용 CPU로 ACL 리디렉션	class copp-service-insertion	패킷/흐름을 SIA 결정을 위해 CPU로 리디렉션해야 하는 경우에 사용됩니다.
IPv6 네트워크 검색	클래스 COP-nd	IPv6 네트워크 검색 패킷을 CPU로 리디렉션하여 더 자세히 처리하려면 참조:RFC4861

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

구성된 CoPP 클래스 맵에서 트래픽이 관찰되었는지 확인하려면 **show policy-map control-plane** 명령을 입력합니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 컨트롤 플레인 폴리싱, 하드웨어 속도 제한 및 액세스 제어 목록을 사용하여 Cisco Catalyst 6500 Series 스위치 보호
- Catalyst 6500 릴리스 15.0SY 소프트웨어 구성 가이드 - CoPP(Control Plane Policing)
- 기술 지원 및 문서 – Cisco Systems