CoPP su switch Nexus serie 7000

Sommario

Introduzione

Questo documento descrive cosa, come e perché Control Plane Policing (CoPP) viene utilizzato sugli switch Nexus serie 7000, che includono i moduli serie F1, F2, M1 e M2 e le schede di linea (LC). Include inoltre le procedure consigliate, nonché le modalità di personalizzazione di una procedura CoPP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della CLI del sistema operativo Nexus.

Componenti usati

Per la stesura del documento, sono stati usati switch Nexus serie 7000 con Supervisor 1 Module.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica di CoPP su switch Nexus serie 7000

Il CoPP è fondamentale per il funzionamento della rete. Un attacco Denial of Service (DoS) al Control/Management Plane, che può essere perpetrato inavvertitamente o malintenzionalmente, in genere comporta alte velocità di traffico che determinano un utilizzo eccessivo della CPU. Il modulo Supervisor impiega un tempo eccessivo per gestire i pacchetti.

Esempi di tali attacchi includono:

- Richieste echo Internet Control Message Protocol (ICMP).
- Pacchetti inviati con **opzioni ip** impostate.

Ciò può comportare:

- Perdita dei messaggi keep-alive e degli aggiornamenti del protocollo di routing.
- Riempimento delle code di pacchetti, con conseguenti perdite indiscriminate.
- Sessioni interattive lente o che non rispondono.

Gli attacchi possono sovraccaricare la stabilità e la disponibilità della rete e causare interruzioni delle attività aziendali.

CoPP è una funzione basata su hardware che protegge il Supervisor dagli attacchi DoS. Controlla la velocità con cui i pacchetti possono raggiungere il Supervisor. La funzione CoPP è modellata come una regola QoS di input collegata all'interfaccia speciale chiamata **control-plane**. Tuttavia, il CoPP è una funzionalità di sicurezza e non fa parte di QoS. Per proteggere il Supervisor, il CoPP separa i pacchetti del piano dati dai pacchetti del piano di controllo (logica dell'eccezione). Identifica i pacchetti di attacco DoS da pacchetti validi (classificazione). Il protocollo CoPP consente di classificare i seguenti pacchetti:

- Ricevi pacchetti
- Pacchetti multicast
- Pacchetti eccezione
- Reindirizza pacchetti
- MAC broadcast + pacchetti non IP
- Broadcast MAC + pacchetti IP (vedere Cisco Bug ID CSCub47533 - Pacchetti in Vlan L2 (senza SVI) con collegamento CoPP)
- Mcast - MAC + pacchetti IP
- MAC router + pacchetti non IP
- Pacchetti ARP

Dopo aver classificato un pacchetto, il pacchetto può essere contrassegnato e usato per assegnare priorità diverse in base al tipo di pacchetto. È possibile impostare le azioni di

conformità, superamento e violazione (trasmissione, rilascio, contrassegno). Se a una classe non è associato alcun policer, viene aggiunto un policer predefinito la cui azione conform è drop. I pacchetti Glean vengono controllati con default-class. Sono supportate una frequenza, due colori e due frequenze, tre colori.

Il traffico che colpisce la CPU sul modulo Supervisor può arrivare attraverso quattro percorsi:

1. Interfacce in banda (porta del pannello anteriore) per il traffico inviato dalle schede di linea.

2. Mgmt0 (interfaccia di gestione) utilizzata per la gestione del traffico.

3. Interfaccia CMP (Control and Monitoring Processor) utilizzata per la console.

4. Switched Ethernet Out Band Channel (EOBC) per controllare le schede di linea dal modulo Supervisor e scambiare i messaggi di stato.

Solo il traffico inviato tramite l'interfaccia Inband è soggetto a CoPP, in quanto è l'unico traffico che raggiunge il modulo Supervisor tramite i motori di inoltro (FE) sulle schede di linea. L'implementazione dello switch Nexus serie 7000 di CoPP è solo basata su hardware, quindi il CoPP non viene eseguito nel software dal modulo Supervisor. La funzionalità CoPP (policing) è implementata su ciascun FE in modo indipendente. Quando le varie tariffe sono configurate per la mappa delle politiche CoPP, è necessario considerare il numero di schede di linea nel sistema.

Il traffico totale ricevuto dal Supervisor è N per X, dove N è il numero di FE sul sistema Nexus 7000 e X è la velocità consentita per la classe specifica. I valori del policer configurati si applicano per FE e il traffico aggregato soggetto a raggiungere la CPU è la somma del traffico conforme e trasmesso su tutti gli FE. In altre parole, il traffico che raggiunge la CPU è uguale alla velocità di conformità configurata moltiplicata per il numero di FE.

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

La configurazione CoPP viene implementata solo nel contesto di dispositivo virtuale predefinito (VDC, Virtual Device Context). tuttavia, le politiche CoPP sono applicabili a tutte le VDC. Lo stesso criterio globale viene applicato a tutte le schede di linea. Il CoPP applica la condivisione delle risorse tra VDC se le porte degli stessi FE appartengono a VDC diversi (serie M1 o LC serie M2). Ad esempio, le porte di un FE, anche in VDC diversi, vengono conteggiate rispetto alla stessa soglia per CoPP.

Se lo stesso FE è condiviso tra VDC diverse e una determinata classe di traffico del control plane supera la soglia, ciò influisce su tutti i VDC dello stesso FE. Si raccomanda di dedicare un FE per VDC al fine di isolare, se possibile, l’applicazione del CoPP.

Quando lo switch viene attivato per la prima volta, la policy predefinita deve essere programmata per proteggere il **control plane**. CoPP fornisce le regole predefinite, che vengono applicate al **control-plane** come parte della sequenza di avvio iniziale.

Perché CoPP su switch Nexus serie 7000

Nexus serie 7000 Switch viene implementato come switch di aggregazione o core. Quindi è l'orecchio e il cervello della rete. Gestisce il carico massimo nella rete. Deve gestire richieste frequenti e burst. Alcune richieste includono:

- **Elaborazione Spanning Tree Bridge Protocol Data Unit (BPDU)** - L'impostazione predefinita è ogni due secondi.
- **Ridondanza del primo hop** - include HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) e GLBP (Gateway Load Balancing Protocol). L'impostazione predefinita è ogni tre secondi.
- **Risoluzione degli indirizzi** - Include Address Resolution Protocol/Neighbor-Discovery (ARP/ND), Forwarding Information Base (FIB) Glean - Fino a una richiesta al secondo, per host, ad esempio raggruppamento NIC (Network Interface Controller).
- **Dynamic Host Control Protocol (DHCP)** - Richiesta DHCP, Relay - Fino a una richiesta al secondo, per host.
- **Protocolli di routing** per il layer 3 (L3).
- **Data Center Interconnect** - Overlay Transport Virtualization (OTV), Multiprotocol Label Switching (MPLS) e Virtual Private LAN Service (VPLS).

Il CoPP è essenziale per proteggere la CPU da server configurati in modo errato o da potenziali attacchi DoS, che consentono alla CPU di avere un ciclo sufficiente per elaborare i messaggi critici del control plane.

Control Plane Processing sullo switch Nexus serie 7000

Lo switch Nexus serie 7000 adotta un approccio con control plane distribuito. Dispone di un multi-core su ciascun modulo di I/O, nonché di un multi-core per il control plane dello switch sul modulo Supervisor. Ripartisce il carico di lavoro intensivo sulla CPU del modulo di I/O per gli Access Control List (ACL) e la programmazione FIB. Scala la capacità del control plane con il numero di schede di linea. In questo modo si evitano i colli di bottiglia della CPU del Supervisor, che si verificano in un approccio centralizzato. I limitatori di velocità hardware e il protocollo CoPP basato su hardware proteggono il control plane da attività dannose o dannose.

Policy di best practice CoPP

La policy BPP (CoPP Best Practices Policy) è stata introdotta in Cisco NX-OS versione 5.2. L'output del comando **show running-config** non visualizza il contenuto del BPP CoPP. Il comando **show run all** visualizza il contenuto di 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 fornisce all'utente quattro opzioni per i criteri predefiniti:

- Ristretta
- Moderate (Medio)
- Incline
- Dense (introdotto nella release 6.0(1))

Se non è selezionata alcuna opzione o se l'impostazione viene ignorata, viene applicata una policy rigorosa. Tutte queste opzioni utilizzano le stesse classi e mappe di classi, ma valori CIR (Committed Information Rate) e BC (Burst Count) diversi per il policing. Nelle versioni Cisco NX-OS precedenti alla 5.2.1, l'opzione è stata modificata con il comando **setup**. Cisco NX-OS versione 5.2.1 ha introdotto un miglioramento al BPP CoPP in modo che l'opzione possa essere modificata senza il comando **setup**; utilizzare il 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
```

Utilizzare il comando **show copp profile <tipo-profilo>** per visualizzare la configurazione predefinita del protocollo CoPP BPP. Utilizzare il comando **show copp status** per verificare che il criterio CoPP sia stato applicato correttamente.

```
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
```

Per visualizzare la differenza tra due BPP CoPP, usare il comando **show copp diff profile <tipo-profilo 1> profile <tipo-profilo 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----------------------------------
```

Come personalizzare un criterio CoPP

Gli utenti possono creare un criterio CoPP personalizzato. Clonare il file CoPP BPP predefinito e collegarlo all'interfaccia del **control plane** perché il file CoPP BPP è di sola lettura.

```
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.
```

Il comando **copp copy profile <tipo-profilo> <prefisso> [suffix]** crea un clone del protocollo CoPP BPP. Questa opzione viene usata per modificare le configurazioni predefinite. Il comando **copp copy profile** è in **modalità di esecuzione**. L'utente può scegliere un prefisso o un suffisso per l'elenco degli accessi, le mappe classi e il nome della mappa dei criteri. Ad esempio, **copp-system-p-policy-strict** viene modificato in **[prefix]copp-policy-strict[suffix]**. Le configurazioni duplicate vengono considerate come configurazioni utente e sono incluse nell'output **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#
```

Èpossibile marcare il traffico che supera e viola una determinata velocità di informazioni consentite (PIR, Permitted Information Rate) con questi comandi:

```
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)#
```

Applicare la policy CoPP personalizzata al control plane dell'interfaccia globale. Per verificare che il criterio CoPP sia stato applicato correttamente, utilizzare il comando show copp status.

```
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 di studio personalizzato sulle policy CoPP

In questa sezione viene descritto un esempio reale in cui il cliente ha bisogno di più dispositivi di monitoraggio per eseguire frequentemente il ping delle interfacce locali. In questo scenario si riscontrano difficoltà quando il cliente desidera modificare la politica CoPP al fine di:

- Aumentare il valore CIR in modo che questi indirizzi specifici possano eseguire il ping sul dispositivo locale e non violare il criterio.
- Consentire agli altri indirizzi IP di mantenere la possibilità di eseguire il ping sul dispositivo locale, ma a un CIR inferiore per la risoluzione dei problemi.

La soluzione viene illustrata nell'esempio seguente, che prevede la creazione di un criterio personalizzato con una mappa delle classi separata. La mappa di classe separata contiene gli indirizzi IP specificati dei dispositivi di monitoraggio e la mappa di classe ha un CIR più alto. In questo modo, rimane anche il *monitoraggio della* mappa delle classi originale, che acquisisce il traffico ICMP per tutti gli altri indirizzi IP a un CIR inferiore.

```
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>
```

Struttura dati CoPP

La struttura dei dati BPP CoPP è costruita come:

- **Configurazione ACL**: ACL IP e ACL MAC.
- **Configurazione classificatore**: Mapping di classi corrispondente ad ACL IP o ACL MAC.
- **Configurazione del controller**: Impostare CIR, BC, uniformare l'azione e violare l'azione. Il policer ha due velocità (CIR e BC) e due colori (conforme e viola).

```
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
```

Fattore di scala CoPP

La configurazione del fattore di scala introdotta in Cisco NX-OS versione 6.0 viene utilizzata per scalare la frequenza dei policer del criterio CoPP applicato per una determinata scheda di linea. In questo modo si aumenta o si riduce la frequenza di controllo per una determinata scheda di linea, ma non si modifica l'attuale politica CoPP. I cambiamenti sono effettivi immediatamente e non è necessario riapplicare la politica del 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
```

Monitoraggio e gestione CoPP

Con Cisco NX-OS release 5.1, è possibile configurare una soglia di rilascio per nome di classe CoPP che attiva un messaggio Syslog nel caso in cui venga superata la soglia. Il comando sta registrando il livello <conteggio byte scartati> <livello di registrazione>.

```
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
```

Di seguito è riportato un esempio di messaggio 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.
```

Contatori CoPP

CoPP supporta le stesse statistiche QoS di qualsiasi altra interfaccia. Vengono visualizzate le statistiche delle classi che formano i criteri del servizio per ogni modulo di I/O che supporta CoPP. Utilizzare il comando **show policy-map interface control-plane** per visualizzare le statistiche relative a CoPP.

> **Nota:** Tutte le classi devono essere monitorate in termini di pacchetti violati.

```
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
```

Per ottenere una visualizzazione aggregata dei contatori conformi e violati per tutti i moduli di I/O e mappa delle classi, utilizzare il **control plane show policy-map interface | i** comando **"class|conform|violated"**.

```
SITE1-AGG1# show policy-map interface control-plane | i "class|conform|violated"
class-map copp-class-critical-CUSTOMIZED-COPP (match-any)
conformed 123126534 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 107272597 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
class-map copp-class-important-CUSTOMIZED-COPP (match-any)
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
conformed 0 bytes; action: transmit
violated 0 bytes; action: drop
```

Le **classi copp-class-l2-default e class-default** devono essere monitorate per evitare aumenti elevati, anche per i contatori conformi. Idealmente, queste due classi devono avere valori bassi per il contatore conformato e almeno nessun aumento del contatore violato.

Contatori ACL

Il comando **statistics per-entry** non è supportato per gli ACL IP o MAC usati nella mappa di classi CoPP e non ha effetto quando applicato agli ACL IP o MAC CoPP. (Non è disponibile alcun controllo CLI eseguito dal parser CLI). Per visualizzare gli accessi ACL MAC CoPP o gli accessi ACL IP su un modulo di I/O, usare il comando **show system internal access-list input entry detail**.

Di seguito è riportato un esempio:

```
!! 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]
```

Best practice per la configurazione CoPP

Di seguito sono riportati i consigli relativi alle best practice per la configurazione del protocollo CoPP:

- Utilizzare la modalità CoPP strict per impostazione predefinita.
- Il profilo Dense CoPP è consigliato quando lo chassis è completamente carico di moduli serie F2 o con più moduli serie F2 rispetto a qualsiasi altro modulo I/O.
- Si consiglia di non disattivare CoPP. Sintonizzare il CoPP predefinito, se necessario.
- Monitorare le perdite non intenzionali e aggiungere o modificare i criteri CoPP predefiniti in base al traffico previsto.
- In base al numero di FE presenti nello chassis, è possibile aumentare o ridurre le impostazioni CIR e BC per CoPP. Ciò si basa anche sul ruolo dei dispositivi nella rete, sui protocolli in esecuzione e così via.
- Poiché i modelli di traffico in un **centro dati** cambiano costantemente, la personalizzazione di un CoPP è un processo costante.
- CoPP e VDC: Tutte le porte dello stesso FE devono appartenere allo stesso VDC, il che è facile per un LC serie F2, ma non per un LC serie M2 o M108. Infatti, la condivisione di risorse

CoPP tra VDC è possibile se le porte dello stesso FE appartengono a VDC diversi (serie M1 o LC serie M2). Le porte di un FE, anche in controller di dominio virtuali diversi, vengono conteggiate sulla stessa soglia per il CoPP.

- La configurazione del fattore di scala è consigliata quando uno chassis è caricato sia con moduli serie F2 che serie M.

Best practice per il monitoraggio CoPP

Di seguito sono riportate alcune raccomandazioni relative alle procedure ottimali per il monitoraggio del CoPP:

- Configurare una soglia dei messaggi syslog per CoPP (Cisco NX-OS release 5.1) per monitorare le cadute imposte da CoPP.
- I messaggi syslog vengono generati se le interruzioni all'interno di una classe di traffico superano la soglia configurata dall'utente.
- La soglia e il livello di registrazione possono essere personalizzati all'interno di ciascuna classe di traffico con il comando **logging drop threshold <packet-count> level<level>**.
- Poiché l'opzione "statistics per-entry" (Statistiche per voce) per ACL MAC CoPP o ACL IP non è supportata, usare il comando **show system internal access-list input entry det** per monitorare gli accessi alle voci di controllo dell'accesso (ACE, Access Control Entries).
- Il comando **class copp-class-l2-default e class-default** deve essere monitorato per garantire che non si verifichino aumenti elevati, anche per i contatori resi conformi.
- Tutte le classi devono essere monitorate in termini di pacchetti violati.
- Poiché **copp-class-critical** è di importanza vitale ma ha una politica di **drop violata**, è buona norma monitorare la frequenza dei pacchetti conformati in modo da ricevere una prima indicazione quando la classe si avvicina al momento in cui inizia la violazione. Se il contatore violato aumenta per questa classe, non significa necessariamente un avviso rosso. Piuttosto, significa che questa situazione deve essere esaminata a breve termine.
- utilizzare il comando **copp profile strict** dopo ogni aggiornamento del codice Cisco NX-OS o almeno dopo ogni aggiornamento principale del codice Cisco NX-OS; se una modifica CoPP è stata precedentemente completata, è necessario riapplicarla.

Conclusioni

- CoPP è una funzione basata su hardware che protegge il Supervisor dagli attacchi DoS.
- I LC delle serie M1, F2 e M2 supportano il protocollo CoPP. I LC della serie F1 non supportano il protocollo CoPP.

- La configurazione CoPP è simile a MQC (Modular QoS CLI).
- La configurazione e il monitoraggio CoPP vengono eseguiti solo in un VDC predefinito.
- Il protocollo CoPP BPP predefinito può essere utilizzato con le opzioni strict, moderate, lenient e dense.
- Clonare CoPP BPP in base a regole CoPP personalizzate per soddisfare requisiti di rete specifici.
- I contatori CoPP (conformati e violati in byte per mappa di classe) vengono visualizzati con il comando **show policy-map interface control-plane**.
- Il traffico ricevuto dalla CPU del modulo Supervisor è uguale al numero totale di FE moltiplicato per la velocità consentita.
- Evitare di condividere le porte di un FE tra VDC diversi.
- Seguire le best practice del programma CoPP per implementare e monitorare correttamente le funzionalità.

Funzionalità non supportate

Queste funzionalità non sono supportate:

- Policy aggregata distribuita.
- Policy di microflusso.
- Esci dal monitoraggio delle eccezioni.
- Supporto CoPP per BPDU proveniente da una porta tunnel dot1q (QinQ): Cisco Discovery Protocol (CDP), DOT1x, Spanning Tree Protocol (STP) e VLAN Trunk Protocol (VTP).