CoPP en los 7000 Series Switch del nexo

Contenido

Introducción

Este documento describe lo que, cómo, y porqué se utilizan las Políticas del plano de control (CoPP) en los 7000 Series Switch del nexo, que incluyen el F1, F2, M1, y los módulos y el linecards (LC) de las M2 Series. También incluye las directivas de la mejor práctica, así como cómo personalizar una directiva de CoPP.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del sistema operativo CLI del nexo.

Componentes Utilizados

La información en este documento se basa en los 7000 Series Switch del nexo con el módulo del Supervisor 1.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

CoPP en la descripción del 7000 Series Switch del nexo

El CoPP es crítico a la operación de la red. Un ataque de Negación de servicio (DoS) al control/al plano de administración, que se pueden perpetrar inadvertidamente o malévolo, implica típicamente las altas velocidades de tráfico que dan lugar a la utilización excesiva de la CPU. El módulo de Supervisor pasa una cantidad de tiempo excesiva que maneja los paquetes.

Los ejemplos de tales ataques incluyen:

- Pedidos de eco del Internet Control Message Protocol (ICMP).
- Paquetes enviados con las IP-**opciones** fijadas.

Esto puede llevar a:

- Pérdida de mensajes señales de mantenimiento y de actualizaciones del Routing Protocol.
- Relleno de las colas de paquete, que da lugar a los descensos indistintos.
- Sesiones interactivas lentas o insensibles.

Los ataques pueden abrumar la estabilidad de la red y la Disponibilidad y llevar a las interrupciones de la red de negocio-afectación.

CoPP es una característica basado en hardware que protege al supervisor contra los ataques DOS. Controla la tarifa en la cual los paquetes se permiten alcanzar al supervisor. La característica de CoPP se modela como una entrada política de calidad de servicio (QoS) asociada a la interfaz especial llamada la **controle de plano**. Sin embargo, CoPP es una función de seguridad y no una parte de QoS. Para proteger al supervisor, el CoPP separa los paquetes planos de los datos de los paquetes del avión del control (lógica de la excepción). Identifica los paquetes de ataque DOS de los paquetes válidos (clasificación). CoPP permite la clasificación de estos paquetes:

- Reciba los paquetes
- Paquetes de multidifusión
- Paquetes de la excepción
- Reoriente los paquetes
- Transmita los paquetes MAC + del no IP
- Transmita los paquetes MAC +IP (véase el Id. de bug Cisco CSCub47533 - los paquetes en L2 Vlan (ningún SVI) que golpea CoPP)
- Paquetes del Mcast MAC +IP
- Paquetes del MAC de router + del no IP
- Paquetes ARP

Después de que se clasifique un paquete, el paquete puede también ser marcado y utilizado para asignar diversas prioridades basadas en el tipo de paquetes. Conforme, excédase, y las acciones de violación (transmita, caiga, disminución) pueden ser fijadas. Si no se asocia ningún policer a una clase, después se agrega un policer predeterminado cuya acción de conformidad es descenso. Espigue los paquetes se limpian con la clase predeterminada. Se soporta una tarifa, y dos valoran, policing tricolor bicolor.

Trafique que golpea el CPU en el módulo de Supervisor puede venir adentro a través de cuatro trayectorias:

1. Interfaces Inband (puerto del panel frontal) para el tráfico enviado por el linecards.

2. Interfaz de administración (mgmt0) usada para el tráfico de administración.

3. Interfaz del Control and Monitoring Processor (CMP) usada para la consola.

4. El Switched Ethernet hacia fuera congriega el canal (EOBC) para controlar el linecards del módulo de Supervisor y para intercambiar los mensajes de estado.

Solamente el tráfico enviado a través de la interfaz Inband está conforme a CoPP, porque éste es el único tráfico que alcanza el módulo de Supervisor a través de los motores de reenvío (FE) en el linecards. La implementación del 7000 Series Switch del nexo de CoPP es basado en hardware solamente, así que significa que CoPP no es realizado en el software por el módulo de Supervisor. Las funciones de CoPP (policing) se implementan en cada FE independientemente. Cuando las diversas tarifas se configuran para el directiva-mapa de CoPP, la consideración debe ser respeto admitido al número de linecards en el sistema.

El tráfico total recibido por el supervisor es tiempos N X, donde está el número N de FE en el sistema del nexo 7000, y X es la tarifa permitida para la clase determinada. Los valores configurados del policer se aplican en a por la base FE, y el tráfico total propenso golpeó el CPU es la suma del tráfico conformado y transmitido en todos los FE. Es decir trafique que golpea el CPU iguala configurado conforma tarifa multiplicada por el número de FE.

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

La configuración de CoPP se implementa solamente en el contexto predeterminado del dispositivo virtual (VDC); sin embargo, las directivas de CoPP son aplicables para todos los VDC. La misma política global es aplicada para todo el linecards. CoPP aplica a los recursos compartidos entre los VDC si los puertos de los mismos FE pertenecen a diversos VDC (M1 Series o las M2 Series LC). Por ejemplo, puertos de un FE, incluso en diversos VDC, cuenta contra el mismo umbral para CoPP.

Si el mismo FE se comparte entre diversos VDC y una clase dada de tráfico del plano del control excede el umbral, esto afecta a todos los VDC en el mismo FE. Se recomienda para dedicar un FE por el VDC para aislar la aplicación de CoPP, si es posible.

Cuando sube el Switch primera vez, la política predeterminada se debe programar para proteger la **controle de plano**. CoPP proporciona las políticas predeterminadas, que se aplican a la **controle de plano** como parte de la secuencia del arranque inicial.

Porqué CoPP en el 7000 Series Switch del nexo

El 7000 Series Switch del nexo se despliega como una agregación o switch del núcleo. Por lo tanto, es el oído y el cerebro de la red. Maneja la carga máxima en la red. Debe manejar las peticiones frecuentes y de la explosión. Algunas de las peticiones incluyen:

- **Proceso del (BPDU) del Unidad de Spanning-Tree Bridge Protocol Data** - El valor por defecto es cada dos segundos.
- **Primera redundancia de salto** - Esto incluye el Hot Standby Router Protocol (HSRP), el Virtual Router Redundancy Protocol (VRRP), y el protocolo del Equilibrio de carga del gateway (GLBP) - valor por defecto es cada tres segundos.
- **Address resolution** - Esto incluye el protocolo Protocolo de resolución de la dirección (ARP)/la detección de vecino (ARP/ND), Base de información de reenvío (FIB) espiga - hasta una petición por segundo, por el host, tal como combinar de Network Interface Controller (NIC).
- **(DHCP) del Dynamic Host Control Protocol** - Pedido de DHCP, retransmisión - Hasta una solicitud por segundo, por el host.
- **Routing Protocol** para la capa 3 (L3).
- **Interconexión del centro de datos** - Virtualización del transporte del recubrimiento (OTV), Multiprotocol Label Switching (MPLS), y servicio virtual del LAN privado (VPL).

CoPP es esencial para proteger el CPU contra los servidores mal configurado o los ataques potenciales DOS, que permite que el CPU tenga bastante ciclo para procesar los mensajes críticos del avión del control.

Controle el proceso plano en el 7000 Series Switch del nexo

El 7000 Series Switch del nexo toma un acercamiento del avión del control distribuido. Tiene un multifilar en cada uno módulo I/O, así como un multifilar para el avión del control del Switch en el módulo de Supervisor. Descarga las tareas intensivas módulo I/O al CPU para las listas de control de acceso (ACL) y la programación de la BOLA. Escala la capacidad del avión del control con el número de linecards. Esto evita el embotellamiento del Supervisor CPU, que se considera en un acercamiento centralizado. Los limitadores de la tarifa del hardware y CoPP basado en hardware protege el avión del control contra el malo o la actividad maliciosa.

Directiva de las mejores prácticas de CoPP

La directiva de las mejores prácticas de CoPP (BPP) fue introducida en la versión 5.2 del Cisco

NX-OS. La salida del **comando show running-config** no visualiza el contenido del CoPP BPP. **La demostración funciona con el comando all** visualiza el contenido 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 proporciona cuatro opciones al usuario para las políticas predeterminadas:

- Estricto
- Moderado
- Clemente
- Denso (introducido en la versión 6.0(1))

Si no se selecciona ninguna opción o si se salta la configuración, después el policing estricto es aplicado. Todas estas opciones utilizan el mismo class-maps y clases, pero la diversas Velocidad de información comprometida (CIR) y explosión cuentan los valores de (Bc) para limpiar. En las versiones del Cisco NX-OS anterior de 5.2.1, el **comando setup** fueron utilizados para cambiar la opción. La versión 5.2.1 del Cisco NX-OS introdujo una mejora al CoPP BPP para poder cambiar la opción sin el **comando setup**; utilice el **comando profile del 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
```

Utilice el comando del **<profile-type> del perfil del copp de la demostración** de ver la configuración predeterminada de CoPP BPP. Utilice el **comando status del copp de la demostración** de verificar que la directiva de CoPP se ha aplicado correctamente.

```
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 la diferencia entre dos CoPP BPPs, utilice el comando del <profile-**tipo 2> del perfil del <profile-tipo 1> del perfil del diff del copp de la demostración**:

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

Cómo personalizar una directiva de CoPP

Los usuarios pueden crear una directiva personalizada de CoPP. Reproduzca el CoPP predeterminado BPP, y asocíelo a la interfaz de la **controle de plano** porque el CoPP BPP es solo lectura.

```
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.
```

El comando del **[suffix] del <profile-type> del perfil de la copia del copp <prefix>** crea un clon del CoPP BPP. Esto se utiliza para modificar las configuraciones predeterminadas. **El comando profile de copia del copp** es un comando del **modo EXEC**. El usuario puede elegir un prefijo o un sufijo para el nombre de la lista de acceso, class-maps, y del directiva-mapa. Por ejemplo, copp-sistema-p-directiva-**estricto** se cambia al **[suffix] copp-directiva-estricto del [prefix]**. Las configuraciones reproducidas se tratan como configuraciones de usuario y se incluyen en la salida del **funcionamiento de la demostración**.

```
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#
```

Es posible marcar abajo del tráfico que excede y viola una velocidad de la información permitida especificada (PIR) con estos 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 la directiva personalizada de CoPP a la **controle de plano** global de la interfaz. Utilice el **comando status del copp de la demostración** para verificar que la directiva de CoPP se ha aplicado correctamente.

```
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
```

Caso práctico personalizado de la directiva de CoPP

Esta sección describe un ejemplo real en el cual el cliente requiera los dispositivos múltiples de la supervisión para hacer ping con frecuencia las interfaces locales. La dificultad se encuentra en este escenario cuando el cliente quiere modificar la directiva de CoPP para:

- Aumente el CIR de modo que estas direcciones específicas puedan hacer ping el dispositivo local y no violar la directiva.
- Permita que los otros IP Addresses mantengan la capacidad de hacer ping el dispositivo local, pero en un CIR más bajo para los propósitos de Troubleshooting.

La solución se muestra en el próximo ejemplo, que es crear una directiva personalizada con un clase-mapa separado. El clase-mapa separado contiene las dirección IP especificadas de los dispositivos de la supervisión y el clase-mapa tiene un CIR más alto. Esto también sale de la *supervisión* original del clase-mapa, que captura el tráfico ICMP para todos los otros IP Addresses en un CIR más bajo.

```
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
```

Estructura de datos de CoPP

La estructura de datos de CoPP BPP se construye como:

- **Configuración ACL**: IP ACL y MAC ACL.
- **Configuración del clasificador**: Clase-mapa que corresponde con IP ACL o MAC ACL.
- **Configuración de establecimiento de política**: Fije el CIR, el BC, la acción de conformidad, y la acción de violación. El policer tiene dos tarifas (CIR y BC), y dos colores (conforme y 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
```

Factor de escala de CoPP

La configuración del Factor de escala introducida en la versión 6.0 del Cisco NX-OS se utiliza para escalar el índice del policer de la directiva aplicada de CoPP para un linecard determinado. Esto aumenta o reduce la tarifa del policer para un linecard determinado, pero no cambia la directiva actual de CoPP. Los cambios son eficaces inmediatamente, y no hay necesidad de reaplicar la directiva 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
```

Supervisión y Administración de CoPP

Con la versión 5.1 del Cisco NX-OS, es posible configurar un umbral de caída por el nombre de la clase de CoPP que acciona un mensaje de Syslog en el evento que se excede el umbral. El comando **está registrando el level> <logging llano <dropped umbral de caída del count> de los 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
```

Aquí está un ejemplo de un mensaje de 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 soporta las mismas estadísticas de QoS que cualquier otra interfaz. Muestra las estadísticas de las clases que forman la política de servicio para cada módulo I/O ese los soportes CoPP. Utilice el comando de la **controle de plano del show policy-map interface** de ver las estadísticas para CoPP.

> Nota: Todas las clases se deben monitorear en términos de paquetes 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 obtener una vista global de los contadores conformados y violados para todo el clase-mapa y los módulos entrada-salida, utilice la **controle de plano del show policy-map interface | "clase i|conforme|"** 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
```

La clase copp-class-l2-default y el class-default se deben monitorear para asegurarse de que no hay aumentos del alto, incluso para los contadores conformados. Idealmente, estas dos clases deben tener valores bajos para el contador conformado y por lo menos ningún aumento contrario violado.

Contadores ACL

El comando de la por-**entrada de las estadísticas** no se soporta para IP ACL o MAC ACL usado en el clase-mapa de CoPP, y no tiene ningún efecto cuando está aplicado a IP ACL de CoPP o a MAC ACL. (No hay control CLI hecho por el analizador de sintaxis CLI). Para ver el CoPP MAC ACL o IP ACL golpea en módulo I/O, utiliza el **comando detail interno de las entradas de la entrada de la lista de acceso del sistema de la demostración**.

Aquí tiene un ejemplo:

```
!! 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]
```

Mejores prácticas de la configuración de CoPP

Éstas son recomendaciones de la mejor práctica para la configuración de CoPP:

- Utilice el modo estricto de CoPP por abandono.

- Se recomienda el perfil denso de CoPP cuando el chasis se carga completamente con los módulos de las F2 Series o se carga con más módulos de las F2 Series que cualquier otro módulo entrada-salida.

- No se recomienda para inhabilitar CoPP. Ajuste el CoPP predeterminado, según las necesidades.

- Monitoree los descensos involuntarios, y agregue o modifique la directiva predeterminada de CoPP del acuerdo al tráfico previsto.

- De acuerdo con el número de FE en el chasis, las configuraciones CIR y BC para CoPP pueden ser aumentadas o ser disminuidas. Esto también se basa en el papel de los dispositivos en la red, los protocolos que se ejecutan, y así sucesivamente.

- Porque los patrones de tráfico cambian constantemente en un **centro de datos**, el arreglo para requisitos particulares de un CoPP es un proceso constante.

- CoPP y VDC: Todos los puertos del mismo FE deben pertenecer al mismo VDC, que es fácil para las F2 Series LC, pero no como fácil para las M2 Series o un M108 LC. Esto es porque los recursos compartidos de CoPP entre los VDC si los puertos del mismo FE pertenecen a diversos VDC (M1 Series o las M2 Series LC). Los puertos de un FE, incluso en diversos VDC, cuenta contra el mismo umbral para CoPP.

- Se recomienda la configuración del Factor de escala cuando un chasis se carga con las F2 Series y las series módulo M.

Mejores prácticas de la supervisión de CoPP

Éstas son recomendaciones de la mejor práctica para la supervisión de CoPP:

- Configure un umbral del mensaje de Syslog para CoPP (versión 5.1 del Cisco NX-OS) para monitorear los descensos aplicados por CoPP.
- Se generan los mensajes de Syslog si los descensos dentro de una clase de tráfico exceden el umbral del usuario configurado.
- El umbral y el nivel del registro se pueden personalizar dentro de cada clase de tráfico con el uso del comando del **<level> del nivel del <packet-count> del umbral de caída del registro**.
- Porque “la opción de la por-entrada de las estadísticas” para CoPP MAC ACL o IP ACL no se soporta, utilice el comando **interno del det de las entradas de la entrada de la lista de acceso del sistema de la demostración** de monitorear los golpes de las entradas de control de acceso (ACE).
- **La clase copp-class-l2-default y el comando class-default** se deben monitorear para asegurarse de que no hay aumentos del alto, incluso para los contadores conformados.
- Todas las clases se deben monitorear en términos de paquetes violados.
- Porque es copp-clase-**crítico** es altamente vital pero tiene una **política para tirar paquetes de la violación**, es una práctica adecuada monitorear el índice de paquetes conformados para recibir una indicación temprana cuando la clase se convierte en cerca al momento donde comienza la infracción. Si el contador violado aumenta para esta clase, no significa necesariamente una alerta roja. Bastante, significa que esta situación se debe investigar en a corto plazo.
- Utilice el comando **estricto del perfil del copp** después de cada actualización de código del Cisco NX-OS, o por lo menos después de cada actualización de código importante del Cisco NX-OS; si una modificación de CoPP fue completada previamente, debe ser reaplicada.

Conclusiones

- CoPP es una característica basado en hardware que protege al supervisor contra los ataques DOS.
- El M1, el F2, y las M2 Series LC soportan CoPP. Las F1 Series LC no soportan CoPP.
- La configuración de CoPP es similar a MQC (Modular QoS CLI).
- La configuración y la supervisión de CoPP se realiza solamente en un valor por defecto VDC.
- CoPP predeterminado BPP se puede utilizar con las opciones estrictas, moderadas,

clementes, y densas.

- Reproduzca las reglas personalizadas de CoPP BPP CoPP para hacer juego los requisitos de la red específicos.
- Los contadores de CoPP (conformados y violados en los bytes por el clase-mapa) se visualizan con el comando de la **controle de plano del show policy-map interface**.
- El tráfico recibido por el CPU del módulo de Supervisor iguala el número total de FE por la tarifa permitida.
- Intente evitar los puertos compartidos de un FE a través de diversos VDC.
- Siga las mejores prácticas de CoPP para implementar y monitorear con éxito las características.

Características no admitidas

Estas características no se soportan:

- Policing global distribuido.
- Regulación de microflujo.
- Policing de la excepción de la salida.
- Soporte de CoPP para el BPDU que viene de un puerto dot1q-tunnel (QinQ): Cisco Discovery Protocol (CDP), dot1x, Spanning Tree Protocol (STP), y VLAN Trunk Protocol (VTP).