CoPP nos switches Nexus 7000 Series

Contents

Introduction

Este documento descreve o que, como e por que o Control Plane Policing (CoPP) é usado nos Switches Nexus 7000 Series, que incluem os módulos F1, F2, M1 e M2 Series e as placas de linha (LCs). Ele também inclui as políticas de melhores práticas e como personalizar uma política CoPP.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento da CLI do sistema operacional Nexus.

Componentes Utilizados

As informações neste documento são baseadas nos Nexus 7000 Series Switches com Supervisor 1 Module.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Visão geral do CoPP no switch Nexus 7000 Series

O CoPP é essencial para a operação da rede. Um ataque de negação de serviço (DoS) ao plano de controle/gerenciamento, que pode ser perpetrado inadvertidamente ou mal, geralmente envolve altas taxas de tráfego que resultam em utilização excessiva da CPU. O módulo Supervisor gasta uma quantidade excessiva de tempo tratando os pacotes.

Exemplos desses ataques incluem:

- Solicitações de eco do Internet Control Message Protocol (ICMP).
- Pacotes enviados com **ip-options** definidos.

Isso pode levar a:

- Perda de mensagens de manutenção de atividade e atualizações do protocolo de roteamento.
- Enchimento de filas de pacotes, o que resulta em quedas indiscriminadas.
- Sessões interativas lentas ou sem resposta.

Os ataques podem sobrecarregar a estabilidade e a disponibilidade da rede e levar a interrupções da rede que afetam os negócios.

CoPP é um recurso baseado em hardware que protege o Supervisor contra ataques de DoS. Ele controla a taxa na qual os pacotes têm permissão para acessar o Supervisor. O recurso CoPP é modelado como uma política de QoS de entrada conectada à interface especial chamada de **plano de controle**. No entanto, o CoPP é um recurso de segurança e não faz parte da QoS. Para proteger o Supervisor, o CoPP separa os pacotes de plano de dados dos pacotes do plano de controle (Lógica de exceção). Identifica pacotes de ataque do DoS de pacotes válidos (Classificação). O CoPP permite a classificação destes pacotes:

- Pacotes de recepção
- Pacotes multicast
- Pacotes de exceção
- Redirecionar pacotes
- Broadcast MAC + pacotes não IP
- Pacotes MAC + IP de broadcast (consulte Cisco Bug ID CSCub47533 - Pacotes em L2 Vlan (sem SVI) atingindo CoPP)
- Mcast MAC + pacotes IP
- Roteador MAC + pacotes não IP
- Pacotes ARP

Depois que um pacote é classificado, ele também pode ser marcado e usado para atribuir prioridades diferentes com base no tipo de pacote. Conformar, exceder e violar ações (transmissão, queda, marcação) podem ser definidas. Se nenhum vigilante estiver anexado a uma classe, um vigilante padrão será adicionado, cuja ação de conformidade será liberada. Os pacotes Glean são policiados com classe padrão. São suportadas uma taxa, duas cores e duas taxas, três políticas de cores.

O tráfego que atinge a CPU no módulo Supervisor pode entrar por quatro caminhos:

1. Interfaces internas (porta do painel frontal) para tráfego enviado por placas de linha.

2. Management Interface (mgmt0) usada para o tráfego de gerenciamento.

3. Interface do processador de controle e monitoramento (CMP - Control and Monitoring Processor) usada para o console.

4. EOBC (Switched Ethernet Out Band Channel) para controlar as placas de linha do módulo Supervisor e trocar mensagens de status.

Somente o tráfego enviado pela interface Inband está sujeito ao CoPP, porque esse é o único tráfego que alcança o módulo Supervisor através dos FEs (Forwarding Engines, mecanismos de encaminhamento) nas placas de linha. A implementação de CoPP do switch Nexus 7000 Series é baseada somente em hardware, o que significa que o CoPP não é executado em software pelo módulo Supervisor. A funcionalidade de CoPP (policiamento) é implementada em cada FE independentemente. Quando as várias taxas são configuradas para o mapa de políticas de CoPP, deve-se considerar o número de placas de linha no sistema.

O tráfego total recebido pelo supervisor é N vezes X, em que N é o número de FEs no sistema Nexus 7000 e X é a taxa permitida para a classe específica. Os valores configurados do vigilante se aplicam por FE, e o tráfego agregado propenso a atingir a CPU é a soma do tráfego conformado e transmitido em todos os FEs. Em outras palavras, o tráfego que atinge a CPU é igual à taxa de conformidade configurada multiplicada pelo número de FEs.

- LC N7K-M148GT-11/L tem 1 FE
- LC N7K-M148GS-11/L tem 1 FE
- LC N7K-M132XP-12/L tem 1 FE
- LC N7K-M108X2-12L tem 2 FE
- LC N7K-F248XP-15 tem 12 FE (SOC)
- LC N7K-M235XP-23L tem 2 FE
- LC N7K-M206FQ-23L tem 2 FE
- LC N7K-M202CF-23L tem 2 FE

A configuração de CoPP só é implementada no contexto de dispositivo virtual padrão (VDC); no entanto, as políticas de CoPP são aplicáveis a todos os VDCs. A mesma política global é aplicada a todas as placas de linha. O CoPP aplica o compartilhamento de recursos entre VDCs se as portas dos mesmos FEs pertencerem a VDCs diferentes (M1 Series ou M2 Series LC). Por exemplo, as portas de um FE, mesmo em VDCs diferentes, contam contra o mesmo limite para CoPP.

Se o mesmo FE for compartilhado entre VDCs diferentes e uma determinada classe de tráfego de plano de controle exceder o limite, isso afetará todos os VDCs no mesmo FE. Recomenda-se dedicar um FE por VDC para isolar a aplicação de CoPP, se possível.

Quando o switch é ativado pela primeira vez, a política padrão deve ser programada para proteger o **plano de controle**. O CoPP fornece as políticas padrão, que são aplicadas ao **plano de controle** como parte da sequência inicial de inicialização.

Por que CoPP no switch Nexus 7000 Series

O switch Nexus 7000 Series é implantado como um switch central ou de agregação. Daí, é o ouvido e o cérebro da rede. Ele lida com a carga máxima na rede. Ele deve lidar com solicitações frequentes e intermitentes. Algumas das solicitações incluem:

- **Processamento de unidade de dados de protocolo de ponte de árvore de abrangência (BPDU - Spanning Tree Bridge Protocol Data Unit)** - O padrão é a cada dois segundos.
- **Redundância de primeiro salto** - Inclui o HSRP (Hot Standby Router Protocol), o VRRP (Virtual Router Redundancy Protocol) e o GLBP (Gateway Load Balancing Protocol) - O padrão é a cada três segundos.
- **Resolução de endereços** - Inclui o Address Resolution Protocol/Neighbor-Discovery (ARP/ND), Forwarding Information Base (FIB) Glean - Até uma solicitação por segundo, por host, como agrupamento de NIC (Network Interface Controller).
- **Dynamic Host Control Protocol (DHCP)** - Solicitação de DHCP, Retransmissão - Até uma solicitação por segundo, por host.
- **Protocolos de roteamento** para a camada 3 (L3).
- **Interconexão de data center** - Overlay Transport Virtualization (OTV), Multiprotocol Label Switching (MPLS) e Virtual Private LAN Service (VPLS).

O CoPP é essencial para proteger a CPU contra servidores mal configurados ou ataques de DoS potenciais, o que permite que a CPU tenha ciclo suficiente para processar mensagens críticas do plano de controle.

Processamento plano de controle no switch Nexus 7000 Series

O switch Nexus 7000 Series adota uma abordagem de plano de controle distribuído. Ele tem um multi-core em cada módulo de E/S, bem como um multi-core para o plano de controle do switch no módulo Supervisor. Descarrega tarefas intensas na CPU do módulo de E/S para listas de controle de acesso (ACL) e programação FIB. Ele dimensiona a capacidade do plano de controle com o número de placas de linha. Isso evita o gargalo da CPU do supervisor, visto em uma abordagem centralizada. Limitadores de taxa de hardware e CoPP baseado em hardware protegem o plano de controle contra atividades mal-intencionadas ou mal-intencionadas.

Política de práticas recomendadas da CoPP

A política de práticas recomendadas (BPP) da CoPP foi apresentada no Cisco NX-OS versão 5.2.

A saída do comando **show running-config** não exibe o conteúdo do CoPP BPP. O comando **show run all** exibe o conteúdo do CoPP BPP.

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

O CoPP fornece quatro opções para o usuário para as políticas padrão:

- Rígido
- Moderate
- Lenient
- Denso (apresentado na versão 6.0(1))

Se nenhuma opção for selecionada ou se a configuração for ignorada, será aplicada vigilância rigorosa. Todas essas opções usam os mesmos mapas de classe e classes, mas diferentes valores de Committed Information Rate (CIR) e Burst Count (BC) para vigilância. Nas versões do Cisco NX-OS anteriores à 5.2.1, o comando **setup** foi usado para alterar a opção. O Cisco NX-OS versão 5.2.1 introduziu uma melhoria no CoPP BPP para que a opção possa ser alterada sem o comando **setup**; use o comando **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
```

Use o comando **show copp profile <profile-type>** para exibir a configuração padrão do CoPP BPP. Use o comando **show copp status** para verificar se a política do CoPP foi aplicada corretamente.

```
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
```

Para ver a diferença entre dois CoPP BPPs, use o comando **show copp diff profile <profile-type 1> profile <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----------------------------------------
```

Como personalizar uma política de CoPP

Os usuários podem criar uma política de CoPP personalizada. Clonar o CoPP BPP padrão e anexá-lo à interface **do plano de controle** porque o CoPP BPP é somente leitura.

```
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.
```

O comando **copp copy profile <profile-type> <prefix> [suffix]** cria um clone do CoPP BPP. Isso é usado para modificar as configurações padrão. O comando **copp copy profile** é um comando **exec mode**. O usuário pode escolher um prefixo ou sufixo para a lista de acesso, os mapas de classe e o nome do mapa de política. Por exemplo, **copp-system-p-policy-strict** é alterado para **[prefix]copp-policy-strict[suffix]**. As configurações clonadas são tratadas como configurações do usuário e incluídas na saída **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#
```

Épossível marcar o tráfego que excede e viola uma Taxa de Informações Permitidas (PIR - Peritted Information Rate) especificada com estes comandos:

```
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)#
```

Aplique a política de CoPP personalizada ao plano de controle da interface global. Use o comando show copp status para verificar se a política do CoPP foi aplicada corretamente.

```
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
```

Estudo de caso de política de CoPP personalizada

Esta seção descreve um exemplo real em que o cliente exige vários dispositivos de monitoramento para fazer ping frequentemente nas interfaces locais. Dificuldades encontradas neste cenário quando o cliente deseja modificar a política de CoPP para:

- Aumente a CIR para que esses endereços específicos possam fazer ping no dispositivo local e não violar a política.
- Permita que os outros endereços IP mantenham a capacidade de fazer ping no dispositivo local, mas em uma CIR mais baixa para fins de solução de problemas.

A solução é mostrada no próximo exemplo, que é criar uma política personalizada com um mapa de classes separado. O mapa de classe separado contém os endereços IP especificados dos dispositivos de monitoramento e o mapa de classe tem uma CIR mais alta. Isso também deixa o

monitoramento do mapa de classe original, que captura o tráfego ICMP para todos os outros endereços IP em uma CIR mais baixa.

```
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>
```

Estrutura de dados do CoPP

A estrutura de dados do CoPP BPP é construída como:

- **Configuração da ACL**: ACL IP e ACL MAC.
- **Configuração do classificador**: Mapa de classe correspondente à ACL IP ou à ACL MAC.
- **Configuração do policer**: Defina CIR, BC, siga a ação e viole a ação. O vigilante tem duas taxas (CIR e BC) e duas cores (conformar-se e violar).

```
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
```

Fator de escala CoPP

A configuração de fator de escala introduzida no Cisco NX-OS Release 6.0 é usada para dimensionar a taxa de vigilância da política de CoPP aplicada para uma placa de linha específica. Isso aumenta ou reduz a taxa do vigilante para uma placa de linha específica, mas não altera a política atual de CoPP. As alterações são efetivas imediatamente e não há necessidade de reaplicar a política do CoPP.

```
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
```

Monitoramento e gerenciamento de CoPP

Com o Cisco NX-OS Release 5.1, é possível configurar um limite de queda por nome de classe CoPP que dispara uma mensagem de Syslog caso o limite seja excedido. O comando é **logging drop threshold <drop bytes count> level <logging level>**.

```
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
```

Aqui está um exemplo de uma mensagem Syslog:

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

Contadores CoPP

O CoPP suporta as mesmas estatísticas de QoS que qualquer outra interface. Ele mostra as estatísticas das classes que formam a política de serviço para cada módulo de E/S que suporta CoPP. Use o comando **show policy-map interface control-plane** para exibir as estatísticas do CoPP.

> **Note**: Todas as classes devem ser monitoradas em termos de pacotes violados.

```
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
```

Para obter uma visão agregada de contadores conformados e violados para todos os módulos de mapa de classe e E/S, use o **comando show policy-map interface control-plane | i** comando **"class|accept|violated"**.

```
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
```

A **classe copp-class-l2-default e class-default** devem ser monitoradas para garantir que não haja aumentos altos, mesmo para contadores conformados. Idealmente, essas duas classes devem ter valores baixos para contadores conformados e pelo menos nenhum aumento de contador violado.

Contadores de ACL

O comando **statistics per-entry** não é suportado para a ACL IP ou MAC usada no mapa de classe

CoPP e não tem efeito quando aplicado à ACL IP CoPP ou à ACL MAC. (Não há nenhuma verificação CLI feita pelo analisador CLI). Para visualizar os acertos da ACL MAC ou da ACL IP do CoPP em um módulo de E/S, use o comando **show system internal access-list input detail**.

Aqui está um exemplo:

```
!! 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]
```

Práticas recomendadas de configuração do CoPP

Estas são as melhores práticas recomendadas para a configuração de CoPP:

- Use o modo CoPP restrito por padrão.
- O perfil denso de CoPP é recomendado quando o chassi é totalmente carregado com módulos F2 Series ou carregado com mais módulos F2 Series do que qualquer outro módulo de E/S.
- Não é recomendado desativar o CoPP. Ajuste o CoPP padrão, conforme necessário.
- Monitore quedas não intencionais e adicione ou modifique a política CoPP padrão de acordo com o tráfego esperado.
- Com base no número de FEs no chassi, as configurações de CIR e BC para CoPP podem ser aumentadas ou reduzidas. Isso também se baseia na função dos dispositivos na rede, nos protocolos em execução e assim por diante.

- Como os padrões de tráfego mudam constantemente em um **data center**, a personalização de um CoPP é um processo constante.

- CoPP e VDC: Todas as portas do mesmo FE devem pertencer ao mesmo VDC, que é fácil para um LC F2 Series, mas não tão fácil para um LC M2 Series ou M108. Isso ocorre porque o compartilhamento de recursos do CoPP entre VDCs se as portas do mesmo FE pertencem a VDCs diferentes (LC da série M1 ou M2). As portas de um FE, mesmo em VDCs diferentes, contam contra o mesmo limite para CoPP.

- A configuração do fator de escala é recomendada quando um chassi é carregado com módulos F2 Series e M Series.

Práticas recomendadas de monitoramento de CoPP

Estas são recomendações de melhores práticas para monitoramento de CoPP:

- Configure um limite de mensagem de syslog para CoPP (Cisco NX-OS Versão 5.1) para monitorar as quedas impostas pelo CoPP.

- As mensagens de syslog serão geradas se as quedas em uma classe de tráfego excederem o limite configurado pelo usuário.

- O limite e o nível de registro podem ser personalizados em cada classe de tráfego com o uso do comando **logging drop threshold <packet-count> level <level>**.

- Como a opção "statistics per-entry" para a ACL MAC do CoPP ou ACL IP não é suportada, use o comando **show system internal access-list input det** para monitorar acessos de entrada de controle de acesso (ACE).

- Os comandos **class copp-class-l2-default e class-default** devem ser monitorados para garantir que não haja aumentos altos, mesmo para contadores conformados.

- Todas as classes devem ser monitoradas em termos de pacotes violados.

- Como **classe copp crítica** é altamente vital, mas tem uma política **de queda violada**, é uma boa prática monitorar a taxa de pacotes conformados para receber uma indicação antecipada quando a classe se torna perto do momento em que começa a violação. Se o contador violado aumentar para esta classe, não significa necessariamente um alerta vermelho. Pelo contrário, significa que esta situação tem de ser investigada a curto prazo.

- Use o comando **copp profile strict** após cada atualização de código do Cisco NX-OS ou, pelo menos, após cada atualização de código do Cisco NX-OS principal; se uma modificação de CoPP tiver sido concluída anteriormente, ela deverá ser reaplicada.

Conclusões

- CoPP é um recurso baseado em hardware que protege o Supervisor contra ataques de DoS.
- Os LCs M1, F2 e M2 Series suportam CoPP. LCs da série F1 não suportam CoPP.
- A configuração de CoPP é semelhante à MQC (Modular QoS CLI).
- A configuração e o monitoramento de CoPP são executados somente em um VDC padrão.
- O padrão de CoPP BPP pode ser usado com opções rígidas, moderadas, lenientes e densas.
- Clone CoPP BPP para regras de CoPP personalizadas para corresponder a requisitos de rede específicos.
- Os contadores de CoPP (conformados e violados em bytes por mapa de classe) são exibidos com o comando **show policy-map interface control-plane**.
- O tráfego recebido pela CPU do módulo Supervisor é igual ao número total de FEs multiplicado pela taxa permitida.
- Tente evitar portas compartilhadas de um FE em VDCs diferentes.
- Siga as práticas recomendadas de CoPP para implementar e monitorar com êxito os recursos.

Recursos não suportados

Estes recursos não são suportados:

- Política de agregação distribuída.
- Política de microfluxo.
- Política de exceção de saída.
- Suporte de CoPP para BPDU que vem de uma porta de túnel dot1q (QinQ): Cisco Discovery Protocol (CDP), DOT1x, Spanning Tree Protocol (STP) e VLAN Trunk Protocol (VTP).