CoP op Nexus 7000 Series-switches

Inhoud

Inleiding

Dit document beschrijft wat, hoe en waarom de Control Plane Policing (CoPP) wordt gebruikt op de Nexus 7000 Series-switches, die de F1, F2, M1 en M2 Series modules en lijnkaarten (LC's) bevatten. Het omvat ook beleid inzake goede praktijken en de manier waarop een CoPP-beleid kan worden aangepast.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over Nexus-besturingssysteem CLI.

Gebruikte componenten

De informatie in dit document is gebaseerd op de Nexus 7000 Series-switches met supervisor 1-module.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

CoP op de Nexus 7000 Series-switch - Overzicht

De CoPP is van cruciaal belang voor de netwerkwerking. Een Denial of Service (DoS)-aanval op het besturings-/Management-vliegtuig, dat onopzettelijk of verkeerd kan worden uitgevoerd, houdt doorgaans een hoog aantal verkeer in dat wordt resulteren in een excessief CPU-gebruik. De module van de supervisor besteedt een gecoördineerde hoeveelheid tijd aan het behandelen van de pakketten.

Voorbeelden van dergelijke aanvallen zijn:

- Internet Control Message Protocol (ICMP)-echo-verzoeken.
- Pakketten verzonden met **ip-opties** ingesteld.

Dit kan leiden tot:

- Verliezen van Houd-in-leven berichten en het routingprotocol updates.
- Het invullen van pakketrijen, wat in willekeurige druppels resulteert.
- Langzame of niet-reagerende interactieve sessies.

De aanvallen kunnen de netwerkstabiliteit en beschikbaarheid overweldigen en tot zaken-beïnvloedende netwerktekorten leiden.

CoPP is een op hardware gebaseerde optie die de supervisor tegen DoS-aanvallen beschermt. Het controleert de snelheid waarmee de pakketten de supervisor mogen bereiken. De CoPP-functie is gemodelleerd als een input-QoS-beleid dat gekoppeld is aan de speciale interface genaamd het **besturingsplane**. CoPP is echter een beveiligingsfunctie en maakt geen deel uit van QoS. Ter bescherming van de supervisor scheidt de CoPP-applicatie gegevenspakketten van de besturingsplane-pakketten (Exception Logic). Het identificeert Dos aanval pakketten van geldige pakketten (Classificatie). CoPP staat classificatie van deze pakketten toe:

- Ontvang pakketten
- Multicastpakketten
- Uitzonderingspakketten
- Packet omleiden
- Broadcast MAC + niet-IP-pakketten
- Broadcast MAC + IP-pakketten (zie Cisco Bug ID CSCub47533 - Packets in L2 VLAN (nr. SVI) met CoPP)
- Mcast MAC + IP-pakketten
- Router MAC + niet-IP-pakketten
- ARP-pakketten

Nadat een pakket is geclassificeerd, kan het pakket ook worden gemarkeerd en gebruikt om verschillende prioriteiten toe te wijzen, gebaseerd op het type pakketten. Bevestig, overschrijd en violeer acties (verzenden, neerzetten, mark-down) kunnen worden ingesteld. Als geen politieagent aan een klasse is verbonden, dan wordt een standaard politieman toegevoegd wiens conforme actie is neergezet. Glein-pakketten worden gecontroleerd met een standaardklasse. Eén frequentie, twee kleur en twee snelheden, drie kleurtoezicht worden ondersteund.

Het verkeer dat de CPU op de Supervisor module bereikt, kan door vier paden worden ingevoerd:

1. Inband interfaces (voorpaneelpoort) voor verkeer verzonden door lijnkaarten.

2. Management Interface (GMT0) gebruikt voor beheerverkeer.

3. Control- en Monitoring Processor (CMP)-interface die voor de console wordt gebruikt.

4. Switched Ethernet Out Band Channel (EOBC) om de lijnkaarten van de Supervisor module te besturen en statusberichten uit te wisselen.

Alleen het verkeer dat via de Inband-interface wordt verstuurd, is aan CoPP onderhevig, omdat dit het enige verkeer is dat de Supervisor-module bereikt via de verzendingsmotoren (FE's) op de lijnkaarten. De Nexus 7000 Series Switch-implementatie van CoPP is alleen op hardware gebaseerd, wat betekent dat CoPP niet in software wordt uitgevoerd door de Supervisor module. CoPP-functionaliteit (toezicht) wordt op elke FE afzonderlijk geïmplementeerd. Wanneer de verschillende tarieven voor de CoPP-beleidskaart zijn ingesteld, moet rekening worden gehouden met het aantal lijnkaarten in het systeem.

Het totale door de supervisor ontvangen verkeer is N maal X, waarbij N het aantal FE's op het Nexus 7000-systeem is, en X het voor de specifieke klasse toegestane tarief. De ingestelde poliswaarden gelden per FE-basis, en het geaggregeerde verkeer dat de CPU dreigt te treffen, is de som van het in beslag genomen en verzonden verkeer op alle FE's. Met andere woorden: verkeer dat de CPU bereikt, is gelijk aan de geconfigureerd conforme snelheid, vermenigvuldigd met het aantal FE's.

- N7K-M148GT-11/L LC heeft 1 FE
- N7K-M148GT-11/L LC heeft 1 FE
- N7K-M132XP-12/L LC heeft 1 FE
- N7K-M108X2-12L LC heeft 2 FE
- N7K-F248XP-15 LC heeft 12 FE (SOC)
- N7K-M235XP-23L LC heeft 2 FE
- N7K-M206FQ-23L LC heeft 2 FE
- N7K-M202CF-23L LC heeft 2 FE

CoPP-configuratie wordt alleen geïmplementeerd in de standaard virtuele apparaatcontext (VDC); het CoPP-beleid geldt echter voor alle VDC's. Hetzelfde algemene beleid wordt toegepast op alle lijnkaarten. CoPP past het delen van middelen tussen VDC's toe indien havens van dezelfde FE's tot verschillende VDC's behoren (M1 Series of M2 Series LC). Havens van één FE, zelfs in verschillende VDC's, tellen bijvoorbeeld mee tegen dezelfde drempel voor CoPP.

Als dezelfde FE wordt gedeeld tussen verschillende VDC's en een bepaalde klasse van controlevliegtuigverkeer de drempel overschrijdt, heeft dit gevolgen voor alle VDC's op dezelfde FE. Aanbevolen wordt één FE per VDC te oormerken om CoPP-handhaving indien mogelijk te isoleren.

Als de schakelaar voor het eerst opkomt, moet het standaardbeleid worden geprogrammeerd om het **controlevlak** te beschermen. CoPP biedt het standaardbeleid, dat op **besturingsplane** wordt toegepast als onderdeel van de eerste opstartvolgorde.

Waarom CoP op de Nexus 7000 Series-switch

De Nexus 7000 Series-switch wordt ingezet als een aggregatie- of kernschakelaar. Daarom is het het oor en de hersenen van het netwerk. Hiermee kan de maximale lading in het netwerk worden verwerkt. Het moet veelvuldige en barstende verzoeken behandelen. Enkele verzoeken zijn:

- **Spanning Tree Protocol Data Unit (BPDU)-verwerking** - de standaardinstelling is elke twee seconden.
- **First Hopredundantie** - Dit omvat Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP) en Gateway taakverdeling Protocol (GLBP) - Standaard is elke drie seconden.
- **adresresolutie** - Dit omvat protocol voor adresoplossing/buurtontdekking (ARP/ND), doorsturen van informatie Base (FIB) Glean - Tot één verzoek per seconde, per host, zoals netwerkinterfacecontroller (NIC)-team.
- **Dynamic Host Control Protocol (DHCP)** - DHCP-aanvraag, Relay - Tot één verzoek per seconde, per host.
- **Routing Protocols** voor Layer 3 (L3).
- **Data Center Interconnect** - Overlay Transport Virtualization (OTV), Multiprotocol Label Switching (MPLS) en Virtual Private LAN Service (VPLS).

CoPP is essentieel om de CPU te beschermen tegen foutieve servers of potentiële DoS-aanvallen, waardoor de CPU over voldoende programma's beschikt om kritische besturingssysteemmeldingen te verwerken.

Control Plane Processing op de Nexus 7000 Series switch

De Nexus 7000 Series-switch heeft een gedistribueerde regelafstand. Het heeft een multi-core op elke I/O module, evenals een multi-core voor het schakelbesturingsplane op de Supervisor module. Hiermee worden intensieve taken geofferd aan de I/O module CPU voor toegangscontrolelijsten (ACL's) en FIB-programmering. Het schaalt de capaciteit van het controlevlak met het aantal lijnkaarten. Dit vermijdt het knelpunt van supervisor CPU, dat in een gecentraliseerde benadering wordt gezien. Beperkers van hardwaresnelheden en op hardware gebaseerde CoPP beschermen het besturingsplane tegen slechte of kwaadaardige activiteit.

CoP-beleid voor beste praktijken

CoP Best Practices Policy (BPP) is geïntroduceerd in Cisco NX-OS release 5.2. De

opdrachtoutput van show-run geeft de inhoud van de CoPP BPP niet weer. Laat alle opdracht uitvoeren om de inhoud van CoPP BPP weer te geven.

```
-----------------------------------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
```

CoPP biedt de gebruiker vier opties voor een standaardbeleid:

- strikt
- Middelmatig
- buigzaam
- Dense (geïntroduceerd in release 6.0(1))

Als geen optie is geselecteerd of als de instelling is overgeslagen, wordt strikt toezicht toegepast. Al deze opties gebruiken dezelfde class-maps en -klassen, maar de verschillende Committed Information Rate (CIR)- en Burst Count (BC)-waarden voor toezicht. In Cisco NX-OS releases eerder dan 5.2.1 werd de setup-opdracht gebruikt om de optie te wijzigen. Cisco NX-OS release 5.2.1 introduceerde een verbetering van de CoPP BPP, zodat de optie kan worden gewijzigd zonder de setup-opdracht. gebruik de opdracht copp profile.

```
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
```

Gebruik de opdracht Show copp profile <profile-type> om de standaard CoPP BPP-configuratie te bekijken. Gebruik de opdracht Show copp status om te controleren of het CoPP-beleid correct is toegepast.

```
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
```

Om het verschil tussen twee CoPP BPP's te bekijken, gebruikt u de opdracht Show copp diff

profile <profile-type 1> profiel <profile-type 2>:

```
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----------------------------------------
```

Een CoP-beleid aanpassen

Gebruikers kunnen een aangepast CoPP-beleid maken. Schakel de standaard CoPP BPP uit en sluit deze aan op de besturingsplane-interface omdat de CoPP BPP alleen-lezen is.

```
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.
```

Met de opdracht Copyright <profile-type> <prefix> [achtervoegsel] wordt een kloon van de CoPP BPP gecreëerd. Dit wordt gebruikt om de standaardinstellingen te wijzigen. De opdracht Copp Copyright Profile is een Exec Mode opdracht. Gebruiker kan een prefix of achtervoegsel kiezen voor de toegangslijst, class-maps en beleid-map naam. Bijvoorbeeld, copp-system-p-policy-strictie wordt gewijzigd in [prefix]copp-policy-strictie[suffix]. Gekloonde configuraties worden behandeld als gebruikersconfiguraties en zijn opgenomen in de output van de show run.

```
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#
```

Het is mogelijk om verkeer te markeren dat een gespecificeerd Verboden Inlichtingspercentage (PIR) overschrijdt en schendt met deze opdrachten:

```
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)#
```

Pas het op maat gemaakte CoP-beleid toe op het mondiale **raakvlak**. Gebruik de opdracht **status** van **tooncomputer** om te controleren of het CoPP-beleid correct is toegepast.

```
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
```

Aangepaste CoP-beleidscasestudy

In dit deel wordt een reëel voorbeeld beschreven waarin de klant meerdere bewakingsapparatuur nodig heeft om de lokale interfaces veelvuldig te kunnen aanvullen. Problemen worden in dit scenario aangetroffen wanneer de klant het CoPP-beleid wil wijzigen om:

- Vergroot de CIR zodat deze specifieke adressen het lokale apparaat kunnen pingelen en het beleid niet kunnen schenden.
- Laat de andere IP-adressen de mogelijkheid behouden om het lokale apparaat te pingelen, maar bij een lagere CIR voor de probleemoplossing.

De oplossing wordt getoond in het volgende voorbeeld, dat is om een aangepast beleid met een

afzonderlijke class-map te creëren. De afzonderlijke class-map bevat de gespecificeerde IP adressen van de bewakingsapparaten en de class-map heeft een hogere CIR. Dit verlaat ook de originele class-map *controle*, die ICMP verkeer voor alle andere IP adressen bij een lagere CIR opneemt.

```
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>
```

CoP-gegevensstructuur

De CoPP BPP-gegevensstructuur is geconstrueerd als:

- **Configuratie ACL**: IP ACL en MAC ACL.
- **Classifier-configuratie**: Klasse-kaart die IP ACL of MAC overeenkomt.
- **Configuratie client**: Stel CIR, BC, conforme actie en schijn de handeling. De politie heeft twee tarieven (CIR en BC), en twee kleuren (in overeenstemming en overtreden).

```
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
```

CoP-schaalfactor

De schaalfactorconfiguratie die in Cisco NX-OS release 6.0 is geïntroduceerd, wordt gebruikt om het politietarief van het toegepaste CoPP-beleid voor een bepaalde lijnkaart te schalen. Dit verhoogt of verlaagt de rente voor een bepaalde lijnkaart, maar wijzigt het huidige CoPP - beleid niet. De veranderingen zijn onmiddellijk van kracht en het is niet nodig het CoPP-beleid opnieuw toe te passen.

```
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
```

CoP-bewaking en -beheer

Met Cisco NX-OS release 5.1 kan u een vervolgkeuzemogelijkheid per CoPP-klasse configureren

die een systeemmelding activeert als de drempelwaarde wordt overschreden. De opdracht is het **drempelwaarde voor loggen <laten vallen bytes aantal> niveau <logingniveau>**.

```
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
```

Hier is een voorbeeld van een Syslog-bericht:

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

CoP-tellers

CoPP ondersteunt dezelfde QoS statistieken als elke andere interface. Het toont de statistieken van de klassen die het dienstenbeleid vormen voor elke I/O-module die CoPP ondersteunt. Gebruik de opdracht **Beleids-kaart interface-besturingsplane** om de statistieken voor CoPP te bekijken.

> Opmerking: Alle klassen moeten worden gecontroleerd in termen van overtreden pakketten.

```
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
```

Om een geaggregeerde weergave te verkrijgen van in elkaar vormde en overtreden tellers voor alle class-map- en I/O-modules, **gebruikt** u **het** in **de**,**beleidskaart** gebruikte **besturingsplane voor de interface van de show. | i "class|conform|overtreden"** opdracht.

```
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
```

De **class copp-class-l2-default en class-default** moeten worden gemonitord om er zeker van te zijn dat er geen hoge verhogingen zijn, zelfs niet voor meegewerkte tellers. Idealiter moeten deze twee klassen een lage waarde hebben voor de conforme teller en ten minste geen geschonden tegenstijging.

ACL-tellers

De opdracht **statistieken per-ingang** wordt niet ondersteund voor IP ACL of MAC die in CoPP klasse-kaart wordt gebruikt en het heeft geen effect wanneer toegepast op CoPP IP ACL of MAC ACL. (Er is geen CLI controle uitgevoerd door de CLI Parser). Om de ACL-toetsen van CoPP MAC of IP op een I/O-module te bekijken, **gebruikt** u de opdracht **detail van** de **invoer van het systeem interne access-list**.

Hierna volgt een voorbeeld:

```
!! 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]
```

CoP Configuration Best Practices

Dit zijn aanbevelingen voor de beste praktijken voor de CoPP-configuratie:

- Gebruik standaard de CoPP-modus.
- Dense CoPP-profiel wordt aanbevolen wanneer het chassis volledig is geladen met F2 Series modules of is geladen met meer F2 Series modules dan enige andere I/O-modules.
- Het wordt niet aanbevolen om CoPP uit te schakelen. Trek de standaard CoPP indien nodig in.
- Controleer onbedoelde druppels en voeg het standaard CoPP-beleid toe of wijzig dit in overeenstemming met het verwachte verkeer.
- Op basis van het aantal FE's in het chassis kunnen de CIR- en BC-instellingen voor CoPP

worden verhoogd of verlaagd. Dit is ook gebaseerd op de rol van de apparaten op het netwerk, protocollen die lopen, enzovoort.

- Omdat verkeerspatronen in een **datacenter** voortdurend veranderen, is de aanpassing van een CoPP een constant proces.

- CoPP en VDC: Alle poorten van dezelfde FE zouden tot dezelfde VDC moeten behoren, wat makkelijk is voor een F2 Series LC, maar niet zo makkelijk voor een M2 Series of M108 LC. Dit komt doordat de verdeling van de CoPP-middelen tussen VDC's als havens van dezelfde FE tot verschillende VDC's behoren (M1-serie of M2-serie LC). De poorten van één FE, zelfs in verschillende VDC's, tellen mee tegen dezelfde drempel voor CoPP.

- De configuratie van de schaalfactor wordt aanbevolen wanneer een chassis wordt geladen met zowel F2 Series als M Series modules.

CoP Monitoring Best Practices

Dit zijn aanbevelingen voor goede praktijken voor de bewaking van CoPP:

- Configureer een syslig-berichtdrempel voor CoPP (Cisco NX-OS release 5.1) om de druppels die door CoPP worden afgedwongen te controleren.

- Er worden syslogberichten gegenereerd als de druppels binnen een verkeersklasse de door de gebruiker ingestelde drempel overschrijden.

- De logdrempel en het niveau kunnen binnen elke verkeersklasse worden aangepast met gebruik van de **logdrempelwaarde <pakkettel> niveau <niveau>**-opdracht.

- Omdat de optie "statistics per-entry" voor CoPP MAC of IP ACL niet wordt ondersteund, gebruik de opdracht **van de** det **van het systeem interne access-list** om hits van de toegangscontrole (ACE) te controleren.

- De **class copp-class-l2-default en class-default** opdracht moeten worden gemonitord om er zeker van te zijn dat er geen hoge verhogingen zijn, zelfs niet voor geconformeerde tellers.

- Alle klassen moeten worden gecontroleerd in termen van overtreden pakketten.

- Omdat **kritiek van de copp-klasse** van zeer essentieel belang is maar een **strijdig** dalingsbeleid heeft, is het een goede praktijk om de snelheid van gecodeerde pakketten te controleren om een vroege indicatie te ontvangen wanneer de klasse dichtbij het moment loopt waar de inbreuk begint. Als de aangetaste teller voor deze klasse toeneemt, betekent dit niet noodzakelijk een rode waarschuwing. Het betekent eerder dat deze situatie op korte termijn moet worden onderzocht.

- Gebruik de opdracht **copp-profiel** beperken na elke Cisco NX-OS codesupgrade, of ten minste na elke belangrijke Cisco NX-OS-codesupgrade. indien een CoPP-wijziging eerder is voltooid, moet deze opnieuw worden toegepast.

Conclusies

- CoPP is een op hardware gebaseerde optie die de supervisor tegen DoS-aanvallen beschermt.
- M1, F2 en M2 Series LCs ondersteunen CoP. F1 Series LCs ondersteunen geen CoPP.
- De CoPP-configuratie is vergelijkbaar met MQC (modulaire QoS CLI).
- CoPP configuratie en controle worden alleen uitgevoerd in een standaard VDC.
- Standaard CoPP BPP kan worden gebruikt met strikte, matige, milde en dichte opties.
- Clone CoPP BPP op aangepaste CoPP-regels om aan specifieke netwerkvereisten te voldoen.
- CoP tellers (gevormd en overtreden in bytes per class-map) worden weergegeven met de opdracht **van het** besturen **van de** interface **beleid-map**.
- Het verkeer dat door de CPU van de Supervisor-module wordt ontvangen, is gelijk aan het totale aantal FE's maal het toegestane tarief.
- Probeer gedeelde poorten van één FE over verschillende VDC's te vermijden.
- Volg de CoP-optimale werkwijzen om de functies met succes te implementeren en te controleren.

Niet-ondersteunde functies

Deze functies worden niet ondersteund:

- Gedistribueerd geaggregeerd toezicht.
- Toezicht microflow
- Toezicht op uitzonderingen.
- CoPP-ondersteuning voor BPDU die afkomstig is van een dot1q-tunnelpoort (QinQ): Cisco Discovery Protocol (CDP), DOT1x, Spanning Tree Protocol (STP) en VLAN Trunk Protocol (VTP).