CoPP на коммутаторах Cisco Nexus серии 7000

Содержание

Введение

Этот документ описывает то, что, как, и почему Контроль уровня управления (CoPP) используется на Коммутаторах Cisco Nexus серии 7000, которые включают F1, F2, M1, и Модули Серии M2 и линейные карты (LC). Это также включает политику оптимального метода, а также как настроить политику CoPP.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с CLI операционной системы Nexus.

Используемые компоненты

Сведения в этом документе основываются на Коммутаторах Cisco Nexus серии 7000 с Модулем Supervisor 1.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

CoPP на обзоре коммутатора Cisco Nexus серии 7000

CoPP важен по отношению к функционированию сети. Атака типа отказ в обслуживании (DOS) к Контролю/Панели управления, который может быть совершен или непреднамеренно или злонамеренно, как правило, включает высокие скорости трафика тот результат в избыточном использовании CPU. Модуль супервизора проводит беспорядочное количество времени, обрабатывающее пакеты.

Примеры таких атак включают:

- Запросы эха Протокола ICMP.
- Пакеты переданы с набором **IP опций**.

Это может привести:

- Потеря сообщений поддержки активности и обновлений протокола маршрутизации.
- Заполнение очередей пакета, которое приводит к неразборчивым отбрасываниям.
- Медленные или безразличные интерактивные сеансы.

Атаки могут сокрушить устойчивость сети и доступность и привести к влияющим на бизнес выходам сети из строя.

CoPP является аппаратной функцией, которая защищает Супервизор от атак DoS. Это управляет скоростью, на которой пакетам позволяют достигнуть Супервизора. Функция CoPP смоделирована как входная политика QoS, подключенная к специальному интерфейсу, названному **уровнем управления**. Однако CoPP является характеристикой безопасности и не частью QoS. Для защиты Супервизора CoPP разделяет пакеты плоскости данных от пакетов уровня управления (Логика Исключения). Это определяет attack packet DoS от Допустимых пакетов (Классификация). CoPP обеспечивает классификацию этих пакетов:

- Прием пакетов
- Пакеты групповой адресации
- Пакеты исключения
- Пакеты перенаправления
- Широковещательный MAC + пакеты не-IP
- Широковещательный MAC + пакеты IP (См. идентификатор ошибки Cisco CSCub47533 - Пакеты в L2 Vlan (Никакой SVI) совершающий нападки CoPP),

- MAC - адрес многоадресной передачи + пакеты IP
- MAC-адрес маршрутизатора + пакеты не-IP
- Пакеты ARP

После того, как пакет классифицирован, пакет может также отмечаться и использоваться для присвоения других приоритетов на основе типа пакетов. Приспособьте, превысьте, и действия нарушения (передача, отбрасывание, скидка с цены) могут быть установлены. Если никакой ограничитель не присоединен к классу, то ограничитель по умолчанию добавлен, чье действие согласования является отбрасыванием. Подобранные пакеты охраняются с классом по умолчанию. Одна скорость, два цвета и две скорости, три цветного применения политик поддерживается.

Трафик, который поражает ЦП в Модуль супервизора, может войти через четыре пути:

1. Внутриполосные интерфейсы (порт лицевой панели) для трафика передали с методической точностью карты.

2. Интерфейс управления (mgmt0) используемый для трафика управления.

3. Control и Monitoring Processor (CMP) интерфейс используется для консоли.

4. Коммутируемый Ethernet Канал Полосы (EOBC) для управления линейными картами от Модуля супервизора и обменных сообщений о статусе.

Только трафик, передаваемый через Внутриполосный интерфейс, подвергается CoPP, потому что это - единственный трафик, который достигает Модуля супервизора через механизмы пересылки (FE) на линейных картах. Реализация Коммутатора Cisco Nexus серии 7000 CoPP является аппаратной только, что означает, что CoPP не выполнен в программном обеспечении Модулем супервизора. Функциональность CoPP (применение политик) внедрена на каждом FE независимо. Когда различные скорости настроены для CoPP policy-map, рассмотрение должно быть взято в отношении карт числа линий в системе.

Общий трафик, полученный Supervisor I N времена X, где N является количеством FE в системе Nexus 7000, и X, является скоростью, обеспечил отдельный класс. Настроенные значения ограничителя применяются на на основание FE, и совокупный трафик, склонный для удара ЦП, является суммой которому приспосабливают и передаваемого трафика на всех FE. Другими словами, трафик, который поражает ЦП, равняется настроенному, приспосабливают скорости, умноженной на количество FE.

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

Конфигурация CoPP только внедрена в контексте виртуального устройства (VDC) по умолчанию; однако, политика CoPP применима для всех VDC. Та же глобальная политика применена для всех линейных карт. Если порты тех же FE принадлежат другим VDC (LC Серии M2 или Серии M1), CoPP применяет распределение ресурсов между VDC. Например,

порты одного FE, даже в других VDC, говорят против того же порога для CoPP.

Если тот же FE разделен между другими VDC, и данный класс трафика уровня управления превышает порог, это влияет на все VDC на том же FE. Рекомендуется выделить один FE на B постоянного тока для изоляции осуществления CoPP, если это возможно.

Когда коммутатор подходит первоначально, политика по умолчанию должна быть запрограммирована для защиты **уровня управления**. CoPP предоставляет политику по умолчанию, которая применена к **уровню управления** как часть последовательности начального запуска.

Почему CoPP на коммутаторе Cisco Nexus серии 7000

Коммутатор Cisco Nexus серии 7000 развернут как агрегация или основной коммутатор. Следовательно, это - ухо и мозг сети. Это обрабатывает максимальную загрузку в сети. Это должно обработать частый и пакетные запросы. Некоторые запросы включают:

- **Обработка Блока данных протокола моста (BPDU) Связующего дерева** - По умолчанию каждые две секунды.
- **Первое Резервирование переходов** - Это включает Протокол HSRP, Протокол VRRP и протокол распределения нагрузки для шлюзов (GLBP) - По умолчанию каждые три секунды.
- **Определение адресов** - Это включает протокол разрешения адресов/Neighbor-Discovery (ARP/ND), Glean Базы данных переадресации (FIB) - До одного запроса в секунду, на хост, такой как группировка Network Interface Controller (NIC).
- **Протокол управления динамическими узлами (DHCP) (DHCP)** - Запрос DHCP, Реле - До одного запроса в секунду, на хост.
- **Протоколы маршрутизации** для уровня 3 (L3).
- **Межсоединение ЦОД** - Виртуализация транспорта наложения (OTV), многопротокольная коммутация по меткам (MPLS) и служба виртуальной локальной частной сети (VPLS).

CoPP важен для защиты ЦП против серверов неверна настроенного или потенциальных атак DoS, который позволяет ЦП иметь достаточно цикла для обрабатывания важных сообщений уровня управления.

Обработка уровня управления на коммутаторе Cisco Nexus серии 7000

Коммутатор Cisco Nexus серии 7000 проявляет подход плоскости распределенного управления. Это имеет многоядерное на каждом Модуле i/o, а также многоядерное для уровня управления коммутатора на Модуле супервизора. Это разгружает интенсивные задачи к ЦП Модуля i/o для программирования FIB и списков контроля доступа (ACL). Это масштабирует емкость уровня управления с картами числа линий. Это избегает узкого

места ЦПУ-супервизора, которое замечено в централизованном подходе. Аппаратные ограничители скорости и аппаратный CoPP защищают уровень управления от плохого или нежелательных действий.

Политика оптимальных методов CoPP

Политика оптимальных методов (BPP) CoPP была представлена в Выпуске 5.2 Cisco NX-OS. Выходные данные **команды show running-config** не отображают содержание бит/пкс CoPP. **Показ выполняет все** показы команды содержание бит/пкс CoPP.

```
----------------------------------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 предоставляет четыре возможности пользователю для политики по умолчанию:

- Строгий
- Умеренный
- Снисходительный
- Плотный (представленный в выпуске 6.0 (1))

Если никакая опция не выбрана или, если установлено пропущена, то строгое применение политик применено. Все эти опции используют те же карты классов и классы, но другие значения (bc) количества Committedinformation rate (CIR) (гарантированная скорость передачи) и Пакета для применения политик. В версиях Cisco NX-OS ранее, чем 5.2.1, команда **настройки** использовалась для изменения опции. Выпуск 5.2.1 Cisco NX-OS представил усовершенствование бит/пкс CoPP так, чтобы опция могла быть изменена без команды **настройки**; используйте команду **профиля 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
```

Используйте **показ copp** команда **<profile-type> профиля** для просмотра конфигурации бит/пкс CoPP по умолчанию. Используйте **команду show copp status**, чтобы проверить, что

политика CoPP была применена правильно.

```
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
```

Для просмотра различия между двумя CoPP BPPs используйте **показ copp diff профиль <протип файла 1>** команда **<profile-type 2> профиля**:

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

Как настроить политику CoPP

Пользователи могут создать специализированную политику CoPP. Клонируйте бит/пкс CoPP по умолчанию и подключите его к интерфейсу **уровня управления**, потому что бит/пкс CoPP только для чтения.

```
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.
```

Профиль копии copp <протип файла> <префиксная> [суффиксная] команда создает клон бит/пкс CoPP. Это используется для изменения конфигураций по умолчанию. Команда **профиля копии copp** является командой **режима EXEC**. Пользователь может выбрать префикс или суффикс для access-list, карт классов и названия policy-map. Например, **copp-system-p-policy-strict** изменен для **[снабжения префиксом] copp-policy-strict [суффикс]**. Клонированные конфигурации рассматриваются как пользовательские конфигурации и включены в **выходные данные 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#
```

Возможно отметить трафик, который превышает и нарушает указанную Разрешенную скорость передачи данных (PIR) с этими командами:

```
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)#
```

Примените специализированную политику CoPP к глобальному интерфейсному **уровню управления**. Используйте **команду show copp status**, чтобы проверить, что политика CoPP была применена правильно.

```
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
```

Специализированный пример практического применения политики CoPP

В этом разделе описываются реальный пример, в котором клиент требует множественных устройств мониторинга для частого прозванивания локальных интерфейсов. Когда клиент хочет модифицировать политику CoPP чтобы к, с трудностью встречаются в этом сценарии:

- Увеличьте CIR так, чтобы эти точные адреса могли пропинговать локальное устройство

и не нарушить политику.

- Позвольте другим IP-адресам поддерживать способность пропинговать локальное устройство, но в более низком CIR для целей устранения проблем.

Решение показывают в следующем примере, который должен создать специализированную политику с отдельным class-map. Отдельный class-map содержит указанные IP - адреса устройств мониторинга, и class-map имеет более высокий CIR. Это также оставляет исходный *мониторинг* class-map, который перехватывает трафик ICMP для всех других IP-адресов в более низком CIR.

```
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
```

Структура данных CoPP

Структура данных бит/пкс CoPP создана как:

- **Конфигурация списков управления доступом (ACL)**: ACL IP и ACL MAC.
- **Конфигурация классификатора**: Class-map соответствующий ACL IP или ACL MAC.
- **Конфигурация ограничителя скорости**: CIR Набора, BC, действие согласования и действие нарушения. Ограничитель имеет две скорости (CIR и BC), и два цвета (приспособьте и нарушьте).

```
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
```

Масштабный коэффициент CoPP

Конфигурация масштабного коэффициента, представленная в Выпуске 6.0 Cisco NX-OS, используется для масштабирования скорости ограничителя прикладной политики CoPP для

карты частичного канала. Это увеличивает или уменьшает скорость ограничителя для карты частичного канала, но не изменяет текущую политику CoPP. Изменения сразу являются эффективными, и нет никакой потребности повторно применить политику 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
```

Мониторинг CoPP и менеджмент

С Выпуском 5.1 Cisco NX-OS возможно настроить порог отбрасывания на имя класса CoPP, которое инициирует Сообщение системного журнала в конечном счете, порог превышен. Команда **регистрирует порог отбрасывания <отброшенное количество байтов> уровень <уровень регистрации>**.

```
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
```

Вот пример Сообщения системного журнала:

```
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
```

Счетчики CoPP

CoPP поддерживает того же QoS statistics как любой другой интерфейс. Это показывает статистику классов, которые формируют политику обслуживания для каждого Модуля i/o, который поддерживает CoPP. Используйте **команду show policy-map interface control-plane** для просмотра статистики для CoPP.

> **Примечание:** Все классы должны быть проверены с точки зрения нарушенных пакетов.

```
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
```

Для получения составного представления которым приспосабливают и нарушенных счетчиков для всего class-map и Модулей i/o, используйте **уровень управления show policy-map interface | я "class|conform|violated"** команда.

```
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
```

Класс copp-class-l2-default и class-default должны быть проверены, чтобы гарантировать, что нет никаких высоких увеличений, даже для счетчиков, которым приспосабливают. Идеально, эти два класса должны иметь низкие значения для счетчика, которому приспосабливают, и по крайней мере никакого нарушенного встречного увеличения.

Счетчики ACL

Команда statistics per-entry не поддерживается для ACL IP или ACL MAC, используемого в CoPP class-map, и это не имеет никакого эффекта, когда применился к ACL MAC или CoPP IP ACL. (Нет никакой проверки CLI, сделанной Синтаксическим анализатором CLI). Для

просмотра CoPP MAC ACL или соответствий ACL IP на Модуле i/o, используйте **show system, внутренние записи ввода access-list детализируют** команду.

Например:

```
!! 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]
```

Оптимальные методы конфигурации CoPP

Это рекомендации по оптимальному использованию для конфигурации CoPP:

- Используйте строгий режим CoPP по умолчанию.
- Когда шасси полностью загружено Модулями Серии F2 или загружено большим количеством Модулей Серии F2, чем какие-либо другие Модули i/o, плотный профиль CoPP рекомендуется.
- Не рекомендуется отключить CoPP. Настройте CoPP по умолчанию по мере необходимости.
- Контролируйте непреднамеренные отбрасывания, и добавьте или модифицируйте политику CoPP по умолчанию в соответствии с ожидаемым трафиком.
- На основе количества FE в шасси CIR и BC параметры настройки для CoPP могут быть увеличены или уменьшены. Это также на основе роли устройств в сети, выполнении протоколов, и так далее.

- Поскольку структуры трафика постоянно изменяются в **ЦОД**, кастомизация CoPP является постоянным процессом.

- CoPP и VDC: Все порты того же FE должны принадлежать тому же VDC, который легок для LC Серии F2, но не как легкий для Серии M2 или M108 LC. Это вызвано тем, что распределение ресурсов CoPP между VDC, если порты того же FE принадлежат другим VDC (LC Серии M2 или Серии M1). Порты одного FE, даже в других VDC, говорят против того же порога для CoPP.

- Когда шасси загружено и Модулями Серии M и Серии F2, конфигурация масштабного коэффициента рекомендуется.

CoPP, контролирующий оптимальные методы

Это рекомендации по оптимальному использованию для мониторинга CoPP:

- Настройте порог сообщения системного журнала для CoPP (Выпуск 5.1 Cisco NX-OS) для мониторинга отбрасываний, принужденных CoPP.

- Если отбрасывания в классе трафика превышают настраиваемый порог, сообщения системного журнала генерируются.

- Порог регистрации и уровень могут быть настроены в каждом классе трафика с использованием **порога отбрасывания регистрации <количество пакетов>** команда **<level> уровня**.

- Поскольку опция "statistics per-entry" для CoPP MAC ACL или ACL IP не поддерживается, используйте **show system внутренние записи ввода access-list det** команда для мониторинга соответствий Элементов управления доступом (ACE).

- **Класс copp-class-l2-default и команда class-default** должны быть проверены, чтобы гарантировать, что нет никаких высоких увеличений, даже для счетчиков, которым приспосабливают.

- Все классы должны быть проверены с точки зрения нарушенных пакетов.

- Поскольку **copp-class-critical** очень жизненно важен, но имеет **нарушить** политику **отбрасывания**, это - полезный прием для мониторинга скорости пакетов, которым приспосабливают, для получения ранней индикации, когда класс становится близко к моменту, где это начинает нарушение. Если нарушенный счетчик увеличивается для этого класса, это не обязательно означает боевую готовность. Скорее это означает, что эта ситуация должна быть исследована в короткий срок.

- Используйте **строгую** команду **профиля copp** после каждого обновления кода Cisco NX-OS, или по крайней мере после каждого главного обновления кода Cisco NX-OS; если модификация CoPP была ранее завершена, это должно быть, повторно применил.

Заключения

- CoPP является аппаратной функцией, которая защищает Супервизор от атак DoS.
- M1, F2 и LC Серии M2 поддерживают CoPP. LC Серии F1 не поддерживают CoPP.
- Конфигурация CoPP подобна MQC (Modular QoS CLI).
- Конфигурация CoPP и мониторинг выполнены только в VDC по умолчанию.
- Бит/пкс CoPP по умолчанию может использоваться со строгими, умеренными, снисходительными, и плотными опциями.
- Клонируйте бит/пкс CoPP к специализированным правилам CoPP для соответствия с определенными требованиями к сети.
- Счетчики CoPP (приспособленный и нарушенный в байтах на class-map) отображены с **командой show policy-map interface control-plane**.
- Трафик, полученный ЦП Модуля супервизора, равняется общему числу времен FE позволенная скорость.
- Попытайтесь избежать общих портов одного FE через другие VDC.
- Примените оптимальные методы CoPP, чтобы успешно внедрить и контролировать функции.

Неподдерживаемые функции

Эти функции не поддерживаются:

- Распределенное составное применение политик.
- Управление микропотоком.
- Выходное применение политик исключения.
- CoPP поддерживают для BPDU, который прибывает из туннельного порта dot1q (QinQ): Протокол CDP, DOT1x, Протокол STP (STP) и Транкинговый протокол VLAN (VTP).