CoPP em 7000 Series Switch do nexo

Índice

Introdução

Este documento descreve o que, como, e porque o Policiamento do plano de controle (CoPP) é usado nos 7000 Series Switch do nexo, que incluem o F1, F2, M1, e os módulos do M2 Series e as placas de linha (LC). Igualmente inclui políticas do melhor prática, assim como como personalizar uma política de CoPP.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do sistema operacional CLI do nexo.

Componentes Utilizados

A informação neste documento é baseada nos 7000 Series Switch do nexo com módulo do Supervisor 1.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

CoPP na vista geral do 7000 Series Switch do nexo

O CoPP é crítico à operação de rede. Um ataque de recusa de serviço (DOS) ao controle/plano de gerenciamento, que podem ser perpetrados inadvertidamente ou maliciosamente, envolve tipicamente as taxas altas do tráfego que conduzem à utilização de CPU em excesso. O módulo do supervisor gasta uma quantidade de tempo desordenado que segura os pacotes.

Os exemplos de tais ataques incluem:

- Requisições de eco do Internet Control Message Protocol (ICMP).
- Pacotes enviados com as IP-**opções** ajustadas.

Isto pode conduzir a:

- Perda de mensagens e de atualizações de protocolo de roteamento da manutenção de atividade.
- Enchimento das filas de pacote, que conduz às gotas indiscriminadas.
- Sessões interativa lentas ou sem resposta.

Os ataques podem oprimir a estabilidade de rede e a Disponibilidade e conduzi-los às paradas de rede deimpacto.

CoPP é uma característica com base em hardware que proteja o supervisor dos ataques DoS. Controla a taxa em que os pacotes são permitidos alcançar o supervisor. A característica de CoPP é modelada como uma política de QoS da entrada anexada à relação especial chamada o **controle plano**. Contudo, CoPP é uns recursos de segurança e não parte de um QoS. A fim proteger o supervisor, o CoPP separa pacotes planos dos dados dos pacotes do plano do controle (lógica da exceção). Identifica pacotes de ataque DoS dos pacotes válidos (classificação). CoPP permite a classificação destes pacotes:

- Receba pacotes
- Pacotes de transmissão múltipla
- Pacotes da exceção
- Reoriente pacotes
- Transmita MAC + pacotes não-IP
- Transmita pacotes MAC +IP (veja a identificação de bug Cisco CSCub47533 - pacotes em L2 Vlan (nenhum SVI) que bate CoPP)
- Pacotes do Mcast MAC +IP
- MAC de roteador + pacotes não-IP
- Pacotes ARP

Depois que um pacote é classificado, o pacote pode igualmente ser marcado e usado para atribuir as prioridades diferentes baseadas no tipo de pacotes. Conforme-se, exceda-se, e viole-se ações (transmita, deixe cair, Mark-para baixo) pode ser ajustado. Se nenhum vigilante é anexado a uma classe, a seguir um vigilante do padrão está adicionado cuja a conform action seja gota. Recolha pacotes são policiados com classe padrão. Uma taxa, e dois avalie, um policiamento de duas cores de três cores é apoiada.

Trafique que bate o CPU no módulo do supervisor pode entrar através de quatro trajetos:

1. Relações Inband (porta do painel dianteiro) para o tráfego enviado por placas de linha.

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

3. Relação do Control and Monitoring Processor (CMP) usada para o console.

4. Os Ethernet comutados para fora unem o canal (EOBC) para controlar as placas de linha do módulo do supervisor e para trocar mensagens de status.

Somente o tráfego enviado através da relação Inband é sujeito a CoPP, porque este é o único tráfego que alcança o módulo do supervisor através dos motores da transmissão (FE) nas placas de linha. A aplicação do 7000 Series Switch do nexo de CoPP é com base em hardware somente, assim que significa que CoPP não está executado no software pelo módulo do supervisor. A funcionalidade de CoPP (policiamento) é executada em cada FE independentemente. Quando as várias taxas são configuradas para o mapa de política de CoPP, a consideração deve ser consideração recolhida ao número de placas de linha no sistema.

O tráfego total recebido pelo supervisor é tempos N X, onde N é o número de FE no sistema do nexo 7000, e X é a taxa permitida a classe particular. Os valores configurados do vigilante aplicam-se na pela base FE, e o tráfego agregado inclinado bateu o CPU é a soma do tráfego conformado e transmitido em todos os FE. Ou seja trafique que bate o CPU iguala configurado se conforma taxa multiplicada pelo número de FE.

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

A configuração de CoPP é executada somente no contexto do dispositivo virtual do padrão (VDC); contudo, as políticas de CoPP são aplicáveis para todos os VDC. A mesma política global é aplicada para todas as placas de linha. CoPP aplica o compartilhamento de recurso entre VDC se as portas dos mesmos FE pertencem aos VDC diferentes (M1 Series ou M2 Series LC). Por exemplo, portas de um FE, mesmo em VDC diferentes, contagem contra o mesmo ponto inicial para CoPP.

Se o mesmo FE está compartilhado entre VDC diferentes e uma classe dada de tráfego plano do controle excede o ponto inicial, isto afeta todos os VDC no mesmo FE. Recomenda-se dedicar um FE pelo VDC a fim isolar a aplicação de CoPP, se possível.

Quando o interruptor vem acima da primeira vez, a política padrão deve ser programada para

proteger o **controle plano**. CoPP fornece as políticas padrão, que são aplicadas ao **controle plano** como parte da sequência de partida inicial.

Porque CoPP no 7000 Series Switch do nexo

O 7000 Series Switch do nexo é distribuído como uma agregação ou um switch central. Daqui, é a orelha e o cérebro da rede. Segura a carga máxima na rede. Deve segurar pedidos frequentes e da explosão. Alguns dos pedidos incluem:

- **Processamento do (BPDU) da unidade de dados do Spanning-Tree Bridge Protocol** - O padrão é cada dois segundos.
- **Primeira redundância de salto** - Isto inclui o Hot Standby Router Protocol (HSRP), o Virtual Router Redundancy Protocol (VRRP), e o protocolo do Balanceamento de carga do gateway (GLBP) - padrão é cada três segundos.
- **Address resolution** - Isto inclui o protocolo Protocolo de resolución de la dirección (ARP)/descoberta vizinha (ARP/ND), banco de informação de encaminhamento (FIB) recolhe - até um pedido por segundo, pelo host, tal como o equipe de Network Interface Controller (NIC).
- **Protocolo de controle dinâmico de host (DHCP)** - Requisição DHCP, relé - Até um pedido por segundo, pelo host.
- **Protocolos de roteamento** para a camada 3 (L3).
- **Interconexão do centro de dados** - Virtualização do transporte da folha de prova (OTV), Multiprotocol Label Switching (MPLS), e serviço virtual da LAN privada (VPL).

CoPP é essencial a fim proteger o CPU contra server desconfigurados ou ataques DoS do potencial, que permite que o CPU tenha bastante ciclo para processar mensagens críticas do plano do controle.

Controle o processamento plano no 7000 Series Switch do nexo

O 7000 Series Switch do nexo toma uma aproximação do plano do controle distribuído. Tem um multi-núcleo em cada módulo de E/S, assim como um multi-núcleo para o plano do controle do interruptor no módulo do supervisor. Offloads tarefas intensivas ao módulo de E/S CPU para as listas de controle de acesso (ACL) e a programação FIB. Escala a capacidade do plano do controle com o número de placas de linha. Isto evita o gargalo do Supervisor CPU, que é considerado em uma aproximação centralizada. Os limitadores da taxa do hardware e CoPP com base em hardware protegem o plano do controle do mau ou da atividade mal-intencionada.

Política dos melhores prática de CoPP

A política dos melhores prática de CoPP (BPP) foi introduzida na liberação 5.2 do Cisco NX-OS.

A saída do **comando show running-config** não indica o índice do CoPP BPP. **A mostra executa o comando all** indica o índice de 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
```

CoPP fornece quatro opções ao usuário para políticas padrão:

- Restrito
- Moderado
- Leve
- Denso (introduzido na liberação 6.0(1))

Se nenhuma opção é selecionada ou se estabelecido está saltado, a seguir o policiamento restrito é aplicado. Todas estas opções usam os mesmos mapas de classe e classes, mas a taxa de informação comprometida (CIR) e a explosão diferentes contam valores do (Bc) para policiar. No Cisco NX-OS libera-se mais cedo de 5.2.1, o **comando setup** foram usados para mudar a opção. A liberação 5.2.1 do Cisco NX-OS introduziu um realce ao CoPP BPP de modo que a opção pudesse ser mudada sem o **comando setup**; use o **comando profile do copp**.

```
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 do **<profile-type> do perfil do copp da mostra** ver a configuração de CoPP BPP do padrão. Use o **comando status do copp da mostra** verificar que a política de CoPP esteve 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
```

A fim ver a diferença entre dois CoPP BPPs, use o <profile-**tipo <profile-tipo** comando do **perfil do diff do copp da mostra do perfil 1> 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 personalizada de CoPP. Clone o padrão CoPP BPP, e anexe-o à relação do **controle plano** porque o CoPP BPP é de leitura apenas.

```
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 do **[suffix] do <prefix> do <profile-type> do perfil da cópia do copp** cria um clone do CoPP BPP. Isto é usado a fim alterar as configurações padrão. **O comando profile de cópia do copp** é um comando do **modo exec**. O usuário pode escolher um prefixo ou um sufixo para a lista de acesso, os mapas de classe, e o nome do mapa de política. Por exemplo, copp-sistema-p-política-**restrito** é mudado ao **[suffix] copp-política-restrito do [prefix]**. As configurações clonadas são tratadas como configurações do usuário e incluídas na saída da **corrida da mostra**.

```
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 abaixo do tráfego que excede e viola uma taxa de informação permitida especificada (PIR) 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 personalizada de CoPP ao **controle plano** global da relação. Use o **comando status do copp da mostra** a fim verificar que a política de CoPP esteve 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
```

Casos Práticos personalizados da política de CoPP

Esta seção descreve um exemplo real em que o cliente exige dispositivos múltiplos da monitoração a fim sibilar frequentemente as interfaces local. A dificuldade está encontrada nesta encenação quando o cliente quer alterar a política de CoPP:

- Aumente o CIR de modo que estes endereços específicos possam sibilar o dispositivo local e não violar a política.
- Permita que os outros endereços IP de Um ou Mais Servidores Cisco ICM NT mantenham a capacidade para sibilar o dispositivo local, mas em um CIR mais baixo para propósitos de Troubleshooting.

A solução é mostrada no exemplo seguinte, que é criar uma política personalizada com um mapa de classe separado. O mapa de classe separado contém os endereços IP especificados dos dispositivos da monitoração e o mapa de classe tem um CIR mais alto. Isto igualmente sae do mapa de classe original que *monitora*, que captura o tráfego ICMP para todos os outros endereços IP de Um ou Mais Servidores Cisco ICM NT em um CIR mais baixo.

```
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
```

Estrutura de dados de CoPP

A estrutura de dados de CoPP BPP é construída como:

- **Configuração ACL**: IP ACL e MAC ACL.
- **Configuração do classificador**: Mapa de classe que combina IP ACL ou MAC ACL.
- **Configuração do vigilante**: Ajuste o CIR, o BC, a conform action, e o violate action. O vigilante tem duas taxas (CIR e BC), e duas cores (se conforme e se viole).

```
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
```

Fator de Escala de CoPP

A configuração do Fator de Escala introduzida na liberação 6.0 do Cisco NX-OS é usada para escalar a taxa do vigilante da política aplicada de CoPP para uma placa de linha particular. Isto aumenta ou reduz a taxa do vigilante para uma placa de linha particular, mas não muda a política atual de CoPP. As mudanças são eficazes imediatamente, e não há nenhuma necessidade de reaplicar a política de 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
```

Monitoração e Gerenciamento de CoPP

Com Cisco NX-OS libere 5.1, ele é possível para configurar um limiar de queda pelo nome de classe de CoPP que provoca um mensagem do syslog no evento que o ponto inicial é excedido. O comando **está registrando o level> <logging nivelado <dropped limiar de queda do count> dos bytes**.

```
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
```

Está aqui um exemplo de um mensagem do syslog:

```
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
```

Contadores de CoPP

CoPP apoia as mesmas estatísticas de QoS que toda a outra relação. Mostra as estatísticas das classes que formam a política de serviços para cada módulo de E/S que apoia CoPP. Use o comando do **controle plano da relação do mapa de política da mostra** ver as estatísticas para CoPP.

> Nota: Todas as classes devem ser monitoradas em termos dos 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
```

A fim obter uma ideia agregada de contadores conformados e violados para todo o mapa de classe e módulos de E/S, use o **controle plano da relação do mapa de política da mostra | eu "classifico|conforme-se|"** comando **violado**.

```
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 o class-default devem ser monitorados para assegurar-se de que não haja nenhum aumento da elevação, mesmo para contadores conformados. Idealmente, estas duas classes devem ter valores baixos para o contador conformado e pelo menos nenhum aumento contrário violado.

Contadores ACL

O comando da por-**entrada das estatísticas** não é apoiado para IP ACL ou MAC ACL usado no mapa de classe de CoPP, e não tem nenhum efeito quando aplicado a IP ACL de CoPP ou a MAC ACL. (Não há nenhuma verificação CLI feita pelo Parser CLI). A fim ver o CoPP MAC ACL ou IP ACL bate em um módulo de E/S, usa o **comando detail interno das entradas da entrada da lista de acesso do sistema da mostra**.

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]
```

Melhores prática da configuração de CoPP

Estas são recomendações da melhor prática para a configuração de CoPP:

- Use o modo restrito de CoPP à revelia.
- O perfil denso de CoPP é recomendado quando o chassi é carregado inteiramente com os módulos do F2 Series ou carregado com mais módulos do F2 Series do que todos os outros módulos de E/S.
- Não se recomenda desabilitar CoPP. Ajuste o padrão CoPP, como necessário.
- Monitore gotas sem intenção, e adicionar ou altere a política de CoPP do padrão do acordo ao tráfego previsto.
- Baseado no número de FE no chassi, os ajustes CIR e BC para CoPP podem ser aumentados ou diminuído. Isto é baseado igualmente no papel dos dispositivos na rede, os protocolos que são executado, e assim por diante.
- Porque os testes padrão de tráfego mudam constantemente em um **centro de dados**, 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 F2 Series LC, mas não como fácil para um M2 Series ou um M108 LC. Isto é porque o compartilhamento de recurso de CoPP entre VDC se as portas do mesmo FE pertencem aos VDC diferentes (M1 Series ou M2 Series LC). As portas de um FE, mesmo em VDC diferentes, contagem contra o mesmo ponto inicial para CoPP.
- A configuração do Fator de Escala é recomendada quando um chassi é carregado com o F2 Series e os módulos da série M.

Melhores prática da monitoração de CoPP

Estas são recomendações da melhor prática para a monitoração de CoPP:

- Configurar um ponto inicial do mensagem do syslog para CoPP (liberação 5.1 do Cisco NX-OS) a fim monitorar as gotas reforçadas por CoPP.
- Os mensagens do syslog são gerados se as gotas dentro de uma classe de tráfego excedem o ponto inicial do configurado pelo usuário.
- O ponto inicial e o nível de registro podem ser personalizados dentro de cada classe de tráfego com uso do comando de **registro do <level> do nível do <packet-count> do limiar de queda**.
- Porque das “a opção da por-entrada estatísticas” para CoPP MAC ACL ou IP ACL não é apoiada, use o comando **interno do det das entradas da entrada da lista de acesso do sistema da mostra** monitorar batidas das entradas de controle de acesso (ACE).
- **A classe copp-class-l2-default e o comando class-default** devem ser monitorados para assegurar-se de que não haja nenhum aumento da elevação, mesmo para contadores conformados.
- Todas as classes devem ser monitoradas em termos dos pacotes violados.
- Porque copp-classe-**crítico** é altamente vital mas tem uma política da **gota da violação**, é uma boa prática monitorar a taxa de pacotes conformados a fim receber uma indicação adiantada quando a classe se transforma próximo ao momento onde começa a violação. Se o contador violado aumenta para esta classe, não significa necessariamente um alerta vermelho. Um pouco, significa que esta situação deve ser investigada na curto prazo.
- Use o comando **restrito do perfil do copp** após cada upgrade de código do Cisco NX-OS, ou pelo menos após cada upgrade de código principal do Cisco NX-OS; se uma alteração de CoPP foi terminada previamente, deve ser reaplicada.

Conclusões

- CoPP é uma característica com base em hardware que proteja o supervisor dos ataques DoS.
- O M1, o F2, e o M2 Series LC apoiam CoPP. O F1 Series LC não apoia CoPP.
- A configuração de CoPP é similar a MQC (Modular QoS CLI).
- A configuração e a monitoração de CoPP são executadas somente em um padrão VDC.
- O padrão CoPP BPP pode ser usado com opções restritas, moderados, leves, e densas.
- Clone CoPP BPP CoPP personalizado ordena a fim combinar requisitos de rede específicos.

- Os contadores de CoPP (conformados e violados nos bytes pelo mapa de classe) são indicados com o comando do **controle plano da relação do mapa de política da mostra**.
- O tráfego recebido pelo CPU do módulo do supervisor iguala o número total de FE vezes a taxa permitida.
- Tente evitar portas compartilhadas de um FE através dos VDC diferentes.
- Siga melhores prática de CoPP a fim executar e monitorar com sucesso as características.

Recursos não suportados

Estas características não são apoiadas:

- Policiamento distribuído do agregado.
- Vigilância de microfluxo.
- Policiamento da exceção da saída.
- Apoio de CoPP para o BPDU que vem de uma porta dot1q-tunnel (QinQ): Cisco Discovery Protocol (CDP), dot1x, Spanning Tree Protocol (STP), e protocolo VLAN Trunk (VTP).