CoPP en los switches Nexus de la serie 7000

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Descripción general de CoPP en el switch Nexus serie 7000
Por qué CoPP en el switch Nexus serie 7000
Procesamiento del plano de control en el switch Nexus serie 7000
Política de prácticas recomendadas de CoPP
Cómo personalizar una política CoPP
Caso práctico de política de CoPP personalizada
Estructura de datos de CoPP
Factor de escalabilidad de CoPP
Administración y supervisión de CoPP
Contadores CoPP
Contadores ACL
Prácticas recomendadas de configuración de CoPP
Prácticas recomendadas de supervisión de CoPP
Conclusiones
Características no admitidas

Introducción

Este documento describe qué, cómo y por qué se utiliza Control Plane Policing (CoPP) en los switches Nexus serie 7000, que incluyen los módulos F1, F2, M1 y M2 Series y las tarjetas de línea (LC). También se incluyen políticas de mejores prácticas y cómo personalizar una política de CoPP.

Prerequisites

Requirements

Cisco recomienda que conozca la CLI del sistema operativo Nexus.

Componentes Utilizados

La información de este documento se basa en los switches Nexus serie 7000 con el módulo Supervisor 1.

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.

Descripción general de CoPP en el switch Nexus serie 7000

El CoPP es fundamental para el funcionamiento de la red. Un ataque de denegación de servicio (DoS) al plano de control/gestión, que puede perpetrarse de forma involuntaria o maliciosa, suele implicar altas tasas de tráfico que dan lugar a una utilización excesiva de la CPU. El módulo Supervisor dedica una cantidad excesiva de tiempo a gestionar los paquetes.

Algunos ejemplos de estos ataques son:

- Solicitudes de eco del protocolo de mensajes de control de Internet (ICMP).
- Paquetes enviados con **ip-options** set.

Esto puede llevar a:

- Pérdida de mensajes de mantenimiento y actualizaciones del protocolo de ruteo.
- Llenado de colas de paquetes, lo que da lugar a caídas indiscriminadas.
- Sesiones interactivas lentas o sin respuesta.

Los ataques pueden saturar la estabilidad y la disponibilidad de la red y provocar interrupciones de la red que afectan a la empresa.

CoPP es una función basada en hardware que protege al supervisor de los ataques de DoS. Controla la velocidad a la que se permite que los paquetes lleguen al Supervisor. La función CoPP se modela como una política de QoS de entrada conectada a la interfaz especial llamada **plano de control**. Sin embargo, CoPP es una función de seguridad y no parte de QoS. Para proteger el Supervisor, la CoPP separa los paquetes del plano de datos de los paquetes del plano de control (Lógica de excepciones). Identifica los paquetes de ataque DoS de los paquetes válidos (Clasificación). CoPP permite la clasificación de estos paquetes:

- Recibir paquetes
- Paquetes de multidifusión
- Paquetes de excepción
- Redirigir paquetes
- MAC de difusión + paquetes que no son IP
- Broadcast MAC + paquetes IP (consulte Cisco Bug ID CSCub47533 - Paquetes en L2 Vlan (sin SVI) que llegan a CoPP)
- MAC de difusión + paquetes IP
- Router MAC + paquetes que no son IP
- paquetes ARP

Después de clasificar un paquete, el paquete también puede ser marcado y utilizado para asignar diferentes prioridades en función del tipo de paquetes. Se pueden configurar, exceder y violar

acciones (transmitir, descartar, marcar). Si no hay ningún regulador asociado a una clase, se agrega un regulador predeterminado cuya acción de conformidad es drop. Los paquetes Glean se controlan con la clase predeterminada. Se admite una velocidad, dos colores y dos velocidades y tres políticas de color.

El tráfico que llega a la CPU en el módulo Supervisor puede llegar a través de cuatro rutas:

1. Interfaces dentro de la banda (puerto del panel frontal) para el tráfico enviado por tarjetas de línea.

2. Interfaz de gestión (mgmt0) utilizada para el tráfico de gestión.

3. Interfaz del procesador de control y supervisión (CMP) utilizada para la consola.

4. Switched Ethernet Out Band Channel (EOBC) para controlar las tarjetas de línea desde el módulo Supervisor e intercambiar mensajes de estado.

Sólo el tráfico enviado a través de la interfaz dentro de la banda está sujeto a CoPP, porque éste es el único tráfico que llega al módulo Supervisor a través de los motores de reenvío (FE) en las tarjetas de línea. La implementación del switch Nexus serie 7000 de CoPP se basa únicamente en hardware, lo que significa que el módulo Supervisor no realiza la CoPP en el software. La funcionalidad CoPP (regulación) se implementa en cada FE de forma independiente. Cuando las diversas velocidades se configuran para el policy-map de CoPP, se debe tener en cuenta el número de tarjetas de línea en el sistema.

El tráfico total recibido por el Supervisor es N veces X, donde N es el número de FE en el sistema Nexus 7000, y X es la velocidad permitida para la clase en particular. Los valores del regulador de tráfico configurados se aplican por FE, y el tráfico agregado propenso a alcanzar la CPU es la suma del tráfico conformado y transmitido en todos los FE. En otras palabras, el tráfico que llega a la CPU equivale a la velocidad de conformidad configurada 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 (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 sólo se implementa en el contexto de dispositivo virtual (VDC) predeterminado; sin embargo, las políticas de CoPP son aplicables a todos los VDC. La misma política global se aplica a todas las tarjetas de línea. CoPP aplica el uso compartido de recursos entre VDC si los puertos de los mismos FE pertenecen a diferentes VDC (serie M1 o serie M2 LC). Por ejemplo, los puertos de un FE, incluso en VDC diferentes, cuentan con el mismo umbral para CoPP.

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

Cuando el switch se activa por primera vez, la política predeterminada se debe programar para proteger el **plano de control**. CoPP proporciona las políticas predeterminadas, que se aplican al

plano de control como parte de la secuencia inicial.

Por qué CoPP en el switch Nexus serie 7000

El switch Nexus serie 7000 se implementa como switch de agregación o de núcleo. Por lo tanto, es el oído y el cerebro de la red. Administra la carga máxima en la red. Debe gestionar solicitudes frecuentes y ráfagas. Algunas de las solicitudes incluyen:

- **Procesamiento de la unidad de datos del protocolo de puente de árbol de extensión (BPDU)**: el valor predeterminado es cada dos segundos.
- **Redundancia de primer salto**: incluye protocolo de router en espera en caliente (HSRP), protocolo de redundancia de router virtual (VRRP) y protocolo de equilibrio de carga de gateway (GLBP). El valor predeterminado es cada tres segundos.
- **Resolución de direcciones**: incluye protocolo de resolución de direcciones/detección de vecinos (ARP/ND), reenvío de información básica (FIB) global: hasta una solicitud por segundo, por host, como la agrupación del controlador de interfaz de red (NIC).
- **Protocolo de control de host dinámico (DHCP)**: solicitud DHCP, retransmisión: hasta una solicitud por segundo, por host.
- **Protocolos de routing** para la capa 3 (L3).
- **Interconexión del Data Center**: Overlay Transport Virtualization (OTV), Multiprotocol Label Switching (MPLS) y Virtual Private LAN Service (VPLS).

CoPP es esencial para proteger la CPU contra servidores mal configurados o posibles ataques de DoS, lo que permite que la CPU tenga suficiente ciclo para procesar mensajes críticos del plano de control.

Procesamiento del plano de control en el switch Nexus serie 7000

El switch Nexus serie 7000 adopta un enfoque de plano de control distribuido. Tiene un núcleo múltiple en cada módulo de E/S, así como un núcleo múltiple para el plano de control del switch en el módulo Supervisor. Descarga tareas intensivas a la CPU del módulo de E/S para las listas de control de acceso (ACL) y la programación FIB. Escala la capacidad del plano de control con el número de tarjetas de línea. Esto evita los cuellos de botella de la CPU del supervisor, que se ven en un enfoque centralizado. Los limitadores de velocidad de hardware y la CoPP basada en hardware protegen el plano de control de actividades dañinas o dañinas.

Política de prácticas recomendadas de CoPP

La política de prácticas recomendadas (BPP) de CoPP se presentó en Cisco NX-OS versión 5.2. El resultado del comando **show running-config** no muestra el contenido del CoPP BPP. El

comando **show run all** muestra 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
- Moderada
- indulgente
- Denso (introducido en la versión 6.0(1))

Si no se selecciona ninguna opción o si se omite la configuración, se aplica una regulación estricta. Todas estas opciones utilizan los mismos mapas de clase y clases, pero para la regulación de tráfico se utilizan diferentes valores de Velocidad de información comprometida (CIR) y de Recuento de ráfaga (BC). En las versiones anteriores a 5.2.1 de Cisco NX-OS, el comando **setup** se utilizó para cambiar la opción. Cisco NX-OS Release 5.2.1 introdujo una mejora en CoPP BPP para que la opción pueda cambiarse sin el **comando setup**; use el 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
```

Utilice el comando **show copp profile <profile-type>** para ver la configuración predeterminada de CoPP BPP. Utilice el comando **show copp status** para verificar que la política 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 BPP, utilice el 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----------------------------------------
```

Cómo personalizar una política CoPP

Los usuarios pueden crear una política CoPP personalizada. Clonar el CoPP BPP predeterminado y adjuntarlo a la interfaz **del plano de control** porque el CoPP BPP es de sólo 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 **copp copy profile <profile-type> <prefix> [sufix]** crea un clon de CoPP BPP. Esto se utiliza para modificar las configuraciones predeterminadas. El comando **copp copy profile** es un **comando exec mode**. El usuario puede elegir un prefijo o sufijo para la lista de acceso, mapas de clase y nombre de mapa de políticas. Por ejemplo, **copp-system-p-policy-strict** se cambia a **[prefix]copp-policy-strict[sufix]**. Las configuraciones clonadas se tratan como configuraciones de usuario y se incluyen en el resultado **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#
```

Es posible marcar el tráfico que excede y viola una Velocidad de información permitida (PIR) especificada 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 política CoPP personalizada al **plano de control** de la interfaz global. Utilice el comando **show copp status** para verificar que la política 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 de política de CoPP personalizada

Esta sección describe un ejemplo real en el que el cliente necesita varios dispositivos de monitoreo para hacer ping con frecuencia a las interfaces locales. En esta situación, el cliente desea modificar la política CoPP para:

- Aumente el CIR para que estas direcciones específicas puedan hacer ping al dispositivo local y no violar la política.
- Permita que las otras direcciones IP mantengan la capacidad de hacer ping al dispositivo local, pero a un CIR inferior para propósitos de troubleshooting.

La solución se muestra en el siguiente ejemplo, que consiste en crear una política personalizada

con un mapa de clase independiente. El mapa de clase separado contiene las direcciones IP especificadas de los dispositivos de monitoreo y el mapa de clase tiene un CIR más alto. Esto también deja el *monitoreo* de mapa de clase original, que captura el tráfico ICMP para todas las demás direcciones IP en un CIR inferior.

```
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>
```

Estructura de datos de CoPP

La estructura de datos de CoPP BPP se construye de la siguiente manera:

- **Configuración de ACL**: ACL IP y ACL MAC.
- **Configuración del clasificador**: Class-map que coincide con ACL IP o ACL MAC.
- **Configuración del regulador**: Establezca CIR, BC, accione de conformidad y viole la acción. El regulador de tráfico tiene dos velocidades (CIR y BC) y dos colores (conformidad y violación).

```
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
```

Factor de escalabilidad de CoPP

La configuración del factor de escala introducida en Cisco NX-OS versión 6.0 se utiliza para escalar la tasa de regulación de la política CoPP aplicada para una tarjeta de línea determinada. Esto aumenta o reduce la velocidad del regulador de tráfico para una tarjeta de línea determinada, pero no cambia la política CoPP actual. Los cambios son efectivos inmediatamente, y no hay necesidad de volver a aplicar la política 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
```

Administración y supervisión de CoPP

Con Cisco NX-OS Release 5.1, es posible configurar un umbral de caída por nombre de clase

CoPP que activa un mensaje de Syslog en caso de que se exceda el umbral. El comando es **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
```

A continuación se muestra un ejemplo de un mensaje de 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

CoPP admite las mismas estadísticas de QoS que cualquier otra interfaz. Muestra las estadísticas de las clases que forman la política de servicio para cada módulo de E/S que admite CoPP. Utilice el comando **show policy-map interface control-plane** para ver las estadísticas de CoPP.

> **Nota:** Todas las clases deben monitorearse 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 agregada de los contadores conformados y violados para todos los módulos de mapa de clase y E/S, utilice el **plano de control de interfaz show policy-map | es el** comando **"clase|conformidad|infracción"**.

```
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 class-default** deben monitorearse para asegurarse de que no haya aumentos altos, incluso para los contadores conformados. Lo ideal es que estas dos clases tengan valores bajos para un contador conformado y al menos no se viole el aumento del contador.

Contadores ACL

El comando **statistics per-entry** no se soporta para ACL IP o ACL MAC utilizado en el mapa de clase CoPP, y no tiene efecto cuando se aplica a ACL IP o ACL MAC CoPP. (El analizador de CLI no realiza ninguna comprobación de CLI). Para ver los resultados de ACL MAC o ACL IP de CoPP en un módulo de E/S, utilice el comando **show system internal access-list input entries detail**.

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]
```

Prácticas recomendadas de configuración de CoPP

Estas son recomendaciones de prácticas recomendadas para la configuración de CoPP:

- Utilice el modo CoPP estricto de forma predeterminada.
- Se recomienda un perfil denso de CoPP cuando el chasis está completamente cargado con módulos F2 Series o con más módulos F2 Series que cualquier otro módulo de E/S.
- No se recomienda inhabilitar CoPP. Ajuste la CoPP predeterminada, según sea necesario.
- Supervise las caídas no deseadas y agregue o modifique la política CoPP predeterminada de acuerdo con el tráfico esperado.
- Según el número de FE en el chasis, la configuración de CIR y BC para CoPP puede aumentarse o reducirse. Esto también se basa en la función de los dispositivos en la red, los

protocolos que se ejecutan, etc.

- Debido a que los patrones de tráfico cambian constantemente en un **Data Center**, la personalización de una CoPP es un proceso constante.

- CoPP y VDC: Todos los puertos del mismo FE deben pertenecer al mismo VDC, que es fácil para una LC de la serie F2, pero no tan fácil para una serie M2 o M108 LC. Esto se debe a que el recurso compartido CoPP entre VDC si los puertos del mismo FE pertenecen a diferentes VDC (serie M1 o serie M2 LC). Los puertos de un FE, incluso en diferentes VDC, cuentan con el mismo umbral para CoPP.

- Se recomienda la configuración del factor de escala cuando se carga un chasis con los módulos F2 y M Series.

Prácticas recomendadas de supervisión de CoPP

Estas son recomendaciones de prácticas recomendadas para el monitoreo de CoPP:

- Configure un umbral de mensaje de syslog para CoPP (Cisco NX-OS versión 5.1) para supervisar las caídas aplicadas por CoPP.

- Los mensajes de Syslog se generan si las caídas dentro de una clase de tráfico exceden el umbral configurado por el usuario.

- El umbral y el nivel de registro se pueden personalizar dentro de cada clase de tráfico con el uso del comando **logging drop threshold <packet-count> level <level>**.

- Debido a que no se admite la opción "estadísticas por entrada" para CoPP MAC ACL o IP ACL, utilice el comando **show system internal access-list input entries det** para monitorear los resultados de las Entradas de Control de Acceso (ACE).

- Los comandos **class copp-class-l2-default y class-default** deben monitorearse para asegurarse de que no haya aumentos altos, incluso para los contadores conformados.

- Todas las clases deben monitorearse en términos de paquetes violados.

- Debido a que **copp-class-key** es muy vital pero tiene una **política de caída de infracción**, es una buena práctica monitorear la velocidad de los paquetes conformados para recibir una indicación temprana cuando la clase se acerca al momento en que comienza la violación. Si el contador violado aumenta para esta clase, no significa necesariamente una alerta roja. Más bien, significa que esta situación debe investigarse a corto plazo.

- Utilice el comando **copp profile strict** después de cada actualización de código de Cisco NX-OS, o al menos después de cada actualización de código principal de Cisco NX-OS; si se ha completado previamente una modificación de CoPP, debe volver a aplicarse.

Conclusiones

- CoPP es una función basada en hardware que protege al supervisor de los ataques de DoS.
- Las LC de las series M1, F2 y M2 soportan CoPP. Las LC de la serie F1 no soportan CoPP.
- La configuración CoPP es similar a MQC (Modular QoS CLI).
- La configuración y supervisión de CoPP se realiza solamente en un VDC predeterminado.
- La CoPP BPP predeterminada se puede utilizar con opciones estrictas, moderadas, indulgentes y densas.
- Clonar CoPP BPP a reglas CoPP personalizadas para satisfacer los requisitos específicos de la red.
- Los contadores CoPP (conformados y violados en bytes por class-map) se muestran con el comando **show policy-map interface control-plane**.
- El tráfico recibido por la CPU del módulo Supervisor es igual al número total de FE por la velocidad permitida.
- Intente evitar los puertos compartidos de un FE a través de diferentes VDC.
- Siga las prácticas recomendadas de CoPP para implementar y monitorear con éxito las funciones.

Características no admitidas

Estas funciones no son compatibles:

- Regulación de agregado distribuida.
- Regulación de microflujo.
- Regulación de excepciones de salida.
- Compatibilidad con CoPP para BPDU que proviene de un puerto de túnel dot1q (QinQ): Protocolo de detección de Cisco (CDP), DOT1x, protocolo de árbol de extensión (STP) y protocolo troncal de VLAN (VTP).