Nexus 7000 Series 스위치의 CoPP

목차

소개

이 문서에서는 F1, F2, M1 및 M2 Series 모듈과 LC(Line Card)가 포함된 Nexus 7000 Series 스위치에서 CoPP(Control Plane Policing)가 사용되는 내용, 방법 및 이유에 대해 설명합니다. 또한 모범 사례 정책 및 CoPP 정책을 사용자 지정하는 방법도 포함합니다.

사전 요구 사항

요구 사항

Nexus 운영 체제 CLI에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 Supervisor 1 모듈이 포함된 Nexus 7000 Series 스위치를 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.

Nexus 7000 Series 스위치의 CoPP 개요

CoPP는 네트워크 운영에 매우 중요합니다.컨트롤/관리 플레인에 대한 DoS(Denial of Service) 공격은 의도하지 않거나 악의적으로 수행될 수 있으며 일반적으로 높은 트래픽 비율로 인해 과도한 CPU 사용률이 발생합니다.수퍼바이저 모듈은 패킷을 처리하는 데 과도한 시간을 소비합니다.

이러한 공격의 예는 다음과 같습니다.

- ICMP(Internet Control Message Protocol) 에코 요청.
- **ip-options** 집합으로 전송된 패킷

이 경우 다음과 같은 결과가 발생할 수 있습니다.

- Keep-alive 메시지 및 라우팅 프로토콜 업데이트 손실.
- 패킷 대기열을 채우면 무차별 삭제됩니다.
- 느리고 응답하지 않는 대화형 세션입니다.

공격은 네트워크 안정성과 가용성을 압도하고 비즈니스에 영향을 미치는 네트워크 중단으로 이어질 수 있습니다.

CoPP는 DoS 공격으로부터 Supervisor를 보호하는 하드웨어 기반 기능입니다.패킷이 수퍼바이저에 도달할 수 있는 속도를 제어합니다.CoPP 기능은 **컨트롤 플레인**이라는 특수 인터페이스에 연결된 입력 QoS 정책과 같이 모델링됩니다.그러나 CoPP는 QoS의 일부가 아닌 보안 기능입니다 .CoPP는 수퍼바이저를 보호하기 위해 데이터 플레인 패킷을 컨트롤 플레인 패킷에서 분리합니다 (예외 논리). 유효한 패킷(분류)에서 DoS 공격 패킷을 식별합니다. CoPP는 다음 패킷을 분류할 수 있습니다.

- 패킷 수신
- 멀티캐스트 패킷
- 예외 패킷
- 패킷 리디렉션
- 브로드캐스트 MAC + 비 IP 패킷
- 브로드캐스트 MAC + IP 패킷(Cisco Bug ID CSCub47533 - CoPP를 적중하는 L2 VLAN의 패킷(SVI 없음) 참조)
- 멀티캐스트 MAC + IP 패킷
- 라우터 MAC + 비 IP 패킷
- ARP 패킷

패킷이 분류되면 패킷을 표시하고 패킷 유형에 따라 다른 우선순위를 할당하는 데 사용할 수도 있습니다.준수, 초과, 위반 작업(전송, 삭제, 마크 다운)을 설정할 수 있습니다.클래스에 연결된 폴리서가 없는 경우, 기본 폴리서가 추가되며, 그 기본 폴리서는 drop입니다.Glean 패킷은 default-class로 폴리싱됩니다.하나의 속도, 두 가지 색상, 두 개의 속도, 세 가지 색상 폴리싱이 지원됩니다.

Supervisor 모듈의 CPU에 도달하는 트래픽은 다음 네 경로를 통해 들어올 수 있습니다.

1. 라인 카드로 전송되는 트래픽에 대한 인밴드 인터페이스(전면 패널 포트)

2. 관리 트래픽에 사용되는 관리 인터페이스(mgmt0)입니다.

3. 콘솔에 사용되는 CMP(Control and Monitoring Processor) 인터페이스입니다.

4. EOBC(Switched Ethernet Out Band Channel)를 통해 수퍼바이저 모듈에서 라인 카드를 제어하고 상태 메시지를 교환합니다.

Inband 인터페이스를 통해 전송되는 트래픽만 CoPP의 대상이 됩니다. 이는 라인 카드의 FE(Forwarding Engine)를 통해 Supervisor 모듈에 도달하는 유일한 트래픽이기 때문입니다 .CoPP의 Nexus 7000 Series 스위치 구현은 하드웨어 기반이므로 Supervisor 모듈에서 CoPP를 소프트웨어에서 수행하지 않습니다.CoPP 기능(폴리싱)은 각 FE에 독립적으로 구현됩니다.CoPP 정책 맵에 대해 다양한 요율이 구성된 경우 시스템의 라인 카드 수에 대해 고려해야 합니다.

Supervisor가 수신한 총 트래픽은 N회 X이며, 여기서 N은 Nexus 7000 시스템의 FE 수이고 X는 특정 클래스에 허용되는 속도입니다.구성된 폴리서 값은 FE별로 적용되며, CPU에 도달하기 쉬운 총 트래픽은 모든 FE에서 구성 및 전송된 트래픽의 합계입니다.즉, CPU를 적중시키는 트래픽은 구성된 conform rate에 FE 수를 곱한 값과 같습니다.

- N7K-M148GT-11/L LC에는 FE 1개가 있음
- N7K-M148GT-11/L LC에는 FE 1개가 있음
- N7K-M132XP-12/L LC에는 FE 1개가 있음
- N7K-M108X2-12L LC에는 FE 2개가 있음
- N7K-F248XP-15 LC에는 12개의 FE(SOC)가 있음
- N7K-M235XP-23L LC에는 FE 2개가 있음
- N7K-M206FQ-23L LC에는 FE 2개가 있음
- N7K-M202CF-23L LC에는 FE 2개가 있음

CoPP 컨피그레이션은 기본 VDC(가상 디바이스 컨텍스트)에서만 구현됩니다.그러나 CoPP 정책은 모든 VDC에 적용됩니다.모든 라인 카드에 동일한 글로벌 정책이 적용됩니다.CoPP는 동일한 FE의 포트가 서로 다른 VDC(M1 Series 또는 M2 Series LC)에 속하는 경우 VDC 간의 리소스 공유를 적용합니다. 예를 들어, FE 1개, 다른 VDC에서도 CoPP에 대해 동일한 임계값에 대해 계산됩니다.

서로 다른 VDC 간에 동일한 FE가 공유되고 컨트롤 플레인 트래픽의 지정된 클래스가 임계값을 초과하면 동일한 FE의 모든 VDC에 영향을 미칩니다.가능한 경우 CoPP 시행을 격리하려면 VDC당 FE를 1개씩 지정하는 것이 좋습니다.

스위치가 처음 나타나면 기본 정책을 프로그래밍하여 **컨트롤 플레인**을 보호해야 합니다.CoPP는 초기 시작 시퀀스의 일부로 **컨트롤 플레인**에 적용되는 기본 정책을 제공합니다.

Nexus 7000 Series 스위치에서 CoPP를 사용해야 하는 이유

Nexus 7000 Series 스위치는 어그리게이션 또는 코어 스위치로 구축됩니다.따라서, 이것은 네트워크의 귀와 뇌입니다.네트워크의 최대 로드를 처리합니다.빈번한 버스트 요청을 처리해야 합니다.일부 요청은 다음과 같습니다.

- **BPDU(Spanning Tree Bridge Protocol Data Unit) 처리** - 기본값은 2초마다 입니다.

- **First Hop Redundancy** - 여기에는 HSRP(Hot Standby Router Protocol), VRRP(Virtual Router Redundancy Protocol), GLBP(Gateway Load Balancing Protocol)가 포함됩니다. 기본값은 3초

입니다.

- **주소 확인** - 여기에는 ARP/ND(Address Resolution Protocol/Neighbor-Discovery), FIB(Forwarding Information Base) Glean - NIC(Network Interface Controller) 팀 구성과 같은 호스트당 초당 최대 하나의 요청이 포함됩니다.
- **DHCP(Dynamic Host Control Protocol)** - DHCP 요청, 릴레이 - 호스트당 초당 최대 하나의 요청.
- 레이어 3(L3)에 대한 **라우팅 프로토콜**
- **데이터 센터 상호 연결** - OTV(Overlay Transport Virtualization), MPLS(Multiprotocol Label Switching) 및 VPLS(Virtual Private LAN Service).

CoPP는 잘못 구성된 서버 또는 잠재적인 DoS 공격으로부터 CPU를 보호하기 위해 필수적입니다. 따라서 CPU는 중요한 컨트롤 플레인 메시지를 처리할 수 있는 충분한 사이클을 갖게 됩니다.

Nexus 7000 Series 스위치의 컨트롤 플레인 처리

Nexus 7000 Series 스위치는 분산된 컨트롤 플레인 접근 방식을 사용합니다.각 I/O 모듈에 멀티코어가 있으며, 수퍼바이저 모듈의 스위치 컨트롤 플레인용 멀티코어가 있습니다.ACL(Access Control List) 및 FIB 프로그래밍을 위해 집중적인 작업을 입출력 모듈 CPU로 오프로드합니다.라인 카드 수로 컨트롤 플레인 용량을 확장합니다.이를 통해 중앙 집중식 접근 방식에서 볼 수 있는 Supervisor CPU 병목 현상이 방지됩니다.하드웨어 속도 리미터 및 하드웨어 기반 CoPP는 컨트롤 플레인을 악성 또는 악성 활동으로부터 보호합니다.

CoPP 모범 사례 정책

Cisco NX-OS Release 5.2에 CoPP BPP(Best Practices Policy)가 도입되었습니다. **show running-config** 명령 출력에는 CoPP BPP의 내용이 표시되지 않습니다.show run **all** 명령은 CoPP BPP의 내용을 표시합니다.

```
-----------------------------------SNIP----------------------------------------
SITE1-AGG1# show run copp

!! Command: show running-config copp
!! Time: Mon Nov 5 22:21:04 2012

version 5.2(7)
copp profile strict


SITE1-AGG1# show run copp all

!! Command: show running-config copp all
!! Time: Mon Nov 5 22:21:15 2012

version 5.2(7)
------------------------------SNIP---------------------
control-plane
service-policy input copp-system-p-policy-strict
```

```
copp profile strict
```

CoPP는 사용자에게 기본 정책에 대한 4가지 옵션을 제공합니다.

- 엄격한
- 보통
- 너그러운
- Dense(릴리스 6.0(1)에 도입)

옵션을 선택하지 않았거나 설정을 건너뛴 경우 엄격한 폴리싱이 적용됩니다.이러한 모든 옵션은 폴리싱에 동일한 클래스 맵과 클래스를 사용하지만 CIR(Committed Information Rate) 및 BC(Burst Count) 값은 서로 다릅니다.5.2.1 이전 Cisco NX-OS 릴리스에서는 **setup** 명령을 사용하여 옵션을 변경했습니다.Cisco NX-OS Release 5.2.1은 **setup** 명령 없이 옵션을 변경할 수 있도록 CoPP BPP의 향상된 기능을 도입했습니다.copp **profile** 명령을 사용합니다.

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# copp profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1(config)# copp profile strict
SITE1-AGG1(config)# exit
```

show copp **profile <profile-type>** 명령을 사용하여 기본 CoPP BPP 컨피그레이션을 확인합니다 .show copp **status** 명령을 사용하여 CoPP 정책이 올바르게 적용되었는지 확인합니다.

```
SITE1-AGG1# show copp status
Last Config Operation: copp profile strict
Last Config Operation Timestamp: 20:40:27 PST Nov 5 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-system-p-policy-strict
```

두 CoPP BPP 간의 차이를 보려면 show copp diff profile **<profile-type 1> profile <profile-type 2>** 명령을 사용합니다.

```
SITE1-AGG1# show copp diff profile strict profile moderate
A '+' represents a line that has been added and
a '-' represents a line that has been removed.
-policy-map type control-plane copp-system-p-policy-strict
- class copp-system-p-class-critical
- set cos 7
- police cir 39600 kbps bc 250 ms conform transmit violate drop
- class copp-system-p-class-important
- set cos 6
- police cir 1060 kbps bc 1000 ms conform transmit violate drop
----------------------SNIP----------------------------------------
+policy-map type control-plane copp-system-p-policy-moderate
+ class copp-system-p-class-critical
+ set cos 7
+ police cir 39600 kbps bc 310 ms conform transmit violate drop
+ class copp-system-p-class-important
+ set cos 6
+ police cir 1060 kbps bc 1250 ms conform transmit violate drop
----------------------SNIP----------------------------------------
```

CoPP 정책을 사용자 지정하는 방법

사용자는 맞춤형 CoPP 정책을 생성할 수 있습니다.CoPP BPP는 읽기 전용이므로 기본 CoPP BPP를 **복제한** 다음 컨트롤 플레인 인터페이스에 연결합니다.

```
SITE2-AGG1(config)# policy-map type control-plane copp-system-p-policy-strict
^
% String is invalid, 'copp-system-p-policy-strict' is not an allowed string at
'^' marker.
```

copp **copy profile <profile-type> <prefix> [suffix]** 명령은 CoPP BPP의 클론을 생성합니다.기본 컨피그레이션을 수정하는 데 사용됩니다.copp **copy profile** 명령은 **exec mode** 명령입니다.사용자는 access-list, class-maps 및 policy-map 이름의 접두사 또는 접미사를 선택할 수 있습니다.예를 들어 **copp-system-p-policy-strict**는 **[prefix]copp-policy-strict[suffix]로 변경됩니다**.복제된 구성은 사용자 구성으로 처리되며 **show run** 출력에 포함됩니다.

```
SITE1-AGG1# copp copy profile ?
dense The Dense Profile
lenient The Lenient Profile
moderate The Moderate Profile
strict The Strict Profile
SITE1-AGG1# copp copy profile strict ?
prefix Prefix for the copied policy
suffix Suffix for the copied policy
SITE1-AGG1# copp copy profile strict suffix ?
WORD Enter prefix/suffix for the copied policy (Max Size 20)
SITE1-AGG1# copp copy profile strict suffix CUSTOMIZED-COPP
SITE1-AGG1# show run copp | grep policy-map
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1#
```

지정된 PIR(Permitted Information Rate)을 초과하고 위반하는 트래픽을 다음 명령으로 표시할 수 있습니다.

```
SITE1-AGG1(config)# policy-map type
control-plane copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms ?
<CR>
conform Specify a conform action
pir Specify peak information rate

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir ?
<1-80000000000> Peak Information Rate in bps/kbps/mbps/gbps

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps ?
<CR>
<1-512000000> Peak Burst Size in bytes/kbytes/mbytes/packets/ms/us
be Specify extended burst
conform Specify a conform action

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform ?
drop Drop the packet
set-cos-transmit Set conform action cos val
set-dscp-transmit Set conform action dscp val
set-prec-transmit Set conform action precedence val
transmit Transmit the packet

SITE1-AGG1(config-pmap-c)# police cir 59600 kbps bc 250 ms pir 100 mbps conform
set-dscp-transmit ef exceed set dscp1 dscp2 table cir-markdown-map violate
set1 dscp3 dscp4 table1 pir-markdown-map
```

```
SITE1-AGG1(config-pmap-c)#
```

맞춤형 CoPP 정책을 전역 인터페이스 **컨트롤 플레인에 적용합니다**.CoPP 정책이 올바르게 적용되었는지 확인하려면 show copp status 명령을 사용합니다.

```
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# service-policy input ?
copp-policy-strict-CUSTOMIZED-COPP

SITE1-AGG1(config-cp)# service-policy input copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-cp)# exit
SITE1-AGG1# sh copp status
Last Config Operation: service-policy input copp-policy-strict-CUSTOMIZED-COPP
Last Config Operation Timestamp: 18:04:03 UTC May 15 2012
Last Config Operation Status: Success
Policy-map attached to the control-plane: copp-policy-strict-CUSTOMIZED-COPP
```

맞춤형 CoPP 정책 사례 연구

이 섹션에서는 로컬 인터페이스를 자주 ping하기 위해 고객이 여러 모니터링 디바이스를 필요로 하는 실제 예를 설명합니다.고객이 CoPP 정책을 수정하려는 경우 다음과 같은 문제가 발생합니다.

- 이러한 특정 주소가 로컬 디바이스를 ping할 수 있고 정책을 위반하지 않도록 CIR을 높입니다.
- 문제 해결을 위해 다른 IP 주소가 로컬 디바이스를 ping할 수 있는 기능을 유지하지만, 더 낮은 CIR에서 유지할 수 있도록 허용합니다.

다음 예에는 별도의 클래스 맵으로 사용자 지정 정책을 생성하는 솔루션이 나와 있습니다.별도의 클래스 맵에는 모니터링 디바이스의 지정된 IP 주소가 포함되며 클래스 맵에는 더 높은 CIR이 있습니다.이렇게 하면 원래 클래스 맵 *모니터링*이 *유지되며*, 이는 하위 CIR에서 다른 모든 IP 주소에 대한 ICMP 트래픽을 캡처합니다.

```
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
F340.13.19-Nexus7000-1(config)# copp copy profile strict prefix TAC_CHANGE
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# ip access-list TAC_CHANGE-copp-acl-specific-icmp
F340.13.19-Nexus7000-1(config-acl)#
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo
F340.13.19-Nexus7000-1(config-acl)# permit icmp host 1.1.1.1 host 2.2.2.2 echo-reply
F340.13.19-Nexus7000-1(config-acl)#
F340.13.19-Nexus7000-1(config-acl)# exit
F340.13.19-Nexus7000-1(config)# sho ip access-lists TAC_CHANGE-copp-acl-specific-
icmp IP access list TAC_CHANGE-copp-acl-specific-icmp
10 permit icmp 1.1.1.1/32 2.2.2.2/32 echo
20 permit icmp 1.1.1.1/32 2.2.2.2/32 echo-reply
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# class-map type control-plane match-any
TAC_CHANGE-copp-class-specific-icmp
F340.13.19-Nexus7000-1(config-cmap)# match access-group name TAC_CHANGE-copp
-acl-specific-icmp
F340.13.19-Nexus7000-1(config-cmap)#exit
```

```
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#policy-map type control-plane TAC_CHANGE-copp-
policy-strict
F340.13.19-Nexus7000-1(config-pmap)# class TAC_CHANGE-copp-class-specific-icmp
insert-before
TAC_CHANGE-copp-class-monitoring
F340.13.19-Nexus7000-1(config-pmap-c)# set cos 7
F340.13.19-Nexus7000-1(config-pmap-c)# police cir 5000 kbps bc 250 ms conform transmit
violate drop
F340.13.19-Nexus7000-1(config-pmap-c)# exit
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)#
F340.13.19-Nexus7000-1(config-pmap)# exit
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)#
F340.13.19-Nexus7000-1(config)# control-plane
F340.13.19-Nexus7000-1(config-cp)# service-policy input TAC_CHANGE-copp-policy-strict
F340.13.19-Nexus7000-1(config-cp)# end
F340.13.19-Nexus7000-1#
F340.13.19-Nexus7000-1# sho policy-map interface control-plane
Control Plane
service-policy input TAC_CHANGE-copp-policy-strict
<abbreviated output>
class-map TAC_CHANGE-copp-class-specific-icmp (match-any)
match access-group name TAC_CHANGE-copp-acl-specific-icmp
set cos 7
police cir 5000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 4:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 7:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/secclass-map TAC_CHANGE-copp-class-monitoring (match-any)
match access-group name TAC_CHANGE-copp-acl-icmp
match access-group name TAC_CHANGE-copp-acl-icmp6
match access-group name TAC_CHANGE-copp-acl-mpls-oam
match access-group name TAC_CHANGE-copp-acl-traceroute
match access-group name TAC_CHANGE-copp-acl-http-response
match access-group name TAC_CHANGE-copp-acl-smtp-response
match access-group name TAC_CHANGE-copp-acl-http6-response
match access-group name TAC_CHANGE-copp-acl-smtp6-response
set cos 1
police cir 130 kbps bc 1000 ms
conform action: transmit
violate action: drop
module 4:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
```

```
module 7:
conformed 0 bytes,
5-min offered rate 0 bytes/sec
peak rate 0 bytes/sec
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
<abbreviated output>
```

CoPP 데이터 구조

CoPP BPP 데이터 구조는 다음과 같이 구성됩니다.

- **ACL 구성**:IP ACL 및 MAC ACL입니다.
- **분류자 구성**:IP ACL 또는 MAC ACL과 일치하는 클래스 맵.
- **폴리서 구성**:CIR, BC 설정, 동작 준수, 동작 위반폴리서는 두 가지 속도(CIR 및 BC)와 두 가지 색상(conform 및 violations)을 갖습니다.

```
mac access-list copp-system-p-acl-mac-fabricpath-isis
permit any 0180.c200.0015 0000.0000.0000
permit any 0180.c200.0014 0000.0000.0000

ip access-list copp-system-p-acl-bgp
permit tcp any gt 1024 any eq bgp
permit tcp any eq bgp any gt 1024

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-pim
<snip>
match access-group name copp-system-p-acl-mac-fabricpath-isis
policy-map type control-plane copp-system-p-policy-dense
class copp-system-p-class-critical
set cos 7
police cir 5000 kbps bc 250 ms conform transmit violate drop
```

CoPP 확장 계수

Cisco NX-OS Release 6.0에 도입된 Scale Factor Configuration은 특정 라인 카드에 대해 적용된 CoPP 정책의 폴리서 속도를 확장하는 데 사용됩니다.이렇게 하면 특정 라인 카드에 대한 폴리서 속도가 증가하거나 감소하지만 현재 CoPP 정책은 변경되지 않습니다.변경 사항은 즉시 적용되며 CoPP 정책을 다시 적용할 필요가 없습니다.

```
scale factor option configured within control-plane interface:
Scale-factor <scale factor value> module <module number>
<scale factor value>: from 0.10 to 2.00
Scale factor is recommended when a chassis is loaded with both F2 and M
Series modules.
SITE1-AGG1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SITE1-AGG1(config)# control-plane
SITE1-AGG1(config-cp)# scale-factor ?
```

```
<whole>.<decimal> Specify scale factor value from 0.10 to 2.00

SITE1-AGG1(config-cp)# scale-factor 1.0 ?
module Module

SITE1-AGG1(config-cp)# scale-factor 1.0 module ?
<1-10> Specify module number

SITE1-AGG1(config-cp)# scale-factor 1.0 module 4
SITE1-AGG1# show system internal copp info
<snip>
Linecard Configuration:
-----------------------
Scale Factors
Module 1: 1.00
Module 2: 1.00
Module 3: 1.00
Module 4: 1.00
Module 5: 1.00
Module 6: 1.00
Module 7: 1.00
Module 8: 1.00
Module 9: 1.00
Module 10: 1.00
```

CoPP 모니터링 및 관리

Cisco NX-OS Release 5.1에서는 임계값이 초과될 경우 Syslog 메시지를 트리거하는 CoPP 클래스 이름별로 삭제 임계값을 구성할 수 있습니다.이 명령은 **drop threshold <dropped bytes count> level <logging level>을 로깅하고 있습니다**.

```
SITE1-AGG1(config)# policy-map type control-plane
copp-policy-strict-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap)# class copp-class-critical-CUSTOMIZED-COPP
SITE1-AGG1(config-pmap-c)# logging ?
drop Logging for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop ?
threshold Threshold value for dropped packets

SITE1-AGG1(config-pmap-c)# logging drop threshold ?
<CR>
<1-80000000000> Dropped byte count

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 ?
<CR>
level Syslog level

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level ?
<1-7> Specify the logging level between 1-7

SITE1-AGG1(config-pmap-c)# logging drop threshold 100 level 7
```

다음은 Syslog 메시지의 예입니다.

```
%COPP-5-COPP_DROPS5: CoPP drops exceed threshold in class:
copp-system-class-critical,
check show policy-map interface control-plane for more info.
```

CoPP 카운터

CoPP는 다른 인터페이스와 동일한 QoS 통계를 지원합니다.CoPP를 지원하는 모든 I/O 모듈에 대한 서비스 정책을 구성하는 클래스의 통계를 표시합니다.CoPP에 대한 통계를 보려면 **show policy-map interface control-plane** 명령을 사용합니다.

> **참고:**모든 클래스는 위반 패킷과 관련하여 모니터링해야 합니다.

```
SITE1-AGG1# show policy-map interface control-plane
Control Plane

service-policy input: copp-policy-strict-CUSTOMIZED-COPP

class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
match access-group name copp-acl-bgp-CUSTOMIZED-COPP
match access-group name copp-acl-bgp6-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp-CUSTOMIZED-COPP
match access-group name copp-acl-igmp-CUSTOMIZED-COPP
match access-group name copp-acl-msdp-CUSTOMIZED-COPP
match access-group name copp-acl-ospf-CUSTOMIZED-COPP
match access-group name copp-acl-ospf6-CUSTOMIZED-COPP
match access-group name copp-acl-pim-CUSTOMIZED-COPP
match access-group name copp-acl-pim6-CUSTOMIZED-COPP
match access-group name copp-acl-rip-CUSTOMIZED-COPP
match access-group name copp-acl-rip6-CUSTOMIZED-COPP
match access-group name copp-acl-vpc-CUSTOMIZED-COPP
match access-group name copp-acl-eigrp6-CUSTOMIZED-COPP
match access-group name copp-acl-mac-l2pt-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-ldp-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-oam-CUSTOMIZED-COPP
match access-group name copp-acl-mpls-rsvp-CUSTOMIZED-COPP
match access-group name copp-acl-otv-as-CUSTOMIZED-COPP
match access-group name copp-acl-mac-otv-isis-CUSTOMIZED-COPP
match access-group name copp-acl-mac-fabricpath-isis-CUSTOMIZED-COPP
match protocol mpls router-alert
match protocol mpls exp 6
set cos 7
threshold: 100, level: 7
police cir 39600 kbps , bc 250 ms
module 1 :
conformed 22454 bytes; action: transmit
violated 0 bytes; action: drop

module 2 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop

module 3 :
conformed 19319 bytes; action: transmit
violated 0 bytes; action: drop

module 4 :
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

모든 클래스 맵 및 I/O 모듈에 대한 컨피그레이션 및 위반된 카운터의 집계 보기를 얻으려면 **show policy-map interface control-plane을** 사용합니다. **| i "class|conform|violated"** 명령

```
SITE1-AGG1# show policy-map interface control-plane | i "class|conform|violated"
class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
conformed 123126534 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 107272597 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
class-map copp-class-important-CUSTOMIZED-COPP (match-any)
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

클래스 copp-class-l2-default 및 class-default는 구성된 카운터에서도 높은 증가율이 발생하지 않도록 모니터링해야 합니다.이 두 클래스는 구성된 카운터에 대한 값이 낮아야 하며 위반된 카운터가 증가하지 않아야 합니다.

ACL 카운터

CoPP 클래스 맵에서 사용되는 IP ACL 또는 MAC ACL에 대해 **statistics per-entry** 명령은 지원되지 않으며 CoPP IP ACL 또는 MAC ACL에 적용할 때는 영향을 주지 않습니다. (CLI 파서에서 수행한 CLI 검사는 없습니다.) I/O 모듈에서 CoPP MAC ACL 또는 IP ACL 적중을 보려면 **show system internal access-list input detail** 명령을 사용합니다.

예를 들면 다음과 같습니다.

```
!! 0180.c200.0041 is the destination MAC used for FabricPath IS-IS

SITE1-AGG1# show system internal access-list input entries det | grep 0180.c200.0041
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [30042]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [29975]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8965]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [8935]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [58233]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [27689]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[00fc:00f7:00f7] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```

```
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
[0148:00fe:00fe] qos 0000.0000.0000 0000.0000.0000 0180.c200.0041 ffff.ffff.ffff [0]
```

CoPP 구성 모범 사례

다음은 CoPP 구성에 대한 모범 사례 권장 사항입니다.

- 기본적으로 엄격한 CoPP 모드를 사용합니다.
- 섀시에 F2 Series 모듈이 완전히 로드되거나 다른 I/O 모듈보다 더 많은 F2 Series 모듈이 로드될 경우 Dense CoPP 프로파일을 사용하는 것이 좋습니다.
- CoPP는 사용하지 않는 것이 좋습니다.필요에 따라 기본 CoPP를 조정합니다.
- 의도하지 않은 삭제를 모니터링하고 예상되는 트래픽에 따라 기본 CoPP 정책을 추가하거나 수정합니다.
- 섀시의 FE 수에 따라 CoPP에 대한 CIR 및 BC 설정을 늘리거나 줄일 수 있습니다.또한 네트워크에서 디바이스의 역할, 실행 중인 프로토콜 등을 기반으로 합니다.
- **데이터 센터**에서 트래픽 패턴이 지속적으로 변화하기 때문에 CoPP의 사용자 지정은 지속적인 프로세스입니다.
- CoPP 및 VDC:동일한 FE의 모든 포트는 동일한 VDC에 속해야 합니다. 이 VDC는 F2 Series LC에서 쉽게 사용할 수 있지만 M2 Series 또는 M108 LC에서는 쉽지 않습니다.동일한 FE의 포트가 다른 VDC(M1 Series 또는 M2 Series LC)에 속하는 경우 VDC 간에 CoPP 리소스 공유가 이루어지기 때문입니다. 한 FE의 포트(다른 VDC에서도)는 CoPP에 대해 동일한 임계값에 대해 계산됩니다.
- F2 Series 및 M Series 모듈을 모두 사용하여 섀시를 로드하면 스케일 팩터 컨피그레이션이 권장됩니다.

CoPP 모니터링 모범 사례

다음은 CoPP 모니터링을 위한 모범 사례 권장 사항입니다.

- CoPP에서 적용되는 삭제를 모니터링하기 위해 CoPP(Cisco NX-OS Release 5.1)에 대한 syslog 메시지 임계값을 구성합니다.
- 트래픽 클래스 내에서 삭제되는 임계값이 사용자 구성 임계값을 초과할 경우 Syslog 메시지가 생성됩니다.
- logging drop threshold **<packet-count> level <level>** 명령을 사용하여 각 트래픽 클래스 내에서 로깅 임계값 및 레벨**을 사용자 지정할** 수 있습니다.
- CoPP MAC ACL 또는 IP ACL에 대한 "Statistics per-entry" 옵션은 지원되지 않으므로 **show system internal access-list input entries det** 명령을 사용하여 ACE(Access Control Entries) 적

중 수를 모니터링합니다.

- **class copp-class-l2-default 및 class-default** 명령은 구성된 카운터에서도 높은 증가율이 발생하지 않도록 모니터링해야 합니다.
- 모든 클래스는 위반 패킷과 관련하여 모니터링해야 합니다.
- cop-**class-critical**은 매우 중요하지만 **위반된 삭제** 정책을 가지고 있기 때문에 클래스가 위반이 시작되는 시점에 가까워질 때 조기 표시를 수신하기 위해 패킷의 비율을 모니터링하는 것이 좋습니다.위반된 카운터가 이 클래스에 대해 증가한다고 해서 빨간색 경고가 아닐 수 있습니다.오히려 단기적으로 조사해야 한다는 의미다.
- 각 Cisco NX-OS 코드 업그레이드 후 또**는** 각 주요 Cisco NX-OS 코드 업그레이드 후 또는 최소한 각 주요 Cisco NX-OS 코드 업그레이드 후 copp profile strict 명령을 사용합니다.CoPP 수정이 이전에 완료된 경우 다시 적용해야 합니다.

결론

- CoPP는 DoS 공격으로부터 Supervisor를 보호하는 하드웨어 기반 기능입니다.
- M1, F2 및 M2 시리즈 LC는 CoPP를 지원합니다.F1 시리즈 LC는 CoPP를 지원하지 않습니다.
- CoPP 구성은 MQC(Modular QoS CLI)와 유사합니다.
- CoPP 컨피그레이션 및 모니터링은 기본 VDC에서만 수행됩니다.
- 기본 CoPP BPP는 엄격한, 보통, 완화된, 고밀도 옵션과 함께 사용할 수 있습니다.
- 특정 네트워크 요구 사항에 맞게 맞춤형 CoPP 규칙에 CoPP BPP 복제
- CoPP 카운터(class-map당 바이트 단위로 구성 및 위반)는 show policy-map **interface control-plane** 명령**과 함께** 표시됩니다.
- Supervisor 모듈의 CPU에서 받은 트래픽은 총 FE의 배수와 허용되는 환율과 같습니다.
- 서로 다른 VDC에서 하나의 FE의 공유 포트를 사용하지 않도록 하십시오.
- 기능을 성공적으로 구현하고 모니터링하려면 CoPP 모범 사례를 따르십시오.

지원되지 않는 기능

다음 기능은 지원되지 않습니다.

- 분산 집계 폴리싱.
- 마이크로플로우 폴리싱.

- 이그레스 예외 폴리싱.
- QinQ(dot1q 터널 포트)에서 오는 BPDU에 대한 CoPP 지원:CDP(Cisco Discovery Protocol), DOT1x, STP(Spanning Tree Protocol) 및 VTP(VLAN Trunk Protocol).