Nexus 플랫폼에서 컨트롤 플레인 정책 위반 확인

목차

소개

이 문서에서는 Cisco Nexus 스위치의 CoPP(Control Plane Policing)에 대한 세부 정보 및 기본이 아닌 클래스 위반에 대한 관련 영향에 대해 설명합니다.

사전 요구 사항

CoPP(Control Plane Policing), 지침 및 제한 사항, 일반 컨피그레이션에 대한 기본 정보를 이해하는 것이 좋습니다. QoS(Quality-of-Service) 폴리싱(CIR) 기능뿐만 아니라 이 기능에 대한 자세한 내용은 해당 문서를 참조하십시오.

https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/Security/cisco-nexus-9000-nx-os-security-configuration-guide-102x/m-configuring-copp.html

https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/116043-copp-nexus7000-tshoot-00.html

https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/qos/cisco-nexus-9000-nx-os-quality-of-service-configuration-guide-102x/m-configuring-policing.html

사용되는 구성 요소

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

배경 정보

컨트롤 플레인 트래픽은 두 개의 보호 레이어, 하드웨어 속도 리미터 및 CoPP를 통과하는 일치하는 트래픽을 푸킹하도록 프로그래밍된 리디렉션 ACL(Access Control List)을 통해 수퍼바이저 모듈로 리디렉션됩니다. 수퍼바이저 모듈에 대한 중단이나 공격이 선택되지 않은 경우 심각한 네트워크 중단이 발생할 수 있습니다. 따라서 CoPP는 보호 메커니즘의 역할을 합니다. 컨트롤 플레인 레벨에서 불안정성이 발생하는 경우 루프나 플러드 또는 비인가 디바이스에서 생성된 비정상적인 트래픽 패턴은 세금을 부과하여 수퍼바이저가 합법적인 트래픽을 처리하지 못하도록 할 수 있으므로 CoPP를 확인하는 것이 중요합니다. 이러한 공격은 비인가 디바이스에서 의도치 않게 또는 공격자가 악의적으로 수행할 수 있으며, 일반적으로 수퍼바이저 모듈 또는 CPU로 향하는 트래픽이 높습니다.

CoPP(Control Plane Policing)는 대역 내(전면 패널) 포트를 통해 수신되는 모든 패킷을 분리하고 분류하여 제어판을 보호하는 기능으로, 라우터 주소로 전송되거나 CIR(Committed Input Rate)을 기반으로 수퍼바이저가 개입하고 이를 폴리싱해야 합니다. 이 기능을 사용하면 정책 맵을 컨트롤 플레인에 적용할 수 있습니다. 이 정책 맵은 정상적인 QoS(Quality of Service) 정책처럼 보이며, 비관리 포트에서 스위치에 들어오는 모든 트래픽에 적용됩니다. 폴리싱을 통해 수퍼바이저 모듈을 보호하면 패킷이 삭제되고 스위치가 과중한 상태로 성능에 영향을 미치지 않도록 하여 스위치에서 각 클래스의 커밋된 입력 속도를 초과하는 트래픽의 홍수를 줄일 수 있습니다.

CoPP 카운터를 지속적으로 모니터링하고 타당성을 입증하는 것이 이 문서의 목적입니다. CoPP 위반이 선택되지 않은 경우 제어 평면이 해당 영향을 받는 클래스의 정적인 트래픽을 처리하지 못하게 할 수 있습니다. CoPP 구성은 네트워크 및 인프라 요구 사항에 대응해야 하는 진화하고 지속적인 프로세스입니다. CoPP에는 3가지 기본 시스템 정책이 있습니다. 기본적으로 Cisco는 기본 정책 **'strict'**를 초기 시작점으로 사용하는 것이 좋으며 이 문서의 기초로 사용됩니다.

CoPP는 전면 패널 포트를 통해 수신되는 대역 내 트래픽에만 적용됩니다. 대역 외 관리 포트(mgmt0)는 CoPP의 대상이 아닙니다. Cisco NX-OS 디바이스 하드웨어는 포워딩 엔진별로 CoPP를 수행합니다. 따라서 종합 트래픽이 수퍼바이저 모듈을 압도하지 않도록 속도를 선택합니다. CIR은 모든 모듈의 CPU 바운드 트래픽의 집계 트래픽에 적용되므로 EoR/R 모듈형 스위치에는 특히 중요합니다.

적용 가능한 하드웨어

이 문서에서 다루는 구성 요소는 모든 Cisco Nexus 데이터 센터 스위치에 적용됩니다.

컨트롤 플레인 폴리싱 해석

이 문서의 핵심은 Nexus 스위치에서 볼 수 있는 가장 일반적인 비기본 클래스 위반을 해결하는 것입니다.

표준 CoPP 기본 프로필

CoPP를 해석하는 방법을 이해하려면 먼저 프로필을 적용하고 기본 프로필 또는 사용자 지정 프로필이 스위치에 적용되었는지 확인해야 합니다.

> **참고:** 모범 사례로서 모든 Nexus 스위치에는 CoPP가 활성화되어 있어야 합니다. 이 기능이 활성화되지 않으면 다른 플랫폼이 SUP(Supervisor) 바운드 트래픽을 제한할 수 있으므로 모든 컨트롤 플레인 트래픽이 불안정해질 수 있습니다. 예를 들어, Nexus 9000에서 CoPP가 활성화되지 않은 경우 SUP로 향하는 트래픽은 50pps로 제한되므로 스위치가 거의 작동하지 않습니다. CoPP는 Nexus 3000 및 Nexus 9000 플랫폼의 요구 사항으로 간주됩니다.

CoPP가 활성화되지 않은 경우, '**setup**' 명령을 실행하거나 컨피그레이션 옵션에서 표준 기본 정책 중 하나를 적용하여 스위치에서 다시 활성화하거나 구성할 수 있습니다. **copp 프로필 [dense|unlimited|moderate|strict]**.

보호되지 않는 디바이스는 트래픽을 클래스로 적절하게 분류하고 분리하지 않으므로 특정 기능 또는 프로토콜에 대한 서비스 거부 동작이 해당 범위에 포함되지 않으며 전체 컨트롤 플레인에 영향을 줄 수 있습니다.

> **참고:** CoPP 정책은 TCAM(Ternary Content-Addressable Memory) 분류 리디렉션에 의해 구현되며 '**show system internal access-list input statistics module X(시스템 내부 액세스 목록 입력 통계 모듈 표시)** 아래에서 직접 확인할 수 있습니다. **| b CoPP**' 또는 '**show hardware access-list input detail**'.

N9K1# show copp status Last Config Operation: None Last Config Operation Timestamp: None Last Config Operation Status: None Policy-map attached to the control-plane: copp-system-p-policy-strict copp-system-p-policy-strict is one of the system default profiles, in particular the strict profile. N9K1# show running-config copp !Command: show running-config copp !Running configuration last done at: Tue Apr 26 16:34:10 2022 !Time: Sun May 1 16:30:57 2022 version 10.2(1) Bios:version 05.45 copp profile strict

컨트롤 플레인 폴리싱 클래스

CoPP는 IP 또는 MAC ACL에 해당하는 일치를 기준으로 트래픽을 분류하므로 어떤 트래픽이 어떤 클래스로 분류되는지 이해하는 것이 중요합니다.

플랫폼에 따라 달라지는 클래스는 다를 수 있습니다. 따라서 클래스를 확인하는 방법을 이해하는 것이 중요합니다.

예를 들어 **Nexus 9000** TOR(Top-of-Rack):

```
N9K1# show policy-map interface control-plane
```

```
Control Plane

Service-policy input: copp-system-p-policy-strict
...
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
...
```

이 예에서 class-map cop-**system-p-class-critical은 BGP**(Border Gateway Protocol), OSPF(Open Shortest Path First), EIGRP(Enhanced Interior Gateway Router Protocol)와 같은 라우팅 프로토콜과 관련된 트래픽을 포함하며 vPC와 같은 다른 프로토콜을 포함합니다.

IP 또는 MAC ACL 명명 규칙은 주로 관련된 프로토콜 또는 기능에 대해 자체 설명이며 prefix cop-**system-p-acl-[protocol|feature]입니다**.

특정 클래스를 보려면 show 명령을 실행하는 동안 직접 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
N9K-4# show policy-map interface control-plane class copp-system-p-class-management
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
```

```
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes
module 1 :
transmitted 0 bytes;
5-minute offered rate 0 bytes/sec
conformed 0 peak-rate bytes/sec

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

CoPP 기본 프로파일은 일반적으로 기본 컨피그레이션의 일부로 숨겨져 있지만 'show running-**conf copp all'을** 사용하여 컨피그레이션을 볼 수 있습니다.

```
N9K1# show running-config copp all

!Command: show running-config copp all
!Running configuration last done at: Tue Apr 26 16:34:10 2022
!Time: Sun May 1 16:41:55 2022

version 10.2(1) Bios:version 05.45
control-plane
scale-factor 1.00 module 1
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-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
(snip)
...
```

class-map **copp-system-p-class-critical**은 앞에서 볼 수 있듯이 시스템 ACL을 호출하는 여러 match 문을 참조하며, 기본적으로 숨겨져 있으며 일치하는 분류를 참조합니다. 예를 들어, BGP의 경우:

```
N9K1# show running-config aclmgr all | b copp-system-p-acl-bgp
ip access-list copp-system-p-acl-bgp
10 permit tcp any gt 1023 any eq bgp
20 permit tcp any eq bgp any gt 1023
(snip)
```

즉, 모든 BGP 트래픽이 이 클래스와 일치하며, 동일한 클래스의 다른 모든 프로토콜**과** 함께 cop-system-p-class-critical로 분류됩니다.

Nexus 7000은 Nexus 9000과 매우 유사한 CoPP 기능 구조를 따릅니다.

```
N77-A-Admin# show policy-map interface control-plane
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert
set cos 7
police cir 36000 kbps bc 250 ms
conform action: transmit
violate action: drop
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
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
```

Nexus 7000에서는 모듈형 스위치이므로 이 클래스가 모듈로 나누어져 있습니다. 그러나 CIR은 모든 모듈의 집계에 적용되고 CoPP는 전체 섀시에 적용됩니다. CoPP 확인 및 출력은 기본 또는 관리자 VDC(Virtual Device Context)에서만 볼 수 있습니다.
CoPP 위반을 유발하는 과도한 CPU 바인딩된 트래픽이 있는 VDC의 불안정성이 다른 VDC의 안정성에 영향을 미칠 수 있으므로 컨트롤 플레인 문제가 확인되면 Nexus 7000에서 CoPP를 확인하는 것이 특히 중요합니다.

Nexus 5600에서 클래스는 다릅니다. 따라서 BGP의 경우 고유한 개별 클래스입니다.

```
N5K# show policy-map interface control-plane
Control Plane
(snip)
class-map copp-system-class-bgp (match-any)
match protocol bgp
police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
(snip)
```

Nexus 3100에는 3개의 라우팅 프로토콜 클래스가 있으므로, 어떤 클래스 BGP가 속하는지 확인하려면 참조되는 4개의 CoPP ACL을 상호 참조합니다.
EIGRP는 Nexus 3100의 자체 클래스에서 처리합니다.

```
N3K-C3172# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy

class-map copp-s-routingProto2 (match-any)
match access-group name copp-system-acl-routingproto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-v6routingProto2 (match-any)
match access-group name copp-system-acl-v6routingProto2
police pps 1300
OutPackets 0
DropPackets 0
class-map copp-s-eigrp (match-any)
match access-group name copp-system-acl-eigrp
match access-group name copp-system-acl-eigrp6
police pps 200
OutPackets 0
DropPackets 0
class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 0
DropPackets 0

N3K-C3172# show running-config aclmgr

!Command: show running-config aclmgr
!No configuration change since last restart
!Time: Sun May 1 18:14:16 2022

version 9.3(9) Bios:version 5.3.1
ip access-list copp-system-acl-eigrp
10 permit eigrp any 224.0.0.10/32
ipv6 access-list copp-system-acl-eigrp6
10 permit eigrp any ff02::a/128
ip access-list copp-system-acl-routingproto1
10 permit tcp any gt 1024 any eq bgp
20 permit tcp any eq bgp any gt 1024
30 permit udp any 224.0.0.0/24 eq rip
40 permit tcp any gt 1024 any eq 639
50 permit tcp any eq 639 any gt 1024
70 permit ospf any any
80 permit ospf any 224.0.0.5/32
```

```
90 permit ospf any 224.0.0.6/32
ip access-list copp-system-acl-routingproto2
10 permit udp any 224.0.0.0/24 eq 1985
20 permit 112 any 224.0.0.0/24
ipv6 access-list copp-system-acl-v6routingProto2
10 permit udp any ff02::66/128 eq 2029
20 permit udp any ff02::fb/128 eq 5353
30 permit 112 any ff02::12/128
ipv6 access-list copp-system-acl-v6routingproto1
10 permit 89 any ff02::5/128
20 permit 89 any ff02::6/128
30 permit udp any ff02::9/128 eq 521
```

이 경우 BGP는 ACL cop**-system-acl-routingProto1과 일치하며**, 따라서 CoPP 클래스 BGP가 **copp-s-routingProto1이 됩니다**.

컨트롤 플레인 폴리싱 통계 및 카운터

CoPP는 QoS 통계를 지원하여 특정 클래스에 대해 모든 모듈에 대해 CIR(Committed Input Rate)을 확인하거나 위반하는 트래픽의 집계 카운터를 추적합니다.
각 클래스 맵은 해당 클래스에 따라 CPU 바인딩 트래픽을 분류하고 해당 분류에 속하는 모든 패킷에 대해 CIR을 연결합니다. 예를 들어, BGP 트래픽과 관련된 클래스**는** 참조로 사용됩니다.

Nexus 9000 TOR(top-of-rack)에서 **cop-system-p-class-critical**:

```
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

class-map의 섹션에서 match 문 뒤에 클래스 내의 모든 트래픽과 관련된 작업이 표시됩니다. cop**-system-p-class-critical** 내에서 분류된 모든 트래픽은 우선 순위가 가장 높은 CoS(Class of Service)가 7로 설정되며 이 클래스는 CIR이 36000kbps이고 커밋된 버스트 속도가 1280000바이트입니다. 이 정책을 따르는 트래픽은 SUP로 전달되어 처리되고 모든 위반이 삭제됩니다.

```
set cos 7
police cir 36000 kbps , bc 1280000 bytes
```

다음 섹션에서는 TOR(Top-of-Rack) 스위치에 대한 모듈과 관련된 통계를 제공하며, 모듈 1은 스위

치를 나타냅니다.

```
module 1 :
transmitted 177446058 bytes;
5-minute offered rate 3 bytes/sec
conformed 27 peak-rate bytes/sec
at Sat Apr 23 04:25:27 2022

dropped 0 bytes;
5-min violate rate 0 byte/sec
violated 0 peak-rate byte/sec
```

출력에 표시되는 통계는 히스토리이므로 명령이 실행될 때 현재 통계의 스냅샷을 제공합니다.

다음 두 가지 섹션으로 구성됩니다. **전송** 및 **삭제된** 섹션:
전송된 데이터 포인트는 정책을 따르는 전송된 모든 패킷을 추적합니다. 이 섹션에서는 수퍼바이저가 처리하는 트래픽 유형에 대한 정보를 제공하므로 중요합니다.

5분 제공 속도 값은 현재 속도에 대한 통찰력을 제공합니다.
구성된 피크 속도 및 날짜 - 정책 내에서 계속 구성된 최고 피크 속도(초)의 스냅과 발생 시간을 제공합니다.
새 피크 시간이 표시되면 이 값과 날짜를 대체합니다.

통계의 가장 중요한 부분은 삭제된 데이터 포인트입니다. 전송된 통계와 마찬가지로, 삭제된 섹션에서도 경찰 속도 위반으로 인해 삭제된 누적 바이트를 추적합니다.
또한 지난 5분 동안의 위반 속도, 위반 피크 시간, 그리고 피크 시간이 있을 경우 해당 최대 위반 시간 기록을 제공합니다. 다시 한 번, 새로운 피크 시간이 표시되면 이 값과 날짜를 대체합니다. 다른 플랫폼에서는 출력이 다양하지만 논리는 매우 유사합니다.

Nexus 7000은 동일한 구조를 따르고 확인은 동일하지만, 일부 클래스는 참조된 ACL에 약간 차이가 있습니다.

```
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-lisp
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-rise
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-lisp6
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-rise6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-otv-as
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mpls-ldp
match access-group name copp-system-p-acl-mpls-rsvp
match access-group name copp-system-p-acl-mac-l3-isis
match access-group name copp-system-p-acl-mac-otv-isis
match access-group name copp-system-p-acl-mac-fabricpath-isis
match protocol mpls router-alert
set cos 7
police cir 36000 kbps bc 250 ms
conform action: transmit
violate action: drop
```

```
module 1:
conformed 300763871 bytes,
5-min offered rate 132 bytes/sec
peak rate 125 bytes/sec at Sun May 01 09:50:51 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 2:
conformed 4516900216 bytes,
5-min offered rate 1981 bytes/sec
peak rate 1421 bytes/sec at Fri Apr 29 15:40:40 2022
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
module 6:
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
```

Nexus 5600에서:

```
class-map copp-system-class-bgp (match-any)
match protocol bgp
police cir 9600 kbps , bc 4800000 bytes
conformed 1510660 bytes; action: transmit
violated 0 bytes;
```

속도 또는 최고점에 대한 정보를 제공하지 않지만, 변환 및 위반된 총 바이트를 제공합니다.

Nexus 3100에서 컨트롤 플레인 출력에 OutPackets 및 DropPackets가 표시됩니다.

```
class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
match access-group name copp-system-acl-v6routingproto1
police pps 1000
OutPackets 8732060
DropPackets 0
```

OutPackets는 구성된 패킷을 참조하고, DropPackets는 CIR을 위반합니다. 이 시나리오에서는 연결된 클래스에 드롭이 표시되지 않습니다.

Nexus 3500에서 출력에 HW 및 SW Matched Packets가 표시됩니다.

```
class-map copp-s-routingProto1 (match-any)
match access-group name copp-system-acl-routingproto1
police pps 900
HW Matched Packets 471425
SW Matched Packets 471425
```

HW Matched Packets(HW 매칭 패킷)는 ACL에서 HW로 매칭하는 패킷을 나타냅니다. SW와 일치하는 패킷은 경찰을 준수하는 패킷입니다. HW와 SW에서 일치하는 패킷의 차이는 위반을 의미합니다.
이 경우 값이 일치함에 따라 라우팅 프로토콜-1 클래스 패킷(BGP 포함)에서 삭제된 항목이 표시되지 않습니다.

활성 삭제 위반 확인

컨트롤 플레인 폴리싱 통계는 기록 사항이므로 활성 위반이 증가하는지 여부를 확인하는 것이 중요합니다. 이 작업을 수행하는 일반적인 방법은 두 개의 전체 출력을 비교하고 차이점을 확인하는 것입니다.
이 작업은 수동으로 수행할 수 있으며, Nexus 스위치는 출력 비교를 지원하는 'diff' 도구를 제공합니다.
전체 출력을 비교할 수 있지만, 중점은 삭제된 통계에만 적용되므로 필요하지 않습니다. 따라서 CoPP 출력은 위반에만 집중하도록 필터링할 수 있습니다.

명령은 다음과 같습니다. **show policy-map interface control plane | egrep 클래스|모듈|위반됨|삭제됨 | diff -y**

> **참고:** diff를 위해 명령을 두 번 실행해야 현재 출력과 이전 출력을 비교할 수 있습니다.

```
N9K-3# show policy-map interface control-plane | egrep class|module|violated|dropped | diff -y
    class-map copp-system-p-class-l3uc-data (match-any)              class-map copp-system-p-class-l3uc-data (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-critical (match-any)               class-map copp-system-p-class-critical (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-important (match-any)              class-map copp-system-p-class-important (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-openflow (match-any)               class-map copp-system-p-class-openflow (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-router (match-any        class-map copp-system-p-class-multicast-router (match-any
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-multicast-host (match-any)         class-map copp-system-p-class-multicast-host (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-l3mc-data (match-any)              class-map copp-system-p-class-l3mc-data (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal (match-any)                 class-map copp-system-p-class-normal (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-ndp (match-any)                    class-map copp-system-p-class-ndp (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp (match-any)            class-map copp-system-p-class-normal-dhcp (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-dhcp-relay-response         class-map copp-system-p-class-normal-dhcp-relay-response
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
        violated 0 peak-rate byte/sec                                    violated 0 peak-rate byte/sec
    class-map copp-system-p-class-normal-igmp (match-any)            class-map copp-system-p-class-normal-igmp (match-any)
      module 1 :                                                       module 1 :
        dropped 0 bytes;                                                 dropped 0 bytes;
```

이전 명령을 사용하면 두 클래스 간의 델타를 보고 위반이 증가함을 찾을 수 있습니다.

> **참고:** CoPP 통계는 히스토리이므로, 명령 실행 후 통계를 지워 활성 증가 여부를 확인하는 것이 좋습니다. CoPP 통계를 지우려면 다음 명령을 실행합니다. '**복사본 통계 지우기**'

CoPP 삭제 유형

CoPP는 CIR을 위반하는 모든 CPU 바운드 트래픽이 삭제되므로 단순한 폴리싱 구조입니다. 그럼에도 불구하고 그 영향은 드롭의 유형에 따라 크게 달라집니다. 논리는 동일하지만, **cop-system-p-class-critical**로 향하는 트래픽**을 삭제하는 것은** 동일하지 않습니다.

```
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
```

class-map copp-system-p-class-monitoring으로 향하는 트래픽을 삭제하는 것과 비교됩니다.

```
class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
```

첫 번째 항목은 대부분 라우팅 프로토콜을 다루며, 두 번째 하나는 가장 낮은 우선 순위와 CIR 중 하나인 ICMP(Internet Control Message Protocol)를 처리합니다. CIR의 차이는 100배입니다 따라서 클래스, 영향, 일반적인 확인/확인 및 권장 사항을 이해하는 것이 중요합니다.

CoPP 클래스

클래스 모니터링 - copp-system-p-class-monitoring

이 클래스는 IPv4 및 IPv6용 ICMP 및 문제의 스위치로 전달되는 트래픽의 traceroute를 포함합니다 .

```
class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
```

영향

-패킷 손실 또는 레이턴시를 해결할 때 CoPP에 의해 속도가 제한된 인밴드 포트를 통해 스위치를 ping하는 것이 일반적인 오해입니다. CoPP가 ICMP를 과도하게 제한하므로, 트래픽이 낮거나 정체 상태가 낮더라도 CIR을 위반할 경우 대역 내 인터페이스를 직접 ping할 때 패킷 손실을 볼 수 있습니다.

예를 들어, 라우팅 포트에서 직접 연결된 인터페이스를 ping하여 패킷 페이로드가 500인 경우 삭제를 주기적으로 볼 수 있습니다.

```
N9K-3# ping 192.168.1.1 count 1000 packet-size 500
...
```

```
--- 192.168.1.1 ping statistics ---
1000 packets transmitted, 995 packets received, 0.50% packet loss
round-trip min/avg/max = 0.597/0.693/2.056 ms
```

ICMP 패킷의 목적지인 Nexus에서 위반이 탐지되고 CPU가 보호되면서 CoPP에서 해당 패킷을 삭제했음을 알 수 있습니다.

```
N9K-4# show policy-map interface control-plane class copp-system-p-class-monitoring
Control Plane

Service-policy input: copp-system-p-policy-strict

class-map copp-system-p-class-monitoring (match-any)
match access-group name copp-system-p-acl-icmp
match access-group name copp-system-p-acl-icmp6
match access-group name copp-system-p-acl-traceroute
set cos 1
police cir 360 kbps , bc 128000 bytes
module 1 :
transmitted 750902 bytes;
5-minute offered rate 13606 bytes/sec
conformed 13606 peak-rate bytes/sec
at Sun May 01 22:49:24 2022

dropped 2950 bytes;
5-min violate rate 53 byte/sec
violated 53 peak-rate byte/sec at Sun May 01 22:49:24 2022
```

레이턴시 또는 패킷 손실 문제를 해결할 경우, 컨트롤 플레인 트래픽이 될 스위치 자체로 이동되지 않고 데이터 플레인을 통해 연결할 수 있는 호스트를 사용하는 것이 좋습니다. 데이터 플레인 트래픽은 SUP 개입 없이 하드웨어 레벨에서 전달/라우팅되므로 CoPP에서 폴리싱되지 않으며 일반적으로 드롭이 발생하지 않습니다.

권장 사항

- 스위치가 아닌 데이터 플레인을 통해 스위치에 ping을 전송하여 패킷 손실에 대한 오탐(false positive) 결과를 확인합니다.

-NMS(Network Monitoring System) 또는 클래스에 대해 커밋된 입력 속도를 통해 버스트를 방지하려면 스위치에 ICMP를 적극적으로 사용하는 툴 제한 CoPP는 클래스에 속하는 모든 집계 트래픽에 적용됩니다.

클래스 관리 - cop-system-p-class-management

이 클래스는 IPv4 및 IPv6 통신을 위해 통신(SSH, 텔넷), 전송(SCP, FTP, HTTP, SFTP, TFTP), 클럭(NTP), AAA(Radius/TACACS) 및 모니터링(SNMP)에 사용할 수 있는 다양한 관리 프로토콜을 포함합니다.

```
class-map copp-system-p-class-management (match-any)
match access-group name copp-system-p-acl-ftp
match access-group name copp-system-p-acl-ntp
match access-group name copp-system-p-acl-ssh
match access-group name copp-system-p-acl-http
match access-group name copp-system-p-acl-ntp6
match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
```

```
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snmp6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6
set cos 2
police cir 36000 kbps , bc 512000 bytes
```

영향

이 클래스와 관련된 가장 일반적인 동작 또는 삭제는 다음과 같습니다.

-SSH/텔넷을 통해 연결할 때 CLI 속도가 느려지는 것으로 인식됨 클래스에 활성 중단이 있는 경우 통신 세션이 느려지고 삭제로 인해 손상될 수 있습니다.
-스위치에서 FTP, SCP, SFTP, TFTP 프로토콜을 사용하여 파일을 전송합니다. 가장 일반적인 동작은 대역 내 관리 포트를 통해 시스템/킥스타트 부팅 이미지를 전송하려는 시도입니다. 따라서 클래스의 총 대역폭에 의해 결정되는 전송 세션이 닫히거나 종료되는 전송 시간이 늘어날 수 있습니다.
-NTP 동기화 문제, 이 클래스는 비인가 NTP 에이전트 또는 공격을 완화하므로 중요합니다.
-AAA Radius 및 TACACS 서비스도 이 클래스에 속합니다. 이 클래스에 영향을 미치는 것으로 인식되면 사용자 계정의 스위치에 대한 권한 부여 및 인증 서비스에 영향을 미칠 수 있으며, 이는 CLI 명령 지연에도 영향을 줄 수 있습니다.
-SNMP는 이 클래스 아래에서도 폴리싱됩니다. SNMP 클래스로 인해 삭제되는 가장 일반적인 동작은 NMS 서버에 있으며, NMS 서버에서는 워크, 대량 수집 또는 네트워크 스캔을 수행합니다. 정기적인 불안정이 발생하는 경우 일반적으로 NMS 수집 스케줄과 상관관계가 있습니다.

권장 사항

-CLI 속도가 느려지는 것으로 인식되면 콘솔 액세스 또는 관리 대역 외 액세스(mgmt0)를 사용합니다.

-시스템 이미지를 스위치에 업로드해야 하는 경우 대역 외 관리 포트(mgmt0)를 사용하거나 USB 포트를 사용하여 가장 빠른 전송을 수행하십시오.

-NTP 패킷이 손실된 경우 'show ntp peer-status'를 선택하고 연결 가능 열을 확인합니다. 드롭이 377로 변환되지 않습니다.

- AAA 서비스에 문제가 있는 경우, 로컬 전용 사용자를 사용하여 문제를 해결하고 동작이 완화될 때까지 문제 해결

-SNMP 문제의 완화에는 공격적 행동 감소, 표적 수집 또는 네트워크 스캐너의 최소화 등이 포함됩니다. 스캐너에서 CPU 수준에서 표시되는 이벤트로 주기적인 시간을 검사합니다.

클래스 L3 유니캐스트 데이터 - copp-system-p-class-l3uc-data

이 클래스는 특히 간결한 패킷을 다룹니다. 이 패킷 유형은 WHRL(Hardware Rate Limiter)에서도 처리됩니다.
수신 IP 패킷이 라인 카드로 전달될 때 다음 홉에 대한 ARP(Address Resolution Protocol) 요청이 확인되지 않으면 라인 카드는 패킷을 수퍼바이저 모듈로 전달합니다.

수퍼바이저는 다음 홉의 MAC 주소를 확인하고 하드웨어를 프로그래밍합니다.

```
class-map copp-system-p-class-l3uc-data (match-any)
match exception glean
set cos 1
```

이는 일반적으로 고정 경로가 사용되고 다음 홉이 도달 불가 또는 확인되지 않을 때 발생합니다.

ARP 요청이 전송되면 소프트웨어에서 하드웨어에 /32 드롭 인접성을 추가하여 동일한 next-hop IP 주소에 대한 패킷이 수퍼바이저에게 전달되지 않도록 합니다. ARP가 확인되면 하드웨어 항목이 올바른 MAC 주소로 업데이트됩니다. ARP 항목이 시간 제한 기간 전에 확인되지 않으면 해당 항목이 하드웨어에서 제거됩니다.

> **참고:** CoPP와 HWRL은 CPU가 보호되도록 연동합니다. 유사한 기능을 수행하는 것처럼 보이지만 HWRL이 먼저 발생합니다. 구현은 ASIC의 포워딩 엔진에 특정 기능이 구현되는 위치를 기반으로 합니다. 이 직렬 접근 방식은 모든 CPU 바인딩된 패킷을 측정하는 세분화 및 멀티레이어 보호를 허용합니다.

HWRL은 모듈의 인스턴스/포워딩 엔진별로 수행되며 'show hardware rate-limiter' 명령을 사용하여 볼 수 있습니다. HWRL은 이 기술 문서의 범위를 벗어납니다.

```
show hardware rate-limiter

Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated bytes since last clear counters


Module: 1
R-L Class Config Allowed Dropped Total
+----------------+----------+--------------------+--------------------+--------------------+
L3 glean 100 0 0 0
L3 mcast loc-grp 3000 0 0 0
access-list-log 100 0 0 0
bfd 10000 0 0 0
fex 12000 0 0 0
span 50 0 0 0
sflow 40000 0 0 0
vxlan-oam 1000 0 0 0
100M-ethports 10000 0 0 0
span-egress disabled 0 0 0
dot1x 3000 0 0 0
mpls-oam 300 0 0 0
netflow 120000 0 0 0
ucs-mgmt 12000 0 0 0
```

영향

- 데이터 플레인 트래픽은 하드웨어에서 처리할 수 없으므로 위반으로 인해 CPU에 부담을 줍니다.

권장 사항

-이 문제의 일반적인 해결 방법은 다음 홉에 도달할 수 있는지 확인하고 configuration 명령으로 조

정(glean-throttling)을 활성화하는 것입니다. '**하드웨어 ip glean throttle**'

참조: https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/Unicast-routing/cisco-nexus-9000-series-nx-os-unicast-configuration-guide-release-102x/m-n9k-configuring-ipv4-93x.html#concept_A6E56C2E174440BBA33F829C23897807

-Nexus 7000에서 8.4(2)는 M3 및 F4 모듈에 대한 인접성에 대한 블룸 필터 지원도 도입했습니다.
참조: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/unicast/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Unicast-Routing-Configuration-Guide-Release/n7k_unicast_config_ipv4.html#concept_4B4BF5FE17DE443EAAD710690FE670EB

-연결할 수 없는 next-hop 주소를 사용하는 고정 경로 구성을 검토하거나 RIB에서 이러한 경로를 동적으로 제거하는 동적 라우팅 프로토콜을 사용합니다.

Class Critical - class-map copp-system-p-class-critical

이 클래스는 IPv4 및 IPv6, (RIP, OSPF, EIGRP, BGP), auto-RP, vPC(virtual port-channel), l2pt 및 IS-IS에 대한 라우팅 프로토콜을 포함하는 L3 관점에서 가장 중요한 컨트롤 플레인 프로토콜을 참조합니다.

```
class-map copp-system-p-class-critical (match-any)
match access-group name copp-system-p-acl-bgp
match access-group name copp-system-p-acl-rip
match access-group name copp-system-p-acl-vpc
match access-group name copp-system-p-acl-bgp6
match access-group name copp-system-p-acl-ospf
match access-group name copp-system-p-acl-rip6
match access-group name copp-system-p-acl-eigrp
match access-group name copp-system-p-acl-ospf6
match access-group name copp-system-p-acl-eigrp6
match access-group name copp-system-p-acl-auto-rp
match access-group name copp-system-p-acl-mac-l2pt
match access-group name copp-system-p-acl-mac-l3-isis
set cos 7
police cir 36000 kbps , bc 1280000 bytes
```

영향

인접성 **삭제 또는** 컨버전스 장애 또는 업데이트/NLRI 전파를 포함할 수 있는 라우팅 프로토콜로 **cop-system-p-class-critical** 전송 불안정성을 삭제합니다.
이 클래스의 가장 일반적인 정책 삭제는 비정상적으로 작동하는(컨피그레이션 오류 또는 장애로 인해) 네트워크의 비정상적으로 작동하는 비인가 디바이스나 확장성과 관련될 수 있습니다.

권장 사항

-비인가 디바이스 또는 L2 불안정 등으로 인해 상위 레이어 프로토콜의 지속적인 재통합이 발생하는 이상 징후가 탐지되지 않을 경우, CoPP 또는 보다 관대한 클래스의 사용자 지정 컨피그레이션이 확장을 수용하기 위해 필요할 수 있습니다.
- 현재 존재하는 기본 프로필에서 사용자 지정 CoPP 프로필을 구성하는 방법은 CoPP 컨피그레이션 가이드를 참조하십시오.
https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/Security/cisco-

nexus-9000-nx-os-security-configuration-guide-102x/m-configuring-copp.html#task_E3D04369F59F471885BC5E8CD24337CA

클래스 중요 - cop-system-p-class-중요

이 클래스는 HSRP, VRRP 및 LLDP를 비롯한 FHRP(First-Hop Redundancy Protocol)와 관련이 있습니다.

```
class-map copp-system-p-class-important (match-any)
match access-group name copp-system-p-acl-hsrp
match access-group name copp-system-p-acl-vrrp
match access-group name copp-system-p-acl-hsrp6
match access-group name copp-system-p-acl-vrrp6
match access-group name copp-system-p-acl-mac-lldp
set cos 6
police cir 2500 kbps , bc 1280000 bytes
```

영향

여기에서 가장 일반적인 동작은 계층 2 불안정 문제, 즉 디바이스가 활성 상태(스플릿 브레인) 시나리오, 적극적인 타이머, 잘못된 컨피그레이션 또는 확장성으로 전환되는 것입니다.

권장 사항

-FHRP에 대해 그룹이 올바르게 구성되고 액티브/스탠바이 또는 기본/보조 역할이 올바르게 협상되었으며 상태에 플랩이 없는지 확인합니다.

-L2에서 컨버전스 문제 또는 L2 도메인에 대한 멀티캐스트 전파 관련 문제를 확인합니다.

클래스 L2 폴리싱되지 않음 - copp-system-p-class-l2-폴리싱되지 않음

L2 폴리싱되지 않은 클래스는 모든 상위 레이어 프로토콜의 기반인 모든 중요한 레이어 2 프로토콜을 의미하며, 따라서 가장 높은 CIR 및 우선순위로 거의 폴리싱되지 않은 것으로 간주됩니다.
이 클래스는 STP(Spanning-Tree Protocol), LACP(Link Aggregation Control Protocol), CFSoE(Cisco Fabric Service over Ethernet)를 효과적으로 처리합니다.

```
class-map copp-system-p-class-l2-unpoliced (match-any)
match access-group name copp-system-p-acl-mac-stp
match access-group name copp-system-p-acl-mac-lacp
match access-group name copp-system-p-acl-mac-cfsoe
match access-group name copp-system-p-acl-mac-sdp-srp
match access-group name copp-system-p-acl-mac-l2-tunnel
match access-group name copp-system-p-acl-mac-cdp-udld-vtp
set cos 7
police cir 50 mbps , bc 8192000 bytes
```

이 클래스는 모든 클래스 중 가장 높은 50Mbps의 경찰 CIR과 가장 높은 버스트 속도 홉수를 제공합니다.

영향

데이터, 제어 및 관리 플레인에 대한 모든 상위 레이어 프로토콜과 통신이 기본 레이어 2 안정성에 의존하므로 이 클래스의 삭제로 인해 글로벌 불안정이 발생할 수 있습니다.

STP 위반 시 TCN 및 STP 통합 문제가 발생할 수 있습니다. 여기에는 STP 분쟁, MAC 플러시, 이동 및 비활성화된 동작 학습이 포함되며, 이로 인해 연결 가능성 문제가 발생하고 네트워크를 불안정하게 하는 트래픽 루프가 발생할 수 있습니다.

이 클래스는 LACP를 참조하므로 포트 채널 채권의 상태를 유지하는 데 사용되는 모든 LACPDU를 포함하는 0x8809와 연결된 모든 이더 타입 패킷을 처리합니다. 이 클래스의 불안정성으로 인해 LACPDU가 삭제되면 포트 채널이 시간 초과될 수 있습니다.

Cisco CSFoE(Fabric Service over Ethernet)는 이 클래스에 속하며 Nexus 스위치 간에 중요한 애플리케이션 제어 상태를 전달하는 데 사용되므로 안정성을 위해 반드시 필요합니다.

CDP, UDLD 및 VTP를 포함하는 이 클래스 내의 다른 프로토콜에도 동일한 내용이 적용됩니다.

권장 사항

-가장 일반적인 동작은 L2 이더넷 불안정성과 관련이 있습니다. 네트워크에서 재컨버전스 또는 비인가 장치가 미치는 영향을 최소화하기 위해 관련 기능 개선 사항이 실행되어 STP가 결정적으로 올바르게 설계되었는지 확인합니다. L2 확장에 참여하지 않는 모든 엔드 호스트 디바이스에 대해 올바른 STP 포트 유형이 구성되어 TCN을 최소화하기 위해 에지/에지 트렁크 포트로 구성되어 있는지 확인합니다.

-BPDUguard, Loopguard, BPDUfilter, RootGuard 등의 STP 개선 사항을 사용하여 장애 범위를 제한하거나 네트워크에서 잘못된 컨피그레이션 또는 비인가 디바이스가 발생하는 문제를 적절히 제한합니다.

참조: https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/layer-2-switching/cisco-nexus-9000-nx-os-layer-2-switching-configuration-guide-102x/m-configuring-stp-extensions.html

-MAC 학습을 비활성화하고 플러시를 생성할 수 있는 MAC 이동 동작을 확인합니다. 참조: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/nx-os-software/213906-nexus-9000-mac-move-troubleshooting-and.html

클래스 멀티캐스트 라우터 - class-map copp-system-p-class-multicast-router

이 클래스는 FHR(First-Hop Router), LHR(Last-Hop Router), IHR(Intermediate-Hop Router) 및 RP(Rendezvous Points)를 포함하여 데이터 플레인 경로의 모든 PIM 지원 디바이스를 통해 라우팅된 멀티캐스트 공유 트리를 설정하고 제어하는 데 사용되는 컨트롤 플레인 PIM(Protocol Independent Multicast) 패킷을 나타냅니다. 이 클래스 내에서 분류된 패킷에는 소스에 대한 PIM 등록, IPv4 및 IPv6 모두에 대한 수신자에 대한 PIM 조인, 일반적으로 PIM(224.0.0.13)으로 향하는 모든 트래픽, MSDP(Multicast Source Discovery Protocol)가 포함됩니다. 여러 클래스에 의해 처리되는 멀티캐스트 또는 RP 기능의 매우 구체적인 부분을 처리하는 몇 가지 추가 클래스가 있습니다.

```
class-map copp-system-p-class-multicast-router (match-any)
match access-group name copp-system-p-acl-pim
match access-group name copp-system-p-acl-msdp
```

```
match access-group name copp-system-p-acl-pim6
match access-group name copp-system-p-acl-pim-reg
match access-group name copp-system-p-acl-pim6-reg
match access-group name copp-system-p-acl-pim-mdt-join
match exception mvpn
set cos 6
police cir 2600 kbps , bc 128000 bytes
```

영향

이 클래스와 관련된 삭제에 대한 주요 영향은 PIM 등록이 RP 또는 PIM 조인을 올바르게 처리하지 않아 공유 또는 최단 경로 트리를 멀티캐스트 스트림의 소스 또는 RP로 불안정하게 하는 멀티캐스트 소스와 통신하는 문제와 관련이 있습니다. 동작에는 누락된 조인으로 인해 제대로 채워지지 않은 OIL(Outgoing Interface List) 또는 환경 전체에서 일관성 있게 보이지 않는 (*, G)이 포함될 수 있습니다. 상호 연결을 위해 MSDP를 사용하는 멀티캐스트 라우팅 도메인 간에도 문제가 발생할 수 있습니다.

권장 사항

-PIM 제어 관련 문제에 대한 가장 일반적인 동작은 확장 문제 또는 비인가 동작을 나타냅니다. 가장 일반적인 동작 중 하나는 UPnP 구현으로 인해 메모리 소모 문제가 발생할 수 있습니다. 이는 필터와 로그 디바이스의 범위를 줄여 해결할 수 있습니다. 디바이스의 네트워크 역할에 따라 멀티캐스트 제어 패킷을 차단 및 필터링하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

Nexus 7K/N9K에서 멀티캐스트 필터링 구성 - Cisco

클래스 멀티캐스트 호스트 - copp-system-p-class-multicast-host

이 클래스는 MLD(Multicast Listener Discovery), 특히 MLD 쿼리, 보고서, 감소 및 MLDv2 패킷 유형을 참조합니다. MLD는 호스트가 특정 그룹에 대한 멀티캐스트 데이터를 요청하는 데 사용하는 IPv6 프로토콜입니다. MLD를 통해 얻은 정보를 통해 소프트웨어는 인터페이스별로 멀티캐스트 그룹 또는 채널 멤버십 목록을 유지 관리합니다. MLD 패킷을 수신하는 디바이스는 요청된 그룹에 대해 수신하는 멀티캐스트 데이터를 전송하거나 알려진 수신자의 네트워크 세그먼트를 전달합니다. MLDv1은 IGMPv2에서 파생되고 MLDv2는 IGMPv3에서 파생됩니다. IGMP는 IP 프로토콜 2 메시지 유형을, MLD는 ICMPv6 메시지의 하위 집합인 IP 프로토콜 58 메시지 유형을 사용합니다.

```
class-map copp-system-p-class-multicast-host (match-any)
match access-group name copp-system-p-acl-mld
set cos 1
police cir 1000 kbps , bc 128000 bytes
```

영향

이 클래스의 드롭은 링크-로컬 IPv6 멀티캐스트 통신에 대한 문제로 해석되며, 이로 인해 수신자의 리스너 보고서 또는 일반 쿼리에 대한 응답이 삭제될 수 있으므로 호스트가 수신할 멀티캐스트 그룹을 검색할 수 없습니다. 이는 스누핑 메커니즘에 영향을 미칠 수 있으며 트래픽을 요청한 예상 인터페이스를 통해 트래픽을 제대로 전달하지 못할 수 있습니다.

권장 사항

-MLD 트래픽은 IPv6의 링크-로컬 레벨에서 중요하므로 이 클래스에 드롭이 있는 경우 가장 일반적인 동작은 확장성, L2 불안정 또는 비인가 디바이스와 관련이 있습니다.

클래스 레이어 3 멀티캐스트 데이터 - copp-system-p-class-l3mc-data 및 클래스 레이어 3 멀티캐스트 IPv6 데이터 - copp-system-p-class-l3mcv6-data

이러한 클래스는 SUP에 대한 멀티캐스트 예외 리디렉션과 일치하는 트래픽을 참조합니다. 이 경우 이러한 클래스에서 처리하는 두 가지 조건이 있습니다. 첫 번째는 RPF(Reverse-Path Forwarding) 실패이고 두 번째는 Destination Miss입니다. Destination Miss는 Layer 3 멀티캐스트 전달 테이블에 대한 하드웨어의 조회가 실패하여 데이터 패킷이 CPU에 펀딩되는 멀티캐스트 패킷을 말합니다. 이러한 패킷은 때때로 데이터 플레인 트래픽을 기반으로 멀티캐스트 컨트롤 플레인을 트리거/설치하고 하드웨어 포워딩 테이블 항목을 추가하는 데 사용됩니다. RPF를 위반하는 데이터 플레인 멀티캐스트 패킷도 이 예외와 일치하고 위반으로 분류됩니다.

```
class-map copp-system-p-class-l3mc-data (match-any)
match exception multicast rpf-failure
match exception multicast dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes

class-map copp-system-p-class-l3mcv6-data (match-any)
match exception multicast ipv6-rpf-failure
match exception multicast ipv6-dest-miss
set cos 1
police cir 2400 kbps , bc 32000 bytes
```

영향

RPF 실패 및 대상 누락(Destination Misses)은 멀티캐스트 라우터를 통해 트래픽이 이동하는 방식과 관련된 설계 또는 컨피그레이션 문제를 나타냅니다. 대상 누락은 상태 생성에서 흔히 발생하고, 삭제는 프로그래밍 및 생성(*, G), (S, G) 실패로 이어질 수 있습니다.

권장 사항

- 기본 유니캐스트 RIB 설계를 변경하거나 RPF 장애가 발생한 경우 특정 인터페이스를 통해 트래픽을 전달하도록 고정 mroute를 추가합니다.

-https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/16450-mcastguide0.html#anc5을 참조하십시오.

클래스 IGMP - cop-system-p-class-igmp

이 클래스는 특정 그룹에 대한 멀티캐스트 데이터를 요청하는 데 사용되고, IGMP 스누핑 기능에서 레이어 2에서 관심 있는 수신자에게 트래픽을 전달하는 그룹 및 관련 발신 인터페이스 목록(OIL)을 유지 관리하는 데 사용하는 모든 버전의 IGMP 메시지를 나타냅니다. IGMP 메시지는 RFC2236(https://datatracker.ietf.org/doc/html/rfc2236)에 설명된 대로 레이어 3 경계를 통과하지 않으므로 로컬에서 중요합니다. TTL(Time to Live)은 1이어야 합니다. 이 클래스에서 처리하는 IGMP 패킷에는 모든 멤버 자격 쿼리(일반 또는 소스/그룹별)가 멤버십과 함께 포함되고 수신자가 보고서를 남겨 둡니다.

```
class-map copp-system-p-class-normal-igmp (match-any)
match access-group name copp-system-p-acl-igmp
set cos 3
police cir 3000 kbps , bc 64000 bytes
```

영향

이 클래스의 삭제는 위반으로 인해 삭제된 IGMP 메시지 유형에 따라 소스와 수신자 간의 모든 멀티캐스트 통신 수준에서 문제로 변환됩니다. 수신기의 멤버십 보고서가 손실되면 라우터는 트래픽에 관심이 있는 디바이스를 인식하지 못하므로 관련 발신 인터페이스 목록에 인터페이스/VLAN을 포함하지 않습니다. 이 디바이스가 쿼리 발생기 또는 전용 라우터인 경우 소스가 로컬 레이어 2 도메인을 초과하는 경우 관련 PIM 조인 메시지가 RP로 트리거되지 않으므로 멀티캐스트 트리 전반에 걸쳐 수신기 또는 RP까지 데이터 플레인을 설정하지 않습니다. 휴가 보고서가 손실되면 수신자는 원치 않는 트래픽을 계속 수신할 수 있습니다. 이는 쿼리 발생기로 트리거된 모든 관련 IGMP 쿼리와 도메인의 멀티캐스트 라우터 간 통신에도 영향을 줄 수 있습니다.

권장 사항

-IGMP 드롭과 관련된 가장 일반적인 동작은 L2 불안정, 타이머 문제 또는 확장성과 관련이 있습니다.

클래스 일반 - cop-system-p-class-normal

이 클래스는 표준 ARP 트래픽과 일치하는 트래픽을 나타내며, 포트 기반 네트워크 액세스 제어에 사용되는 802.1X와 연결된 트래픽도 포함합니다. 이는 ARP 요청, 무상 ARP, 리버스 ARP 패킷이 전체 레이어 2 도메인을 통해 브로드캐스트되고 전파될 때 위반이 발생하는 가장 일반적인 클래스 중 하나입니다. ARP 패킷은 IP 패킷이 아니며, 이러한 패킷에는 L3 헤더가 포함되어 있지 않으므로, L2 헤더의 범위에 대해서만 결정을 내리는 것이 중요합니다. 라우터가 SVI(Switch Virtual Interface)와 같이 해당 서브넷과 연결된 IP 인터페이스로 구성된 경우, 라우터는 하드웨어 브로드캐스트 주소로 이동하므로 SUP에 ARP 패킷을 펀딩합니다. 브로드캐스트 스톰, 레이어 2 루프(STP 또는 플랩 때문에) 또는 네트워크의 루지 디바이스로 인해 ARP 스톰이 발생할 수 있으며, 이로 인해 위반이 크게 증가할 수 있습니다.

```
class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
```

영향

이 클래스의 위반이 미치는 영향은 이벤트 기간 및 환경의 스위치 역할에 크게 좌우됩니다. 이 클래스의 삭제는 ARP 패킷이 삭제되고 있으므로 불완전한 ARP 해상도로 인해 발생하는 두 가지 주요 동작을 야기할 수 있는 SUP 엔진에서 처리되지 않음을 나타냅니다.

엔드 호스트의 관점에서 볼 때, 네트워크의 디바이스는 스위치로 주소 해결을 확인하거나 완료할 수 없습니다. 이 디바이스가 세그먼트의 기본 게이트웨이 역할을 하는 경우, 디바이스가 게이트웨이를 확인할 수 없으므로 해당 L2 이더넷 세그먼트(VLAN) 외부로 라우팅할 수 없습니다. 로컬 세그먼트의 다른 최종 호스트에 대한 ARP 확인을 완료할 수 있는 경우 디바이스는 여전히 로컬 세그먼트에서 통신할 수 있습니다.

스위치의 관점에서 스톰 및 위반이 널리 발생하면 스위치가 생성된 ARP 요청 프로세스를 완료할 수 없게 됩니다. 이러한 요청은 일반적으로 next-hop 또는 직접 연결된 서브넷 확인에 대해 생성됩니다. ARP 회신은 기본적으로 유니캐스트이지만, 스위치가 소유한 MAC로 주소가 지정되므로 여전히 ARP 패킷이므로 동일한 클래스로 분류됩니다. 이는 인접 관리자에게 호스트에 대한 항목이 없는 경우 스위치가 트래픽을 제대로 처리할 수 없으며, 계층 2 헤더 재작성의 문제가 발생할 수 있기 때문에 연결성 문제로 해석됩니다.

이러한 영향은 ARP 위반을 트리거한 기본적인 문제의 범위에 따라 달라집니다. 예를 들어 브로드

캐스트 스톰에서 호스트 및 스위치는 인접성을 해결하기 위해 ARP로 계속 이동하며, 이로 인해 네트워크에서 추가 브로드캐스트 트래픽이 발생할 수 있으며, ARP 패킷이 레이어 2인 경우 L2 루프를 중단하기 위한 TTL(Layer 3 Time to Live)이 없으므로 루프가 중단될 때까지 계속 반복되며 네트워크를 통해 기하급수적으로 증가합니다.

권장 사항

-STP, 플랩 또는 비인가 디바이스와 같이 ARP 스톰을 일으킬 수 있는 기본적인 L2 불안정을 해결합니다. 원하는 방법으로 원하는 루프를 분리하여 링크 경로를 엽니다.

-스톰 제어를 사용하여 ARP 스톰을 줄일 수도 있습니다. 스톰 제어가 활성화되지 않은 경우 인터페이스의 카운터 통계를 확인하여 인터페이스를 통과하는 총 트래픽과 관련하여 인터페이스에서 표시되는 브로드캐스트 트래픽의 비율을 확인합니다.

-스톰이 없지만 여전히 환경에서 지속적인 삭제가 보이는 경우, SUP 트래픽을 확인하여 비인가 디바이스를 식별하여, 네트워크에서 ARP 패킷을 지속적으로 전송하여 합법적인 트래픽에 영향을 미칠 수 있습니다.

-네트워크의 호스트 수와 환경에 있는 스위치의 역할에 따라 증가되는 ARP는 항목을 다시 시도, 해결 및 새로 고치도록 설계되었으므로 ARP 트래픽을 항상 볼 수 있습니다. 산발적인 삭제만 확인되면 네트워크 로드에 따라 일시적일 수 있으며 영향을 감지하지 못합니다. 그러나 비정상적인 상황에서 예상되는 것을 올바르게 식별하고 차별화하기 위해서는 네트워크를 모니터링하고 아는 것이 중요합니다.

클래스 NDP - cop-system-p-acl-ndp

이 클래스는 ICMP 메시지를 사용하여 인접 디바이스의 로컬 링크 레이어 주소를 확인하는 IPv6 인접 디바이스 검색/광고 및 라우터 요청/광고 패킷과 연결된 트래픽을 나타내며, 인접 디바이스의 연결 가능성 및 추적에 사용됩니다.

```
class-map copp-system-p-class-ndp (match-any)
match access-group name copp-system-p-acl-ndp
set cos 6
police cir 1400 kbps , bc 32000 bytes
```

영향

이 클래스의 위반은 로컬 링크의 호스트와 라우터 간의 동적 검색 또는 링크 레이어/로컬 정보를 용이하게 하는 데 사용되므로 인접 디바이스 간의 IPv6 통신을 방해할 수 있습니다. 이러한 커뮤니케이션의 중단은 연결된 로컬 링크를 통해 연결성 문제를 일으킬 수도 있습니다. IPv6 네이버 간에 통신 문제가 있는 경우 이 클래스에 삭제 항목이 없는지 확인합니다.

권장 사항

-인접 디바이스, 특히 인접 디바이스 검색 및/또는 라우터 검색과 관련된 비정상적인 ICMP 동작을 검사합니다.

-주기적인 메시지에 대한 모든 예상 타이머 및 간격 값이 환경 전체에서 일관되고, 라우터 알림 메시지(RA 메시지)와 같이 유효한지 확인합니다.

클래스 일반 DHCP - copp-system-p-class-normal-dhcp

이 클래스는 IPv4 및 IPv6에 대해 동일한 로컬 이더넷 세그먼트의 DHCP(Dynamic Host Control Protocol) 패킷으로 알려진 부트스트랩 프로토콜(BOOTP 클라이언트/서버)과 연결된 트래픽을 나타냅니다. 이는 전체 검색, 제공, 요청 및 승인(DORA) 패킷 교환을 통해 모든 부팅 클라이언트에서 시작되거나 모든 BOOTP 서버로 향하는 트래픽 통신에만 특히 관련이 있으며 DHCPv6/서버 트랜잭션을 통해 DHCPv6/서버 트랜잭션을 포함합니다. 포트 546/547

```
class-map copp-system-p-class-normal-dhcp (match-any)
match access-group name copp-system-p-acl-dhcp
match access-group name copp-system-p-acl-dhcp6
set cos 1
police cir 1300 kbps , bc 32000 bytes
```

영향

이 클래스의 위반이 발생하면 최종 호스트가 DHCP 서버에서 IP를 제대로 획득할 수 없어 자동 IP 주소(APIPA) 범위 169.254.0.0/16으로 돌아갈 수 있습니다. 이러한 위반은 디바이스가 동시에 부팅을 시도하여 클래스와 연결된 CIR을 초과하는 환경에서 발생할 수 있습니다.

권장 사항

-캡처와 함께, 호스트 및 DHCP 서버 측에서 전체 DORA 트랜잭션이 표시되는지 확인합니다. 스위치가 이 통신의 일부인 경우 CPU에 처리되거나 펀딩된 패킷을 확인하고 스위치의 통계를 확인하는 것도 중요합니다. 'show ip dhcp global statistics' 및 리디렉션: 'show system internal access-list sup-redirect stats module 1 | grep -i dhcp'.

클래스 일반 DHCP 릴레이 응답 - copp-system-p-class-normal-dhcp-relay-response

이 클래스는 IPv4 및 IPv6 모두에 대해 DHCP 릴레이 기능과 연결된 트래픽을 나타내며, 릴레이에 구성된 DHCP 서버로 전달됩니다. 이는 특히 모든 BOOTP 서버에서 시작되거나 전체 DORA 패킷 교환을 통해 모든 BOOTP 클라이언트로 전송되는 트래픽 통신과 관련이 있으며 UDP 포트 546/547을 통한 DHCPv6 클라이언트/서버 트랜잭션도 포함합니다.

```
class-map copp-system-p-class-normal-dhcp-relay-response (match-any)
match access-group name copp-system-p-acl-dhcp-relay-response
match access-group name copp-system-p-acl-dhcp6-relay-response
set cos 1
police cir 1500 kbps , bc 64000 bytes
```

영향

이 클래스에 대한 위반은 클래스 copp-system-p-class-normal-dhcp 위반과 동일한 영향을 줍니다. 둘 다 동일한 트랜잭션의 일부이기 때문입니다. 이 클래스는 주로 릴레이 에이전트 서버의 응답 통신에 중점을 둡니다. Nexus는 DHCP 서버 역할을 하지 않으며 릴레이 에이전트 역할만 하도록 설계되었습니다.

권장 사항

클래스 일반 DHCP와 동일한 권장 사항이 여기에 적용됩니다. Nexus의 기능은 릴레이 에이전트 역할만 수행하므로 SUP에서는 호스트와 스위치 간의 전체 트랜잭션이 릴레이 역할을 수행하며 스위치와 서버가 구성되기를 기대합니다.

네트워크에서 실행 중인 예기치 않은 DHCP 서버가 범위에 응답할 수 있는지 또는 DHCP Discover

패킷으로 네트워크를 플러딩하는 루프에 걸린 장치와 같은 비인가 디바이스가 없는지 확인합니다. 다음 명령에서 추가 검사를 수행할 수 있습니다. **'show ip dhcp relay'** 및 **'show ip dhcp relay statistics'**

클래스 NAT 흐름 - copp-system-p-class-nat-flow

이 클래스는 소프트웨어 스위치 NAT 흐름 트래픽을 참조합니다. 새 동적 변환을 생성할 때 번역이 하드웨어에서 프로그래밍될 때까지 플로우가 소프트웨어 포워드되고, CoPP가 이를 폴리싱하여 항목이 하드웨어에 설치되는 동안 수퍼바이저에게 펀딩된 트래픽을 제한합니다.

```
class-map copp-system-p-class-nat-flow (match-any)
match exception nat-flow
set cos 7
police cir 800 kbps , bc 64000 bytes
```

영향

이 클래스의 삭제는 일반적으로 하드웨어에 새로운 동적 변환 및 플로우의 비율이 높은 경우에 발생합니다. 이러한 영향은 폐기되고 최종 호스트에 전달되지 않는 소프트웨어 스위치드 패킷과 관련이 있으며, 이로 인해 손실과 재전송이 발생할 수 있습니다. 항목이 하드웨어에 설치되면 수퍼바이저에게 더 이상의 트래픽이 펀딩되지 않습니다.

권장 사항

- 관련 플랫폼에서 동적 NAT의 지침 및 제한을 확인합니다. 3548과 같이 플랫폼에 문서화된 알려진 제한 사항이 있으며, 이 경우 변환에 몇 초가 걸릴 수 있습니다. 참조: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/93x/interfaces/configuration/guide/b-cisco-nexus-3500-nx-os-interfaces-configuration-guide-93x/b-cisco-nexus-3500-nx-os-interfaces-configuration-guide-93x_chapter_0110.html#id_35947

클래스 예외 - copp-system-p-class-exception

이 클래스는 IP 옵션 및 IP ICMP 도달 불가 패킷과 관련된 예외 패킷을 참조합니다. 목적지 주소가 FIB(Forwarding Information Base)에 없는 경우 SUP는 ICMP 도달 불가 패킷을 다시 발신자에게 전송합니다. IP 옵션이 활성화된 패킷도 이 클래스에 속합니다. IP 옵션에 대한 자세한 내용은 IANA 문서를 참조하십시오. https://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml#ip-parameters-1

```
 class-map copp-system-p-class-exception (match-any)
match exception ip option
match exception ip icmp unreachable
match exception ipv6 option
match exception ipv6 icmp unreachable
set cos 1
police cir 150 kbps , bc 32000 bytes
```

영향

이 클래스는 폴리싱에 중점을 두고 있으며, 이 클래스의 삭제는 오류를 나타내는 것이 아니라 ICMP 연결 불가 및 IP 옵션 패킷의 범위를 제한하는 보호 메커니즘입니다.

권장 사항

-FIB에 없는 대상에 대해 CPU에 표시되거나 펀딩된 트래픽이 있는지 확인합니다.

클래스 리디렉션 - copp-system-p-class-redirect

이 클래스는 시간 동기화에 사용되는 PTP(Precision Time Protocol)와 연결된 트래픽을 참조합니다. 여기에는 예약된 범위 224.0.1.129/32에 대한 멀티캐스트 트래픽, UDP 포트 319/320 및 Etype 0X88F7에 대한 유니캐스트 트래픽이 포함됩니다.

```
class-map copp-system-p-class-redirect (match-any)
match access-group name copp-system-p-acl-ptp
match access-group name copp-system-p-acl-ptp-l2
match access-group name copp-system-p-acl-ptp-uc
set cos 1
police cir 280 kbps , bc 32000 bytes
```

영향

이 클래스의 삭제는 올바르게 동기화되지 않았거나 올바른 계층 구조를 설정하지 않은 장치에서 문제가 발생할 수 있습니다.

권장 사항

- 클럭의 안정성을 확보하고 정확하게 구성되었는지 확인합니다. PTP 디바이스가 멀티캐스트 또는 유니캐스트 PTP 모드에 대해 구성되었는지 확인합니다. 그러나 둘 다 동시에 구성되지는 않습니다. 이 내용은 지침 및 제한 사항에 따라 문서화되며, 커밋된 입력 속도 이상으로 트래픽을 푸시할 수 있습니다.

- 환경의 경계 클럭 및 모든 PTP 디바이스의 설계 및 컨피그레이션을 검토합니다. 모든 지침과 제한 사항은 플랫폼마다 다르므로 따라야 합니다.

클래스 OpenFlow - copp-system-p-class-openflow

이 클래스는 OpenFlow 에이전트 작업과 연결된 트래픽 및 컨트롤러와 에이전트 간의 해당 TCP 연결을 나타냅니다.

```
class-map copp-system-p-class-openflow (match-any)
match access-group name copp-system-p-acl-openflow
set cos 5
police cir 1000 kbps , bc 32000 bytes
```

영향

이 클래스의 삭제로 인해 컨트롤러의 명령을 제대로 수신하지 못하고 처리하여 네트워크의 전달 평면을 관리하는 상담원에 문제가 발생할 수 있습니다

권장 사항

-네트워크에서 중복 트래픽이 발생하지 않도록 하거나 컨트롤러와 에이전트 간의 통신을 방해하는 디바이스가 없는지 확인합니다.

-L2 네트워크에 불안정(STP, 루프)이 없는지 확인합니다.

CoPP 삭제 문제 해결

CoPP 위반 문제를 해결하기 위한 첫 번째 단계는 다음과 같습니다.

- 문제의 영향 및 범위

- 환경을 통한 트래픽 흐름과 영향을 받는 통신에서 스위치의 역할 이해

- 관련 클래스에 위반이 있는지 확인하고 필요한 경우 반복합니다.

예를 들어 나열된 동작이 탐지되었습니다.

-디바이스가 네트워크 외부의 다른 디바이스와 통신할 수 없지만 로컬로 통신할 수 있습니다.

-VLAN 외부의 라우팅된 통신으로 영향을 격리했으며, 스위치가 기본 게이트웨이 역할을 합니다.

-호스트를 확인하면 해당 ARP 테이블을 확인한 후에도 게이트웨이에 대한 항목이 Incomplete(미완료)로 유지된다는 의미입니다.

-게이트웨이를 해결하는 다른 모든 호스트에는 통신 문제가 없습니다. 게이트웨이로 작동하는 스위치의 CoPP 확인은 copp-system-p-class-normal에 위반이 있음을 나타냅니다.

```
class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match protocol arp
set cos 1
police cir 1400 kbps , bc 32000 bytes
module 1 :
transmitted 3292445628 bytes;
dropped 522023852 bytes;
```

-또한 여러 명령 검사가 수행되면서 드롭이 활발하게 증가하고 있음을 보여줍니다.

-이러한 위반은 합법적인 ARP 트래픽을 삭제하여 서비스 거부 동작으로 이어질 수 있습니다.

참고: CoPP는 특정 클래스와 연결된 트래픽에 미치는 영향을 격리하는 것이 중요합니다. 이 예에서는 ARP 및 cop-system-p-class-normal입니다. OSPF와 같은 다른 클래스와 관련된 트래픽은 완전히 다른 클래스에 속하므로 CoPP에서 BGP를 삭제하지 않습니다. 선택하지 않은 상태로 두면 ARP 문제가 다른 문제로 연속될 수 있으며, 이는 ARP에 의존하는 프로토콜에 영향을 미칠 수 있습니다. 예를 들어 ARP 캐시가 시간 초과되어 과도한 위반 때문에 새로 고쳐지지 않을 경우 BGP와 같은 TCP 세션이 종료할 수 있습니다.

-제어 평면 검사는 Ethanalyzer, CPU-mac in-band stats, CPU 프로세스 등 문제를 더욱 격리하는 것이 좋습니다.

Ethanalyzer

CoPP에서 폴리싱한 트래픽은 CPU 바인딩된 트래픽에만 연결되므로 가장 중요한 툴 중 하나는 Ethanalyzer입니다. 이 툴은 TShark의 Nexus 구현이며, 수퍼바이저가 보내고 받은 트래픽을 캡처하고 디코딩할 수 있도록 합니다. 또한 프로토콜 또는 헤더 정보와 같은 다른 기준을 기반으로 하는 필터를 사용할 수 있으므로 CPU에서 보내고 받는 트래픽을 결정하는 데 매우 유용한 도구가 될 수

있습니다.

먼저 Ethanalyzer 툴이 터미널 세션에서 직접 실행되거나 분석을 위해 파일로 전송될 때 수퍼바이저가 확인한 ARP 트래픽을 검토하는 것이 좋습니다. 특정 패턴 또는 동작에 캡처를 집중하도록 필터 및 제한을 정의할 수 있습니다. 이렇게 하려면 유연한 디스플레이 필터를 추가합니다.

일반적으로 잘못된 것은 Ethanalyzer가 스위치를 통해 이동하는 모든 트래픽을 캡처한다는 것입니다. 호스트 간 데이터 플레인 트래픽은 데이터 포트 간 하드웨어 ASIC에 의해 스위칭되거나 라우팅되므로 CPU가 개입할 필요가 없으므로 일반적으로 Ethanalyzer 캡처에서 인식되지 않습니다. 데이터 플레인 트래픽을 캡처하려면 ELAM 또는 SPAN과 같은 다른 툴을 사용하는 것이 좋습니다. 예를 들어, ARP를 필터링하려면 다음 명령을 사용합니다.

etanalyzer 로컬 인터페이스 inband display-filter arp limit-captured-frames 0 autostop duration 60 > arpcpu

구성 가능한 중요 필드:

-'interface inband' - SUP로 전달되는 트래픽을 나타냅니다.

-'display-filter arp' - 적용된 Shark 필터를 참조하고, 대부분의 Wireshark 필터를 수락합니다.

-'limit-captured-frames 0' - 제한을 참조하고, 0은 다른 매개 변수에 의해 중지되거나 수동으로 중지될 때까지 무제한에 해당합니다.

-'autostop duration 60' - 60초 후 ethanalyzer 중지를 의미하므로 CPU에서 표시되는 ARP 트래픽의 60초 스냅샷을 생성합니다.

Ethanalyzer 출력은 '> arpcpu'를 사용하여 bootflash의 파일로 리디렉션되어 수동으로 처리됩니다. 60초 후 캡처가 완료되고 Ethanalyzer가 동적으로 종료되고, 파일 arpcpu가 스위치의 부트플래시에 있으며, 이를 처리하여 상위 Talkers를 추출할 수 있습니다. 예를 들면 다음과 같습니다.

```
show file bootflash:arpcpu | sort -k 3,5 | uniq -f 2 -c | sort -r -n | head lines 50

669 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:47 -> ff:ff:ff:ff:ff:ff ARP Who has 10.1.1.1? Tell
10.1.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:43 -> ff:ff:ff:ff:ff:ff ARP Who has 10.2.1.1? Tell
10.2.1.2
668 2022-05-10 10:29:50.901295 28:ac:9e:ad:5e:41 -> ff:ff:ff:ff:ff:ff ARP Who has 10.3.1.1? Tell
10.3.1.2
```

이 필터는 다음을 기준으로 정렬됩니다. 소스 및 대상 열, 찾은 고유 일치(날짜 열은 무시함), 인스턴스 수를 계산하고 표시되는 번호를 추가하고, 마지막으로 카운트를 기준으로 맨위에서 맨아래로 정렬하고 처음 50개의 결과를 표시합니다.

이 실습 예에서는 60초 만에 세 개의 디바이스에서 600개 이상의 ARP 패킷을 수신했으며, 이는 의심되는 공격자 디바이스로 식별되었습니다. 필터의 첫 번째 열에는 지정된 기간 동안 캡처 파일에서 이 이벤트에 대한 인스턴스 수가 확인되었음을 자세히 설명합니다.

기본적으로 ASIC에 대한 통신인 인밴드 드라이버에서 작동하는 에thanalyzer 툴을 이해하는 것이 중요합니다. 이론적으로, 패킷은 커널과 패킷 관리자를 통과하여 관련 프로세스 자체에 전달해야 합니다. CoPP와 HWRL은 트래픽이 Ethanalyzer에 표시되기 전에 작동합니다. 위반이 증가함에 능동적으로 발생하더라도, 일부 트래픽은 여전히 통과하며 경찰 속도 내에서 이루어지므로 CPU로 푸시되는 트래픽 흐름을 파악할 수 있습니다. 이는 중요한 차이점입니다. Ethanalyzer에 표시된 트래픽은 CIR을 위반하고 삭제된 트래픽이 아닙니다.

또한 모든 관련 SUP 트래픽을 catch하기 위해 지정된 표시 필터 또는 캡처 필터 없이 개방형 방식으로 Ethanalyzer를 사용할 수 있습니다. 이는 문제 해결 접근 방식의 일환으로 격리 조치로 사용할 수 있습니다.

Ethanalyzer에 대한 자세한 내용 및 사용 방법은 TechNote:

https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/116136-trouble-ethanalyzer-nexus7000-00.html

https://community.cisco.com/t5/networking-documents/using-ethanalyzer-on-nexus-platform-for-control-plane-and-data/ta-p/3142665

참고: 8.X 코드 릴리스 이전의 Nexus 7000은 모든 VDC의 SUP 바인딩 트래픽을 포함하는 관리 VDC를 통해서만 윤리분석기 캡처를 수행할 수 있습니다. VDC별 Ethanalyzer는 8.X 코드에 있습니다.

CPU-MAC 대역 내 통계

CPU 바인딩 트래픽과 연결된 인밴드 통계는 인밴드 TX/RX CPU 트래픽의 관련 통계를 유지합니다. 다음 명령을 사용하여 이러한 통계를 확인할 수 있습니다. **'show hardware internal cpu-mac inband stats'**. 현재 속도 및 피크 속도 통계를 확인할 수 있습니다.

```
show hardware internal cpu-mac inband stats`
================ Packet Statistics =======================
Packets received: 363598837
Bytes received: 74156192058
Packets sent: 389466025
Bytes sent: 42501379591
Rx packet rate (current/peak): 35095 / 47577 pps
Peak rx rate time: 2022-05-10 12:56:18
Tx packet rate (current/peak): 949 / 2106 pps
Peak tx rate time: 2022-05-10 12:57:00
```

모범 사례로서, 스위치의 역할과 'show hardware internal cpu-mac inband stats'의 인프라 출력에 따라 크게 다르므로 베이스라인을 생성하고 추적하는 것이 좋습니다. 이 랩 환경에서 일반적인 값과 기록 최고점은 일반적으로 몇 백 pps보다 크지 않으므로 비정상적인 것입니다. **'show hardware internal cpu-mac inband events'** 명령은 피크 사용 및 탐지된 시간과 관련된 데이터를 포함하므로 기록 참조로도 유용합니다.

프로세스 CPU

Nexus 스위치는 Linux 기반 시스템이며, Nexus 운영 체제(NXOS)는 CPU 선점형 스케줄러, 멀티태스킹 및 각 코어 아키텍처의 멀티스레딩을 활용하여 모든 프로세스에 대한 공정한 액세스를 제공하므로, 스파이크가 항상 문제를 나타내지 않습니다. 그러나 지속적인 트래픽 위반이 확인되면 관련 프로세스도 많이 사용되며 CPU 출력 아래에 최상위 리소스로 나타날 수 있습니다. CPU 프로세스의 여러 스냅샷을 생성하여 다음을 사용하여 특정 프로세스의 높은 사용을 확인합니다. **프로세스 cpu 정렬 표시 | 0.0 제외** 또는 **show processes cpu 정렬 | grep <process>**.

프로세스 CPU, 대역 내 통계 및 Ethanalyzer 확인은 수퍼바이저가 현재 처리하는 프로세스 및 트래픽에 대한 통찰력을 제공하고 데이터 플레인 문제에 연속적으로 영향을 미칠 수 있는 컨트롤 플레인 트래픽에서 지속적으로 불안정성을 격리하는 데 도움이 됩니다. CoPP가 보호 메커니즘임을 이해하는 것이 중요합니다. 이것은 SUP에 부과되는 트래픽에만 적용되기 때문에 반동적입니다. 이는 예상 범위를 초과하는 트래픽 속도를 폐기하여 수퍼바이저의 무결성을 보호하도록 설계되었습니다

. 인프라 및 네트워크 설계를 기반으로 특정 CoPP 클래스 및 검증된 영향과 관련된 모든 삭제에 문제가 있거나 개입이 필요한 것은 아닙니다. 프로토콜에는 keepalive 및 일시적인 이벤트를 처리할 수 있는 재시도와 같은 내장 메커니즘이 있으므로, 산발적인 버스트 이벤트로 인한 삭제는 영향을 미치지 않습니다. 설정된 기준 범위를 벗어난 지속적인 이벤트 또는 비정상적인 이벤트에 집중합니다. CoPP는 환경 고유의 프로토콜 및 기능을 준수해야 하며, 발전하는 확장성 요구 사항에 따라 이를 세부적으로 조정하기 위해 모니터링 및 지속적으로 반복되어야 합니다. 드롭이 발생하는 경우 CoPP에서 의도치 않게 또는 오작동 또는 공격에 대한 응답으로 트래픽을 삭제했는지 확인합니다. 어떤 경우든 상황을 분석하고 스위치 자체의 범위를 벗어날 수 있는 환경에 대한 영향 및 시정 조치를 분석하여 간섭할 필요성을 평가합니다.

추가 정보

최신 플랫폼/코드에서는 포트의 미러와 데이터 플레인 트래픽을 CPU로 푸미하여 SPAN-to-CPU를 수행할 수 있습니다. 이는 일반적으로 하드웨어 속도 제한 및 CoPP에 의해 크게 제한됩니다. CPU에 SPAN을 신중하게 사용하는 것이 좋습니다. 이 문서의 범위를 벗어납니다. 이 기능에 대한 자세한 내용은 나열된 기술 노트를 참조하십시오.

https://www.cisco.com/c/en/us/support/docs/switches/nexus-9000-series-switches/215329-nexus-9000-cloud-scale-asic-nx-os-span-t.html