コントロール プレーン ポリシングの設定

この章の内容は、次のとおりです。

- 機能情報の確認，1 ページ
- CoPP の概要，2 ページ
- CoPP のライセンス要件，19 ページ
- CoPP の注意事項と制約事項，19 ページ
- CoPP のデフォルト設定，22 ページ
- CoPP の設定，23 ページ
- CoPP の設定の確認，34 ページ
- CoPP 設定ステータスの表示，37 ページ
- CoPP のモニタリング，38 ページ
- SNMP での CoPP のモニタリング，39 ページ
- CoPP 統計情報のクリア，39 ページ
- CoPP の設定例，40 ページ
- セットアップ ユーティリティによるデフォルト CoPP ポリシーの変更または再適用，43 ページ
- CoPP に関する追加情報，44 ページ
- CoPP の機能の履歴，45 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。こ

のモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

CoPP の概要

コントロール プレーン ポリシング（CoPP）はコントロール プレーンを保護し、それをデータ プレーンから分離することによって、ネットワークの安定性、到達可能性、およびパケット配信を保証します。

この機能により、コントロールプレーンにポリシーマップを適用できるようになります。このポリシー マップは通常の QoS ポリシーのように見え、ルータまたはレイヤ 3 スイッチの任意の IP アドレスに宛てられたすべてのトラフィックに適用されます。ネットワーク デバイスへの一般的な攻撃ベクトルは、過剰なトラフィックがデバイス インターフェイスに転送されるサービス拒絶（DoS）攻撃です。

Cisco NX-OS デバイスは、DoS 攻撃がパフォーマンスに影響しないようにするために CoPP を提供します。このような攻撃は誤って、または悪意を持って実行される場合があり、通常は、スーパーバイザ モジュールまたは CPU 自体に宛てられた大量のトラフィックが含まれます。

スーパーバイザ モジュールは、管理対象のトラフィックを次の 3 つの機能コンポーネント（プレーン）に分類します。

データ プレーン

すべてのデータ トラフィックを処理します。NX-OS デバイスの基本的な機能は、インターフェイス間でパケットを転送することです。スイッチ自身に向けられたものでないパケットは、中継パケットと呼ばれます。データ プレーンで処理されるのはこれらのパケットです。

制御プレーン

ルーティング プロトコルのすべての制御トラフィックを処理します。ボーダー ゲートウェイ プロトコル（BGP）や Open Shortest Path First（OSPF）プロトコルなどのルーティング プロトコルは、デバイス間で制御パケットを送信します。これらのパケットはルータのアドレスを宛先とし、コントロール プレーン パケットと呼ばれます。

管理プレーン

コマンドライン インターフェイス（CLI）や簡易ネットワーク管理プロトコル（SNMP）など、NX-OS デバイスを管理する目的のコンポーネントを実行します。

スーパーバイザ モジュールには、マネージメント プレーンとコントロール プレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザ モジュールの動作が途絶したり、スーパーバイザ モジュールが攻撃されたりすると、重大なネットワークの停止につながります。たとえばスーパーバイザに過剰なトラフィックが加わると、スーパーバイザ モジュールが過負荷になり、NX-OS デバイス全体のパフォーマンスが低下する可能性があります。またたとえば、スーパーバイザ モジュールに対する DoS 攻撃は、コントロール プレーンに対して非常に高速に IP トラフィック ストリームを生成することがあります。これにより、コントロー

ル プレーンは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

次に、DoS 攻撃の例を示します。

- インターネット制御メッセージ プロトコル（ICMP）エコー要求
- IP フラグメント
- TCP SYN フラッディング

これらの攻撃によりデバイスのパフォーマンスが影響を受け、次のようなマイナスの結果をもたらします。

- サービス品質の低下（音声、ビデオ、または重要なアプリケーション トラフィックの低下など）
- ルート プロセッサまたはスイッチ プロセッサの高い CPU 使用率
- ルーティング プロトコルのアップデートまたはキープアライブの消失によるルート フラップ
- 不安定なレイヤ 2 トポロジ
- CLI との低速な、または応答を返さない対話型セッション
- メモリやバッファなどのプロセッサ リソースの枯渇
- 着信パケットの無差別のドロップ

注意 コントロール プレーンの保護策を講じることで、スーパーバイザ モジュールを偶発的な攻撃や悪意ある攻撃から確実に保護することが重要です。

コントロール プレーン保護

コントロール プレーンを保護するために、Cisco NX-OS デバイスはコントロール プレーンに向かうさまざまなパケットを異なるクラスに分離します。クラスの識別が終わると、Cisco NX-OS デバイスはパケットをポリシングします。これにより、スーパーバイザ モジュールに過剰な負担がかからないようになります。

コントロール プレーンのパケット タイプ

コントロール プレーンには、次のような異なるタイプのパケットが到達します。

受信パケット

ルータの宛先アドレスを持つパケット。宛先アドレスには、レイヤ2アドレス（ルータ MAC アドレスなど）やレイヤ 3 アドレス（ルータ インターフェイスの IP アドレスなど）があります。これらのパケットには、ルータ アップデートとキープアライブ メッセージも含まれます。ルータが使用するマルチキャスト アドレス宛てに送信されるマルチキャスト パケットも、このカテゴリに入ります。

例外パケット

スーパーバイザ モジュールによる特殊な処理を必要とするパケット。たとえば、宛先アドレスが Forwarding Information Base（FIB; 転送情報ベース）に存在せず、結果としてミスとなった場合は、スーパーバイザ モジュールが送信側に到達不能パケットを返します。他には、IP オプションがセットされたパケットもあります。

リダイレクト パケット

スーパーバイザ モジュールにリダイレクトされるパケット。ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングやダイナミック アドレス解決プロトコル（ARP）インスペクションなどの機能は、パケットをスーパーバイザ モジュールにリダイレクトします。

収集パケット

宛先 IP アドレスのレイヤ 2 MAC アドレスが FIB に存在していない場合は、スーパーバイザ モジュールがパケットを受信し、ARP 要求をそのホストに送信します。

これらのさまざまなパケットはすべて、コントロール プレーンへの悪意ある攻撃に利用され、Cisco NX-OS デバイスに過剰な負荷をかける可能性があります。CoPP は、これらのパケットを異なるクラスに分類し、これらのパケットをスーパーバイザが受信する速度を個別に制御するメカニズムを提供します。

CoPP の分類

効果的に保護するために、Cisco NX-OS デバイスはスーパーバイザ モジュールに到達するパケットを分類して、パケット タイプに基づいた異なるレート制御ポリシーを適用できるようにします。たとえば、Hello メッセージなどのプロトコル パケットには厳格さを緩め、IP オプションがセットされているためにスーパーバイザ モジュールに送信されるパケットには厳格さを強めることが考えられます。

レート制御メカニズム

パケットの分類が終わると、Cisco NX-OS デバイスにはスーパーバイザ モジュールに到達するパケットのレートを制御するメカニズムがあります。スーパーバイザ モジュールへのトラフィックのレート制御には 2 つのメカニズムを使用します。1 つはポリシング、もう 1 つはレート制限と呼ばれるものです。

ハードウェア ポリサーを使用すると、トラフィックが所定の条件に一致する場合、超過する場合、または違反する場合のそれぞれについて異なるアクションを定義できます。このアクションには、パケットの送信、パケットのマーク付け、およびパケットのドロップがあります。

ポリシングには、次のパラメータを設定できます。

認定情報レート（CIR）

望ましい帯域幅を、ビット レート、またはリンク レートの割合として指定します。

最大情報レート（PIR）

望ましい帯域幅を、ビット レート、またはリンク レートの割合として指定します。

認定バースト（BC）

指定した時間枠内に CIR を超過する可能性があるが、スケジューリングには影響を与えないトラフィック バーストのサイズ。

拡張バースト（BE）

すべてのトラフィックが PIR に達する前に到達する可能性のあるトラフィック バーストのサイズ。

さらに、一致トラフィック、超過トラフィック、および違反トラフィックに対して、送信またはドロップなどの異なるアクションを設定できます。

ポリシング パラメータの詳細については、『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。

デフォルトのポリシング ポリシー

Cisco NX-OS デバイスの初回起動時に、DoS 攻撃からスーパーバイザ モジュールを保護するためのデフォルトの copp-system-p-policy-strict ポリシーが Cisco NX-OS ソフトウェアによりインストールされます。最初のセットアップ ユーティリティで、次のいずれかの CoPP ポリシー オプションを選択することにより、保護レベルを設定できます。

- Strict：このポリシーは、1 レート 2 カラーで BC 値が 250 ms です（ただし、この値が 1000 ms の重要なクラスは除きます）。
- Moderate：このポリシーは、1 レート 2 カラーで BC 値が 310 ms です（ただし、この値が 1250 ms の重要なクラスは除きます）。これらの値は、strict ポリシーより 25% 高く設定されています。
- Lenient：このポリシーは、1 レート 2 カラーで BC 値が 375 ms です（ただし、この値が 1500 ms の重要なクラスは除きます）。これらの値は、strict ポリシーより 50% 高く設定されています。
- Dense：このポリシーは 1 レート、2 カラーです。critical、normal、redirect、exception、undesirable、l2-default および default クラスの BC 値は 250 ms です。important、management、normal-dhcp、normal-dhcp-relay-response、および monitoring クラスの BC 値は 1000 ms です。l2-unpoliced クラスの BC 値は 5 MB です。

（注） シャーシが F2 シリーズ モジュールを満載している場合や、他の I/O モジュールよりも多くの F2 シリーズ モジュールを搭載している場合は、このデフォルト ポリシーを推奨します。

- Skip：コントロール プレーン ポリシーは適用されません。Cisco NX-OS の 5.2 以前のリリースでは、このオプション名は none です。

オプションを選択しなかった場合や、セットアップ ユーティリティを実行しなかった場合には、strict ポリシングが適用されます。strict ポリシーから開始し、必要に応じて、CoPP ポリシーを変更することを推奨します。

copp-system-p-policy ポリシーには、基本的なデバイス操作に最も適した値が設定されています。使用する DoS に対する保護要件に適合するよう、特定のクラスやアクセス コントロール リスト（ACL）を追加する必要があります。デフォルト CoPP ポリシーは Cisco NX-OS ソフトウェアをアップグレードしても変更されません。

注意 **skip** オプションを選択し、続いて CoPP 保護も設定しない場合、Cisco NX-OS デバイスは DoS 攻撃に対して脆弱な状態になります。

Cisco NX-OS リリース 5.2 以降のリリースでは、CLI プロンプトから **setup** コマンドを実行して再度セットアップ ユーティリティを起動する、または**copp profile** コマンドを使用して、CoPP のデフォルト ポリシーを再割り当てできます。

デフォルト クラス マップ

（注） ここで提供されるクラス マップは Cisco NX-OS リリース 6.2(2) 向けです。値の一部は、以前のリリースによって異なる場合があります。

copp-system-class-exception クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-exception
    match exception ip option
    match exception ip icmp unreachable
    match exception ipv6 option
    match exception ipv6 icmp unreachable
```

copp-system-class-critical クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-igmp
    permit igmp any 224.0.0.0/3

ip access-list copp-system-p-acl-lisp
    permit udp any any eq 4342

ip access-list copp-system-p-acl-msdp
    permit tcp any gt 1024 any eq 639
    permit tcp any eq 639 any gt 1024
```

```
ip access-list copp-system-p-acl-bgp
    permit tcp any gt 1024 any eq bgp
    permit tcp any eq bgp any gt 1024

ip access-list copp-system-p-acl-eigrp
    permit eigrp any any

ip access-list copp-system-p-acl-lisp6
    permit udp any any eq 4342

ip access-list copp-system-p-acl-rip
    permit udp any 224.0.0.0/24 eq rip

ip access-list copp-system-p-acl-ospf
    permit ospf any any

ip access-list copp-system-p-acl-pim
    permit pim any 224.0.0.0/24


    permit udp any any eq 496
    permit ip any 224.0.0.13/32

ipv6 access-list copp-system-p-acl-bgp6
    permit tcp any gt 1024 any eq bgp
    permit tcp any eq bgp any gt 1024

ipv6 access-list copp-system-p-acl-ospf6
    permit 89 any any

ipv6 access-list copp-system-p-acl-pim6
    permit 103 any FF02::D/128
    permit udp any any eq pim-auto-rp

ipv6 access-list copp-system-p-acl-rip6
    permit udp any ff02::9/64 eq 521

ip access-list copp-system-p-acl-vpc
    permit udp any any eq 3200

ip access-list copp-system-p-acl-mpls-ldp
    permit udp any eq 646 any eq 646
    permit tcp any any eq 646
    permit tcp any eq 646 any

ip access-list copp-system-p-acl-mpls-oam
    permit udp any eq 3503 any

ip access-list copp-system-p-acl-mpls-rsvp
    permit 46 any any

ip access-list copp-system-p-acl-otv-as
    permit udp any any eq 8472

mac access-list copp-system-p-acl-mac-l2pt
  permit any 0100.0ccd.cdd0 0000.0000.0000

mac access-list copp-system-p-acl-mac-otv-isis
  permit any 0100.0cdf.dfdf 0000.0000.0000

mac access-list copp-system-p-acl-mac-fabricpath-isis
  permit any 0180.c200.0041 0000.0000.0000

mac access-list copp-system-p-acl-mac-l3-isis
    permit any 0180.c200.0015 0000.0000.0000
    permit any 0180.c200.0014.0000.0000.0000

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-rip
    match access-group name copp-system-p-acl-vpc
    match access-group name copp-system-p-acl-bgp6
    match access-group name copp-system-p-acl-lisp
```

```
    match access-group name copp-system-p-acl-ospf
    match access-group name copp-system-p-acl-rip6
    match access-group name copp-system-p-acl-eigrp
    match access-group name copp-system-p-acl-lisp6
    match access-group name copp-system-p-acl-ospf6
    match access-group name copp-system-p-acl-eigrp6
    match access-group name copp-system-p-acl-otv-as
    match access-group name copp-system-p-acl-mac-l2pt
    match access-group name copp-system-p-acl-mpls-ldp
    match access-group name copp-system-p-acl-mpls-oam
    match access-group name copp-system-p-acl-mpls-rsvp
    match access-group name copp-system-p-acl-mac-l3-isis
    match access-group name copp-system-p-acl-mac-otv-isis
    match access-group name copp-system-p-acl-mac-fabricpath-isis
    match protocol mpls router-alert
    match protocol mpls exp 6
```

（注） LISP、LISP6 および MAC レイヤ 3 IS-IS ACL が、Cisco NX-OS リリース 6.1 で追加されました。

copp-system-class-important クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-hsrp
    permit udp any 224.0.0.2/32 eq 1985
    permit udp any 224.0.0.102/32 eq 1985
```

（注） Cisco NX-OS リリース 6.2(2) 以降では、HSRP 制御パケットは、前述のように、既定の宛先アドレスを使用します。6.2(2) 以前の Cisco NX-OS リリースでは、ホットスタンバイ ルータ プロトコル（HSRP）ACL には、次の設定に示すように、最後のオクテットが無視された lenient エントリがあります。

```
ip access-list copp-system-p-acl-hsrp
    permit udp any 224.0.0.0/24 eq 1985
```

```
ipv6 access-list copp-system-p-acl-hsrp6
    permit udp any ff02::66/128 eq 2029

ip access-list copp-system-p-acl-vrrp

    permit ip any 224.0.0.18/32

ip access-list copp-system-p-acl-glbp
    permit udp any eq 3222 224.0.0.0/24 eq 3222

ip access-list copp-system-p-acl-pim-reg
    permit pim any any

ipv6 access-list copp-system-p-acl-icmp6-msgs
    permit icmp any any router-advertisement
    permit icmp any any router-solicitation
    permit icmp any any nd-na
    permit icmp any any nd-ns
    permit icmp any any mld-query
    permit icmp any any mld-report
    permit icmp any any mld-reduction
    permit icmp any any 143

ip access-list copp-system-p-acl-cts
    permit tcp any any eq 64999
    permit tcp any eq 64999 any

ip access-list copp-system-p-acl-pim-mdt-join
    permit udp any 224.0.0.13/32

ipv6 access-list copp-system-p-acl-vrrp6
```

```
    permit ipv6 any ff02::12/128

ip access-list copp-system-p-acl-wccp

    permit udp any eq 2048 any eq 2048

mac access-list copp-system-p-acl-mac-lldp
  permit any 0180.c200.000c 0000.0000.0000 0x88cc

mac access-list copp-system-p-acl-mac-flow-control
  permit any 0180.c200.0001 0000.0000.0000 0x8808

class-map type control-plane match-any copp-system-p-class-important
    match access-group name copp-system-p-acl-cts
    match access-group name copp-system-p-acl-glbp
    match access-group name copp-system-p-acl-hsrp
    match access-group name copp-system-p-acl-vrrp
    match access-group name copp-system-p-acl-wccp
    match access-group name copp-system-p-acl-hsrp6
    match access-group name copp-system-p-acl-vrrp6
    match access-group name copp-system-p-acl-mac-lldp
    match access-group name copp-system-p-acl-mac-flow-control
```

（注） 「permit icmp any any 143」ルールが Cisco NX-OS リリース 6.1 の MLDv2 レポートをサポートするために acl-icmp6-msgs ACL に追加されました。

（注） VRRP6 ACL が Cisco NX-OS リリース 6.2(2) で追加されました。

（注） Cisco NX-OS リリース 6.2(2) 以降では、マルチキャスト トラフィックの動作が、異なるクラスにおいて異なるレートでポリシングされることから、次のようにマルチキャスト トラフィックのタイプによって 3 つのクラス（マルチキャスト ホスト、マルチキャスト ルータ、標準）にグループ化され、一定のレートでポリシングされるように変更されました。

```
ip access-list copp-system-p-acl-igmp
  permit igmp any 224.0.0.0/3
ipv6 access-list copp-system-p-acl-mld
  permit icmp any any mld-query
  permit icmp any any mld-report
  permit icmp any any mld-reduction
  permit icmp any any 143
ip access-list copp-system-p-acl-msdp
  permit tcp any gt 1024 any eq 639
  permit tcp any eq 639 any gt 1024
ipv6 access-list copp-system-p-acl-ndp
  permit icmp any any router-solicitation
  permit icmp any any router-advertisement
  permit icmp any any 137
  permit icmp any any nd-ns
  permit icmp any any nd-na
ip access-list copp-system-p-acl-pim
  permit pim any 224.0.0.0/24
  permit udp any any eq 496
  permit ip any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-mdt-join
  permit udp any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-reg
  permit pim any any
ipv6 access-list copp-system-p-acl-pim6
  permit pim any ff02::d/128
```

```
  permit udp any any eq 496
ipv6 access-list copp-system-p-acl-pim6-reg
  permit pim any any
mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
class-map type control-plane match-any copp-system-p-class-multicast-host
  match access-group name copp-system-p-acl-mld
  match access-group name copp-system-p-acl-igmp
class-map type control-plane match-any copp-system-p-class-multicast-router
  match access-group name copp-system-p-acl-pim
  match access-group name copp-system-p-acl-msdp
  match access-group name copp-system-p-acl-pim6
  match access-group name copp-system-p-acl-pim-reg
  match access-group name copp-system-p-acl-pim6-reg
  match access-group name copp-system-p-acl-pim-mdt-join
class-map type control-plane match-any copp-system-p-class-ndp
  match access-group name copp-system-p-acl-ndp
```

copp-system-class-management クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-tacacs
    permit tcp any any eq tacacs
    permit tcp any eq tacacs any

ip access-list copp-system-p-acl-radius
    permit udp any any eq 1812
    permit udp any any eq 1813
    permit udp any any eq 1645
    permit udp any any eq 1646
    permit udp any eq 1812 any
    permit udp any eq 1813 any
    permit udp any eq 1645 any
    permit udp any eq 1646 any

ip access-list copp-system-p-acl-ntp
    permit udp any any eq ntp

ip access-list copp-system-p-acl-ftp
    permit tcp any any eq ftp-data
    permit tcp any any eq ftp
    permit tcp any eq ftp-data any
    permit tcp any eq ftp any

ip access-list copp-system-p-acl-tftp
    permit udp any any eq tftp
    permit udp any any eq 1758
    permit udp any eq tftp any
    permit udp any eq 1758 any

ip access-list copp-system-p-acl-sftp
    permit tcp any any eq 115
    permit tcp any eq 115 any

ip access-list copp-system-p-acl-ssh
    permit tcp any any eq 22
    permit tcp any eq 22 any

ip access-list copp-system-p-acl-snmp
    permit udp any any eq snmp
    permit udp any any eq snmptrap

ip access-list copp-system-p-acl-telnet
    permit tcp any any eq telnet
    permit tcp any any eq 107
    permit tcp any eq telnet any
    permit tcp any eq 107 any

ipv6 access-list copp-system-p-acl-tacacs6
    permit tcp any any eq tacacs
    permit tcp any eq tacacs any

ipv6 access-list copp-system-p-acl-radius6
```

```
    permit udp any any eq 1812
    permit udp any any eq 1813
    permit udp any any eq 1645
    permit udp any any eq 1646
    permit udp any eq 1812 any
    permit udp any eq 1813 any
    permit udp any eq 1645 any
    permit udp any eq 1646 any

ipv6 access-list copp-system-p-acl-ntp6
    permit udp any any eq ntp
    permit udp any eq ntp any

ipv6 access-list copp-system-p-acl-tftp6
    permit udp any any eq tftp
    permit udp any any eq 1758
    permit udp any eq tftp any
    permit udp any eq 1758 any

ipv6 access-list copp-system-p-acl-ssh6
    permit tcp any any eq 22
    permit tcp any eq 22 any

ipv6 access-list copp-system-p-acl-telnet6
    permit tcp any any eq telnet
    permit tcp any any eq 107
    permit tcp any eq telnet any
    permit tcp any eq 107 any

class-map type control-plane match-any copp-system-p-class-management
    match access-group name copp-system-p-acl-tacacs
    match access-group name copp-system-p-acl-radius
    match access-group name copp-system-p-acl-ntp
    match access-group name copp-system-p-acl-ftp
    match access-group name copp-system-p-acl-tftp
    match access-group name copp-system-p-acl-sftp
    match access-group name copp-system-p-acl-ssh
    match access-group name copp-system-p-acl-snmp
    match access-group name copp-system-p-acl-telnet
    match access-group name copp-system-p-acl-tacacs6
    match access-group name copp-system-p-acl-radius6
    match access-group name copp-system-p-acl-ntp6
    match access-group name copp-system-p-acl-tftp6
    match access-group name copp-system-p-acl-ssh6
    match access-group name copp-system-p-acl-telnet6
```

copp-system-class-normal クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-dhcp
  permit udp any neq bootps any eq bootps
  permit udp any eq bootpc any

ip access-list copp-system-p-acl-dhcp-relay-response
  permit udp any eq bootps any
  permit udp any any eq bootpc

mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e

class-map type control-plane match-any copp-system-p-class-normal
   match access-group name copp-system-p-acl-mac-dot1x
   match exception multicast directly-connected-sources
   match protocol arp

class-map type control-plane match-any copp-system-p-class-normal-dhcp
  match redirect dhcp-snoop
  match access-group name copp-system-p-acl-dhcp

class-map type control-plane match-any copp-system-p-class-normal-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp-relay-response
```

copp-system-class-redirect クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-redirect
    match redirect arp-inspect
```

copp-system-class-monitoring クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-icmp
    permit icmp any any echo
    permit icmp any any echo-reply

ip access-list copp-system-p-acl-traceroute
    permit icmp any any ttl-exceeded
    permit icmp any any port-unreachable
    permit udp any any range 33434 33534

ipv6 access-list copp-system-p-acl-icmp6
    permit icmp any any echo-request
    permit icmp any any echo-reply

class-map type control-plane match-any copp-system-p-class-monitoring
    match access-group name copp-system-p-acl-icmp
    match access-group name copp-system-p-acl-traceroute
    match access-group name copp-system-p-acl-icmp6
```

copp-system-class-l2-unpoliced クラスの設定は次のとおりです。

```
mac access-list copp-system-p-acl-mac-cdp-udld-vtp
    permit any 0100.0ccc.cccc 0000.0000.0000

mac access-list copp-system-p-acl-mac-stp
    permit any 0100.0ccc.cccd 0000.0000.0000
    permit any 0180.c200.0000 0000.0000.0000

mac access-list copp-system-p-acl-mac-lacp
    permit any 0180.c200.0002 0000.0000.0000 0x8809

mac access-list copp-system-p-acl-mac-cfsoe
    permit any 0180.C200.000E 0000.0000.0000 0x8843

mac access-list copp-system-p-acl-mac-gold
    permit any any 0x3737

mac access-list copp-system-p-acl-mac-l2-tunnel
    permit any any 0x8840

class-map type control-plane copp-system-p-class-l2-unpoliced
    match access-group name copp-system-p-acl-mac-stp
    match access-group name copp-system-p-acl-mac-lacp
    match access-group name copp-system-p-acl-mac-cfsoe
    match access-group name copp-system-p-acl-mac-sdp-srp
    match access-group name copp-system-p-acl-mac-l2-tunnel
    match access-group name copp-system-p-acl-mac-cdp-udld-vtp
    match access-group name copp-system-p-acl-mac-gold
```

（注） MAC レイヤ 2 トンネル ACL が、Cisco NX-OS リリース 6.1 で追加されました。

copp-system-class-l2-default クラスの設定は次のとおりです。

```
mac access-list copp-system-p-acl-mac-undesirable
    permit any any

class-map type control-plane copp-system-p-class-l2-default
```

```
    match access-group name copp-system-p-acl-mac-undesirable
    match protocol mpls
```

copp-system-class-fcoe クラスの設定は次のとおりです。

```
mac access-list copp-system-p-acl-mac-fcoe
    permit any any 0x8906
    permit any any 0x8914

class-map type control-plane match-any copp-system-p-class-fcoe
    match access-group name copp-system-p-acl-mac-fcoe
```

（注） copp-system-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。

copp-system-class-undesirable クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-undesirable
    permit udp any any eq 1434

class-map type control-plane match-any copp-system-p-class-undesirable
    match access-group name copp-system-p-acl-undesirable
    match exception fcoe-fib-miss
```

（注） fcoe-fib-miss 一致例外が、Cisco NX-OS リリース 6.1 で追加されました。

```
mac access-list copp-system-acl-mac-cdp-udld-vtp
  permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-acl-mac-cfsoe
  permit any 0180.c200.000e 0000.0000.0000 0x8843
mac access-list copp-system-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-acl-mac-flow-control
  permit any 0180.c200.0001 0000.0000.0000 0x8808
mac access-list copp-system-acl-mac-gold
  permit any any 0x3737
mac access-list copp-system-acl-mac-l2mp-isis
  permit any 0180.c200.0015 0000.0000.0000
  permit any 0180.c200.0014 0000.0000.0000
mac access-list copp-system-acl-mac-l2pt
  permit any 0100.0ccd.cdd0 0000.0000.0000
mac access-list copp-system-acl-mac-lacp
  permit any 0180.c200.0002 0000.0000.0000 0x8809
mac access-list copp-system-acl-mac-lldp
  permit any 0180.c200.000e 0000.0000.0000 0x88c
mac access-list copp-system-acl-mac-stp
  permit any 0100.0ccc.cccd 0000.0000.0000
  permit any 0180.c200.0000 0000.0000.0000
mac access-list copp-system-acl-mac-undesirable
  permit any any
```

strict デフォルト CoPP ポリシー

Cisco NX-OS リリース 6.2(2) での strict CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-strict

    class copp-system-p-class-critical
        set cos 7
```

```
    police cir 36000 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1500 ms conform transmit violate drop

class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-normal
    set cos 1
    police cir 680 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-ndp
    set cos 6
    police cir 680 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1500 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1800 kbps bc 500 ms conform transmit violate drop

class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-exception
    set cos 1
    police cir 360 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit

class copp-system-p-class-undesirable
    set cos 0
    police cir 32 kbps bc 250 ms conform drop violate drop

class copp-system-p-class-fcoe
    set cos 6
    police cir 1060 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-l2-default
    police cir 10 kbps bc 250 ms conform transmit violate drop

class class-default
    set cos 0
    police cir 10 kbps bc 250 ms conform transmit violate drop
```

（注） copp-system-p-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。copp-system-p-class-multicast-router および copp-system-p-class-multicast-host クラスが、Cisco NX-OS リリース 6.2(2) で追加されました。

moderate デフォルト CoPP ポリシー

Cisco NX-OS リリース 6.2(2) での moderate CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-moderate

    class copp-system-p-class-critical
        set cos 7
        police cir 36000 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-important
        set cos 6
        police cir 1400 kbps bc 1250 ms conform transmit violate drop

    class copp-system-p-class-multicast-router
        set cos 6
        police cir 2600 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-management
        set cos 2
        police cir 10000 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-multicast-host
        set cos 1
        police cir 1000 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-normal
        set cos 1
        police cir 680 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-ndp
        set cos 6
        police cir 680 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp
        set cos 1
        police cir 1500 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp-relay-response
        set cos 1
        police cir 1800 kbps bc  620  ms conform transmit violate drop

    class copp-system-p-class-redirect
        set cos 1
        police cir 280 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-exception
        set cos 1
        police cir 360 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-monitoring
        set cos 1
        police cir 130 kbps bc 1250 ms conform transmit violate drop

    class copp-system-p-class-l2-unpoliced
        police cir 8 gbps bc 5 mbytes conform transmit violate transmit

    class copp-system-p-class-undesirable
        set cos 0
        police cir 32 kbps bc 310 ms conform drop violate drop

    class copp-system-p-class-fcoe
        set cos 6
        police cir 1060 kbps bc 1250 ms conform transmit violate drop

    class copp-system-p-class-l2-default
        police cir 10 kbps bc 310 ms conform transmit violate drop

    class class-default
        set cos 0
```

```
        police cir 10 kbps bc 250 ms conform transmit violate drop
```

（注） copp-system-p-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。copp-system-p-class-multicast-router および copp-system-p-class-multicast-host クラスが、Cisco NX-OS リリース 6.2(2) で追加されました。

lenient デフォルト CoPP ポリシー

Cisco NX-OS リリース 6.2(2) での lenient CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-lenient

    class copp-system-p-class-critical
        set cos 7
        police cir 36000 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-important
        set cos 6
        police cir 1400 kbps bc 1500 ms conform transmit violate drop

    class copp-system-p-class-multicast-router
        set cos 6
        police cir 2600 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-management
        set cos 2
        police cir 10000 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-multicast-host
        set cos 1
        police cir 1000 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-normal
        set cos 1
        police cir 680 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-ndp
        set cos 6
        police cir 680 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp
        set cos 1
        police cir 1500 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp-relay-response
        set cos 1
        police cir 1800 kbps bc 750 ms conform transmit violate drop

    class copp-system-p-class-redirect
        set cos 1
        police cir 280 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-exception
        set cos 1
        police cir 360 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-monitoring
        set cos 1
        police cir 130 kbps bc 1500 ms conform transmit violate drop

    class copp-system-p-class-l2-unpoliced
        police cir 8 gbps bc 5 mbytes conform transmit violate transmit

    class copp-system-p-class-undesirable
```

```
        set cos 0
        police cir 32 kbps bc 375 ms conform drop violate drop

    class copp-system-p-class-fcoe
        set cos 6
        police cir 1060 kbps bc 1500 ms conform transmit violate drop

    class copp-system-p-class-l2-default
        police cir 10 kbps bc 375 ms conform transmit violate drop

    class class-default
        set cos 0
        police cir 10 kbps bc 250 ms conform transmit violate drop
```

（注） copp-system-p-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。copp-system-p-class-multicast-router および copp-system-p-class-multicast-host クラスが、Cisco NX-OS リリース 6.2(2) で追加されました。

デンス デフォルト CoPP ポリシー

Cisco NX-OS リリース 6.2(2) でのデンス CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-critical
    set cos 7
    police cir 4500 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1500 ms conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 370 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 2500 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 190 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 300 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 300 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 660 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 800 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 200 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 200 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit
  class copp-system-p-class-undesirable
    set cos 0
    police cir 32 kbps bc 250 ms conform drop violate drop
```

```
class copp-system-p-class-fcoe
  set cos 6
  police cir 600 kbps bc 1000 ms conform transmit violate drop
class copp-system-p-class-l2-default
  police cir 10 kbps bc 250 ms conform transmit violate drop
class class-default
  set cos 0
  police cir 10 kbps bc 250 ms conform transmit violate drop
```

（注） copp-system-p-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。copp-system-p-class-multicast-router および copp-system-p-class-multicast-host クラスが、Cisco NX-OS リリース 6.2(2) で追加されました。

1 秒間あたりのパケットのクレジット制限

特定のポリシーの 1 秒間あたりのパケット（PPS）の合計（ポリシーの各クラス部分の PPS の合計）の上限は、PPS のクレジット制限（PCL）の上限になります。特定のクラスの PPS が増加して PCL 超過すると、設定が拒否されます。目的の PPS を増やすには、PCL を超える PPS の分を他のクラスから減少させる必要があります。

モジュラ QoS コマンドライン インターフェイス

CoPP は、モジュラ QoS コマンドライン インターフェイス（MQC）を使用します。MQC は CLI の構造を持っています。MQC を使用すると、トラフィック クラスの定義、トラフィック ポリシー（ポリシーマップ）の作成、およびインターフェイスへのトラフィック ポリシーの適用が可能になります。トラフィック ポリシーには、トラフィック クラスに適用する CoPP 機能を含めます。

手順の概要

1. **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。
2. **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。トラフィック ポリシー（ポリシー マップ）には、トラフィック クラスと、トラフィック クラスに適用する 1 つまたは複数の CoPP 機能を含めます。トラフィック ポリシー内の CoPP の機能で、分類されたトラフィックの処理方法が決まります。
3. **control-plane** コマンドおよび **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をコントロール プレーンに適用します。

手順の詳細

ステップ 1 **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。
次に、copp-sample-class と呼ばれる新しいマップを作成する例を示します。

```
class-map type control-plane copp-sample-class
```

ステップ 2 **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。トラフィック ポリシー（ポリシー マップ）には、トラフィック クラスと、トラフィック クラスに適用する 1 つまたは複数の CoPP 機能を含めます。トラフィック ポリシー内の CoPP の機能で、分類されたトラフィックの処理方法が決まります。

ステップ 3 **control-plane** コマンドおよび **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をコントロール プレーンに適用します。
次に、コントロール プレーンにポリシー マップを適用する例を示します。

```
control-plane
service-policy input copp-system-policy
```

（注） copp-system-policy は常に設定され、適用されます。このコマンドを明示的に使用する必要はありません。

CoPP と管理インターフェイス

Cisco NX-OS デバイスは、管理インターフェイス（mgmt0）をサポートしないハードウェア ベースの CoPP だけをサポートします。アウトオブバンド mgmt0 インターフェイスは CPU に直接接続するため、CoPP が実装されているインバンド トラフィック ハードウェアは通過しません。

mgmt0 インターフェイスで、ACL を設定して、特定タイプのトラフィックへのアクセスを許可または拒否することができます。

CoPP のバーチャライゼーション サポート

CoPP はデフォルト仮想デバイス コンテキスト（VDC）または管理者 VDC のみで設定できますが、その CoPP 設定は Cisco NX-OS デバイス上のすべての VDC に適用されます。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

CoPP のライセンス要件

この機能には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

CoPP の注意事項と制約事項

CoPP に関する注意事項と制約事項は次のとおりです。

- 最初に strict デフォルト CoPP ポリシーを使用し、後で、データセンターおよびアプリケーションの要件に基づいて CoPP ポリシーを変更することを推奨します。

- シャーシが F2 または F2e シリーズ モジュールを満載している場合や、他のタイプの I/O モジュールよりも多くの F2 または F2e シリーズ モジュールを搭載している場合は、デフォルトのデンス ポリシーを適用することを推奨します。
- シャーシが F2 または F2e と M シリーズの両方のモジュールを搭載している場合は、スケール ファクタを設定し、デフォルトのデンス ポリシーを適用することを推奨します。
- CoPP のカスタマイズは継続的なプロセスです。CoPP を設定するときには、特定の環境で使用されるプロトコルや機能に加えて、サーバ環境に必要なスーパーバイザ機能を考慮する必要があります。これらのプロトコルや機能が変更されたら、CoPP を変更する必要があります。
- CoPP を継続的にモニタすることを推奨します。ドロップが発生した場合は、CoPP がトラフィックを誤ってドロップしたのか、または誤動作や攻撃に応答してドロップしたのかを判定してください。いずれの場合も、状況を分析し、CoPP ポリシーを変更する必要を評価します。
- 他のクラスマップで指定しないトラフィックはすべて、最後のクラス（デフォルト クラス）に配置されます。このクラス内のドロップをモニタし、これらのドロップが必要のないトラフィックに基づいているのか、または設定されていないために追加が必要な機能の結果であるかどうかを調査します。
- アクセス コントロール リスト（ACL）を通してルータ プロセッサにリダイレクトする必要のあるパケット（たとえば、ARP および DHCP）を判定するために、すべてのブロードキャスト トラフィックが CoPP ロジックを通して送信されます。リダイレクトする必要のないブロードキャスト トラフィックは CoPP ロジックに対して照合され、準拠したパケットと違反したパケットの両方がハードウェア内でカウントされますが、CPU には送信されません。CPU に送信する必要のあるブロードキャスト トラフィックと、CPU に送信する必要のないブロードキャスト トラフィックを異なるクラスに分離する必要があります。
- **set cos** 設定を削除する場合、M1 シリーズ モジュールと SVI とトランク ポートがある F2/F2e シリーズ モジュール間の動作に違いがあります。M1 シリーズ モジュールでは、DSCP と UserPriority（UP）両方によって（VLAN ヘッダーで）レイヤ 3 制御パケットを受信すると、キューイングは DSCP を使用して実行されます。F2/F2e シリーズ モジュールでは、キューイングは UP を使用して実行されます。
- 5.2 より前の Cisco NX-OS リリースでは、デフォルトの copp-system-policy ポリシーを変更または再適用するにはセットアップ ユーティリティを使用する必要があります。セットアップ ユーティリティにアクセスするには、CLI で **setup** コマンドを使用します。
- CoPP を設定した後、古いクラス マップや未使用のルーティング プロトコルなど、使用されていないものはすべて削除してください。
- CoPP ポリシーによって、ルーティング プロトコルなどのクリティカルなトラフィック、またはデバイスへのインタラクティブなアクセスがフィルタリングされないように注意してください。このトラフィックをフィルタリングすると、Cisco NX-OS デバイスへのリモート アクセスが禁止され、コンソール接続が必要となる場合があります。

- Cisco NX-OS ソフトウェアは、出力 CoPP とサイレント モードをサポートしません。CoPP は、入力でのみサポートされます（コントロール プレーン インターフェイスに対して **service-policy output copp** コマンドは使用できません）。
- ハードウェアのアクセス コントロール エントリ（ACE）ヒット カウンタは、ACL 論理だけで使用できます。CPU のトラフィックを評価するには、ソフトウェアの ACE ヒット カウンタと **show access-lists** および **show policy-map type control-plane** コマンドを使用します。
- Cisco NX-OS デバイスのハードウェアは、フォワーディング エンジン単位で CoPP を実行します。CoPP は分散ポリシーをサポートしていません。したがって、レートを選択する場合は、集約トラフィックでスーパーバイザ モジュールに過剰な負荷をかけることのない値にしてください。
- スーパーバイザに到達し、CoPP によってドロップされる可能性のあるトラフィックのよりきめ細かなビューを取得するには、SVI で NetFlow 機能を使用できます。それには、ACL ヒット カウントを NetFlow テーブルに示されている値と比較します。
- F1 シリーズ モジュールでは、CoPP はサポートされません。
- Cisco NX-OS Release 5.0 では、CoPP は非 IP トラフィックの分類をサポートしていません。代わりに、ACL を使用して、スーパーバイザ モジュールに到達する非 IP トラフィックをドロップまたは制限できます。
- Cisco NX-OS Release 5.1 から、次のルールが適用されます。
  - CoPP では、非 IP および IP トラフィック クラスがサポートされます。
  - L2PT、OTV-ISIS、および FabricPath-ISIS パケットは、copp-system-class-critical ポリシーの下に分類されます。
  - LLDP およびフロー制御パケットは、copp-system-class-important ポリシーの下に分類されます。
  - Dot1x パケットは、copp-system-class-normal のポリシーの下に分類されます。
  - STP、CDP、UDLD、VTP、LACP、GOLD、および CFSoE パケットは、copp-system-class-l2-unpoliced ポリシーの下に分類されます。これらのパケットは分類されるだけで、ポリシングはされません。対応するポリサーによって、統計情報が簡単に表示されます。これらのパケットは、常にスーパーバイザに転送されます。
  - 非 IP トラフィックの残りは、copp-system-class-l2-default ポリシーの下に分類されます。
  - どの copp クラスにも一致しない IP トラフィックは、class-default ポリシーの下に分類されます。
- CoPP MAC ポリシーは、Cisco NX-OS Release 5.1 からサポートされます。
- インサービス ソフトウェア グレード（ISSU）を使用して Cisco NX-OS Release 5.1 にアップグレードする場合は、FabricPath、OTV、L2PT、LLDP、DHCP、および DOT1X の機能のデフォルト CoPP ポリシーを手動で設定する必要があります。

- Cisco NX-OS Release 5.2 から、CoPP のベスト プラクティス ポリシーは読み取り専用です。その設定を変更する場合は、それをコピーする必要があります。コピーされたポリシーは、ユーザの設定として扱われます。
- ISSU を使用して Cisco NX-OS Release 5.2 にアップグレードする場合は、コントロール プレーンにアタッチされたポリシーがユーザ設定のポリシーとして扱われます。**show copp profile** コマンドを使用して CoPP プロファイルを確認し、必要な変更を加えます。
- インサービス ソフトウェア ダウングレード（ISSD）を使用して Cisco NX-OS Release 5.2 からダウングレードする場合は、CoPP によって互換性のない設定が報告され、CoPP プロファイルをコピーするよう指示されます。それ以前のバージョンでは、すべての設定がユーザ コンフィギュレーション モードに復元されます。
- ISSD を使用せずに Cisco NX-OS Release 5.2 からダウングレードする場合、CoPP 設定は失われ、CoPP ポリシーがコントロール プレーンにアタッチされなくなります。
- ISSU を使用して新しい Cisco NX-OS リリースにアップグレードする場合、新しいリリースのデフォルト CoPP ポリシーは適用されません。独自に設定された CoPP ポリシーがあって、それを使用し続けたい可能性があるため、以前のリリースのポリシーが引き続き適用されます。ただし、以前のバージョンでデフォルトの CoPP ポリシーを変更していない場合は、Cisco NX-OS リリース 5.2 以降のリリースをインストールするときに、**copp profile** [**strict** | **moderate** | **lenient**] コマンドを使用してそのバージョンの最新のデフォルトの CoPP ポリシーを適用することを推奨します。このアクションにより、前のポリシーが削除され新しいポリシーが適用されます。
- Cisco NX-OS リリース 5.2 以降では、デフォルトの CoPP ポリシーは読み取り専用です。修正を行うには、**copp copy profile** {**strict** | **moderate** | **lenient**} {**prefix** | **suffix**} *string* を使用してデフォルトのプロファイルをコピーして、変更を行い、**service-policy input***policy-map-name* コマンドを使用してコントロール プレーンにそのポリシーを適用します。
- 複数のフローが同じクラスにマッピングされる場合、個々のフローの統計情報は使用できません。
- SNMP による CoPP のモニタリングのサポートは、リストされた cbQoSMIB テーブルとコントロール プレーンにアタッチされた要素に限定されます。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

CoPP のデフォルト設定

次の表に、CoPP パラメータのデフォルト設定を示します。

表 *1*：*CoPP* パラメータのデフォルト設定

パラメータ	デフォルト
デフォルト ポリシー	strict
デフォルト ポリシー	9 ポリシー エントリ （注） 関連するクラス マップでサポートされるポリシーの最大数は 128 です。
スケール ファクタ値	1.00

CoPP の設定

ここでは、CoPP の設定方法について説明します。

コントロール プレーン クラス マップの設定

コントロール プレーン ポリシーのコントロール プレーン クラス マップを設定する必要があります。

トラフィックを分類するには、既存の ACL に基づいてパケットを照合します。ACL キーワードの permit および deny は、照合時には無視されます。

IP バージョン 4（IPv4）および IP バージョン 6（IPv6）のパケットに対してポリシーを設定できます。

はじめる前に

デフォルト VDC にいることを確認します。

クラス マップ内で ACE ヒット カウンタを使用する場合は、IP ACL が設定してあることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **class-map type control-plane** [**match-all** | **match-any**] *class-map-name*
3. （任意） switch(config-cmap)# **match access-group name***access-list-name*
4. （任意） switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp redirect**
5. （任意） switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp unreachable**
6. （任意） switch(config-cmap)# **match exception** {**ip** | **ipv6**} **option**
7. （任意） switch(config-cmap)# **match exception** {**ip** | **ipv6**} **unicast rpf-failure**
8. switch(config-cmap)# **match protocol arp**
9. （任意） switch(config-cmap)# **match redirect arp-inspect**
10. （任意） switch(config-cmap)# **match redirect dhcp-snoop**
11. switch(config-cmap)# **exit**
12. （任意） switch(config)# **show class-map type control-plane** [*class-map-name*]
13. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **class-map type control-plane** [**match-all** | **match-any**] *class-map-name*	コントロールプレーンクラスマップを指定し、クラスマップ コンフィギュレーション モードを開始します。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。 （注） class-default、match-all、または match-any をクラス マップ名に使用できません。
ステップ 3	switch(config-cmap)# **match access-group name***access-list-name*	（任意） IP ACL のマッチングを指定します。 （注） ACL キーワードの permit および deny は、CoPP 照合時には無視されます。
ステップ 4	switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp redirect**	（任意） IPv4 または IPv6 ICMP リダイレクト例外パケットのマッチングを指定します。
ステップ 5	switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp unreachable**	（任意） IPv4 または IPv6 ICMP 到達不能例外パケットのマッチングを指定します。

	コマンドまたはアクション	目的
ステップ 6	switch(config-cmap)# **match exception** {**ip** | **ipv6**} **option**	（任意） IPv4 または IPv6 ICMP オプション例外パケットのマッチングを指定します。
ステップ 7	switch(config-cmap)# **match exception** {**ip** | **ipv6**} **unicast rpf-failure**	（任意） IPv4 または IPv6 のユニキャスト Reverse Path Forwarding（ユニキャスト RPF）例外パケットのマッチングを指定します。任意の CoPP クラス マップで、クラス マップのレート制限設定に従い、IPv4 または IPv6 の URPF 例外パケットをレート制限できます。
ステップ 8	switch(config-cmap)# **match protocol arp**	IP アドレス解決プロトコル（ARP）および逆アドレス解決プロトコル（RARP）パケットのマッチングを指定します。
ステップ 9	switch(config-cmap)# **match redirect arp-inspect**	（任意） ARP インスペクション リダイレクト パケットのマッチングを指定します。
ステップ 10	switch(config-cmap)# **match redirect dhcp-snoop**	（任意） DHCP スヌーピング リダイレクト パケットのマッチングを指定します。
ステップ 11	switch(config-cmap)# **exit**	クラスマップ コンフィギュレーション モードを終了します。
ステップ 12	switch(config)# **show class-map type control-plane** [*class-map-name*]	（任意） コントロールプレーンクラスマップの設定を表示します。
ステップ 13	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

コントロール プレーン ポリシー マップの設定

CoPP のポリシー マップを設定する必要があります。ポリシー マップにはポリシング パラメータを含めます。クラスのポリサーを設定しなかった場合、デフォルトのポリサー一致アクションは、ドロップです。Cisco NX-OS ソフトウェアは、クラスが 0 の 1 レート 2 カラー ポリシングと 2 レート 3 カラー ポリシング。

はじめる前に

デフォルト VDC にいることを確認します。

コントロール プレーン クラス マップが設定してあることを確認します。

手順の概要

1. **configure terminal**
2. **policy-map type control-plane***policy-map-name*
3. **class** {*class-map-name* [**insert-before***class-map-name2*] | **class-default**}
4. **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]}
5. **police** [**cir**] {cir-rate [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]
6. **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **conform** {**drop** | **set-cos-transmit***cos-value* | **set-dscp-transmit***dscp-value* | **set-prec-transmit***prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}]
7. **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **pir***pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]]
8. （任意） **logging drop threshold** [*drop-count* [**level** *syslog-level*]]
9. （任意） **setcos** [**inner**] *cos-value*
10. （任意） **setdscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**}
11. （任意） **set precedence** [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}
12. **exit**
13. **exit**
14. （任意） **show policy-map type control-plane** [**expand**] [**name***class-map-name*]
15. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map type control-plane***policy-map-name*
	
	例：
	`switch(config)# policy-map type control-plane ClassMapA`
	`switch(config-pmap)#`
		コントロール プレーン ポリシー マップを指定し、ポリシー マップ コンフィギュレーション モードを開始します。ポリシー マップ名は最大 64 文字で、大文字と小文字は区別されます。

	コマンドまたはアクション	目的

ステップ 3	**class** {*class-map-name* [**insert-before***class-map-name2*] | **class-default**}
	
	例：
	`switch(config-pmap)# class ClassMapA`
	`switch(config-pmap-c)#`
		コントロールプレーン クラスマップ名またはクラスデフォルトを指定し、コントロールプレーン クラス コンフィギュレーション モードを開始します。
		
		class-default クラス マップは、必ずポリシー マップのクラス マップ リストの末尾に位置します。

ステップ 4	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} 例： `switch(config-pmap-c)# police cir 52000`	認定情報レート（CIR）を指定します。レートの有効な範囲は、0 ～ 80000000000 です。CIR のデフォルト単位は bps です。
ステップ 5	**police** [**cir**] {cir-rate [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**] 例： `switch(config-pmap-c)# police cir 52000 bc 1000`	CIR と Committed 認定バースト（BC）を指定します。CIR の有効な範囲は 0 ～ 80000000000 で、BC の有効な範囲は 0 ～ 512000000 です。CIR のデフォルト単位は bps で、BC サイズのデフォルト単位は **bytes** です。
ステップ 6	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **conform** {**drop** | **set-cos-transmit***cos-value* | **set-dscp-transmit***dscp-value* | **set-prec-transmit***prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}] 例： `switch(config-pmap-c)# police cir 52000 conform transmit exceed drop`	CIR と一致アクションを指定します。CIR の有効な範囲は、0 ～ 80000000000 です。レートのデフォルト単位は bps です。*cos-value* と *prec-value* 引数の範囲は 0 ～ 7 です。*dscp-value* 引数の範囲は 0 ～ 63 です。 オプションは次のとおりです。 • **drop**：パケットをドロップします。 • **set-cos-transmit**：サービス クラス（CoS）値を設定します。 • **set-dscp-transmit**：DiffServ コード ポイント値を設定します。 • **set-prec-transmit**：優先順位値を設定します。 • **transmit**：パケットを送信します。 • **set dscp dscp table cir-markdown-map**：超過（exceed）アクションを CIR マークダウン マップに設定します。 • **set dscp dscp table pir-markdown-map**：違反（violate）アクションを PIR マークダウン マップに設定します。 （注） 同じ CIR に BC と一致（conform）アクションを指定できます。

	コマンドまたはアクション	目的
ステップ 7	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **pir***pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]] 例： `switch(config-pmap-c)# police cir 52000 pir 78000 be 2000`	CIR と最大情報レート（PIR）を指定します。CIR の有効な範囲は 0 ～ 80000000000 で、PIR の有効な範囲は 1 ～ 80000000000 です。任意で Extended 拡張バースト（BE）サイズを設定できます。BE の有効な範囲は、1 ～ 512000000 です。CIR のデフォルト単位は **bps**、PIR のデフォルト単位は bps、および BE サイズのデフォルト単位は **bytes** です。 （注） 同じ CIR に BC、一致（conform）アクション、および PIR を指定できます。
ステップ 8	**logging drop threshold** [*drop-count* [**level** *syslog-level*]] 例： `switch(config-pmap-c)# logging drop threshold 100`	（任意） ドロップされたパケットのしきい値を指定し、ドロップ数が設定したしきい値を超えた場合、Syslog を生成します。*drop-count* 引数の範囲は 1 ～ 80000000000 バイトです。*syslog-level* 引数の範囲は 1 ～ 7 であり、デフォルト レベルは 4 です。
ステップ 9	**setcos** [**inner**] *cos-value* 例： `switch(config-pmap-c)# set cos 1`	（任意） 802.1Q CoS 値を指定します。Q-in-Q 環境には **inner** キーワードを使用します。有効な範囲は 0 ～ 7 です。デフォルト値は 0 です。
ステップ 10	**setdscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**} 例： `switch(config-pmap-c)# set dscp 10`	（任意） IPv4 と IPv6 のパケットの DiffServ コード ポイント値を指定します。トンネル カプセル化を設定する場合は、**tunnel** キーワードを使用します。範囲は 0 ～ 63 です。デフォルト値は 0 です。
ステップ 11	**set precedence** [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**} 例： `switch(config-pmap-c)# set precedence 2`	（任意） IPv4 と IPv6 のパケットの優先順位値を指定します。トンネル カプセル化を設定する場合は、**tunnel** キーワードを使用します。有効な範囲は 0 ～ 7 です。デフォルト値は 0 です。

ステップ 12	**exit**
	
	例：
	`switch(config-pmap-c)# exit`
	`switch(config-pmap)#`
		ポリシー マップ クラス コンフィギュレーション モードを終了します。

ステップ 13	**exit**
	
	例：
	`switch(config-pmap)# exit`
	`switch(config)#`
		ポリシーマップ コンフィギュレーションモードを終了します。

	コマンドまたはアクション	目的
ステップ 14	**show policy-map type control-plane** [**expand**] [**name***class-map-name*] 例： `switch(config)# show policy-map type control-plane`	（任意） コントロール プレーン ポリシー マップの設定を表示します。
ステップ 15	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

コントロール プレーン サービス ポリシーの設定

CoPP サービス ポリシーに対して 1 つまたは複数のポリシー マップを設定できます。

はじめる前に

デフォルト VDC にいることを確認します。

コントロール プレーン ポリシー マップが設定してあることを確認します。

手順の概要

1. **configure terminal**
2. **control-plane**
3. **service-policy input** *policy-map-name*
4. **exit**
5. （任意） **show running-config copp** [**all**]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**control-plane**
	
	例：
	`switch(config)# control-plane`
	`switch(config-cp)#`
		コントロール プレーン コンフィギュレーション モードを開始します。

ステップ 3	**service-policy input** *policy-map-name* 例： `switch(config-cp)# service-policy input PolicyMapA`	入トラフィックのポリシーマップを指定します。ポリシーマップが複数ある場合は、このステップを繰り返します。 **no service-policy input** *policy-map-name* コマンドを使用して、コントロールプレーンからポリシーを削除します。

ステップ 4	**exit**
	
	例：
	`switch(config-cp)# exit`
	`switch(config)#`
		コントロール プレーン コンフィギュレーション モードを終了します。

ステップ 5	**show running-config copp** [**all**] 例： `switch(config)# show running-config copp`	（任意） CoPP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ラインカードごとの CoPP のスケール ファクタの設定

ラインカードごとの CoPP のスケール ファクタを設定できます。

スケール ファクタの設定は、特定のラインカードに適用された CoPP のポリシーのポリサー レートのスケーリングに使用されます。受け入れ値は 0.10 ～ 2.00 です。特定のラインカードに対して現在の CoPP ポリシーを変更せずに、ポリサー レートを増加または削減できます。変更はすぐに有効となるため、CoPP ポリシーを再適用する必要はありません。

（注） CoPP のプログラミングが各 I/O モジュールの転送エンジンで実行されます。Cisco Nexus 7000 M シリーズ I/O モジュールには 1 つまたは 2 つの転送エンジンを含むことができ、Cisco Nexus7000 F シリーズ モジュールにはモジュールに応じて 6 ~ 12 の転送エンジンを含むことができます。

M シリーズ モジュールで使用される同一の CoPP ポリシー プロファイル（ストリクト）が F シリーズ モジュールで適用される場合、F シリーズ モジュールからスーパーバイザに来るトラフィックの回数を、M シリーズ モジュールから来るトラフィックよりも多くすることができます。スーパーバイザに過剰な負荷がかかるのを回避するために、F シリーズ モジュールと、F シリーズ モジュールおよび M シリーズ モジュールの特定の組み合わせに対しデンス CoPP プロファイルを設定できます。

インストールされた I/O モジュールに基づいて、I/O モジュールごとにスケール ファクタを設定し、適切な CoPP ポリシー プロファイルを適用するには、これらのガイドラインに従ってください。

- シャーシが F シリーズ モジュールを満載している場合は、スケール ファクタの設定なしでデンス プロファイルを適用することを推奨します。
- シャーシが M シリーズ モジュールを満載している場合は、スケール ファクタの設定なしでストリクト プロファイルを適用することを推奨します。
- シャーシが M シリーズ ライン カードよりも多くの F シリーズ ライン カードを搭載している場合は、M シリーズ ライン カードにのみデンス プロファイルを適用し、スケール ファクタ値 2 を設定することを推奨します。
- シャーシが F シリーズ ライン カードよりも多くの M シリーズ ライン カードを搭載している場合は、F シリーズ ライン カードにのみストリクト プロファイルを適用し、スケール ファクタ値 0.4 を設定することを推奨します。

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. **configure terminal**
2. **control-plane**
3. **scale-factor***value***module***multiple-module-range*
4. （任意） **show running-config copp** [**all**]
5. （任意） **show policy-map interface control-plane** [**class***class-map* | **module***slot*]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**control-plane**
	
	例：
	`switch(config)# control-plane`
	`switch(config-cp)#`
		コントロールプレーンコンフィギュレーションモードを開始します。

ステップ 3	**scale-factor***value***module***multiple-module-range* 例： `switch(config-cp)# scale-factor 1.10 module 1-2`	ラインカードごとにポリサー レートを設定します。許可されたスケール ファクタ値は 0.10 ～ 2.00 です。スケール ファクタ値が設定されている場合、ポリシング値にはモジュールの対応するスケール ファクタ値が乗算され、特定のモジュールにプログラミングされます。 スケール ファクタ値をデフォルトの 1.00 に戻すには、**no scale-factor***value***module***multiple-module-range* コマンドを使用するか、**scale-factor 1 module***multiple-module-range* コマンドを使用して明示的にデフォルトのスケール ファクタ値を 1.00 に設定します。
ステップ 4	**show running-config copp** [**all**] 例： `switch(config-cp)# show running-config copp`	（任意） 実行コンフィギュレーション内の CoPP 設定を表示します。
ステップ 5	**show policy-map interface control-plane** [**class***class-map* | **module***slot*] 例： `switch(config-cp)# show policy-map interface control-plane`	（任意） CoPP ポリシーが適用される場合に適用されるスケール ファクタ値を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの CoPP ポリシーの変更または再適用

別のデフォルト CoPP ポリシーに変更したり、同じデフォルト CoPP ポリシーを再適用したりすることができます。

（注） 5.2 よりも前の Cisco NX-OS リリースでデフォルト CoPP ポリシーを変更または再適用するには、設定ユーティリティを使用する必要があります。設定ユーティリティにアクセスするには **setup** コマンドを使用します。

手順の概要

1. [**no**] **copp profile** [**strict** | **moderate** | **lenient** | **dense**]
2. （任意） **show copp status**
3. （任意） **show running-config copp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	[**no**] **copp profile** [**strict** | **moderate** | **lenient** | **dense**] 例： `switch(config)# copp profile moderate`	CoPP ベスト プラクティス ポリシーを適用します。
ステップ 2	**show copp status** 例： `switch(config)# show copp status`	（任意） 最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、CoPP ベスト プラクティス ポリシーがコントロール プレーンにアタッチされていることを確認することもできます。
ステップ 3	**show running-config copp** 例： `switch(config)# show running-config copp`	（任意） 実行コンフィギュレーション内の CoPP 設定を表示します。

CoPP ベスト プラクティス ポリシーのコピー

Cisco NX-OS Release 5.2 以降では、CoPP ベスト プラクティス ポリシーは、読み取り専用です。その設定を変更する場合は、それをコピーする必要があります。

手順の概要

1. **copp copy profile** {**strict** | **moderate** | **lenient** | **dense**} {**prefix** | **suffix**} *string*
2. （任意） **show copp status**
3. （任意） **show running-config copp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**copp copy profile** {**strict** | **moderate** | **lenient** | **dense**} {**prefix** | **suffix**} *string* 例： `switch# copp copy profile strict prefix abc`	CoPP ベスト プラクティス ポリシーのコピーを作成します。 CoPP は、指定したプレフィックスまたはサフィックスのすべてのクラス マップおよびポリシー マップの名前を変更します。
ステップ 2	**show copp status** 例： `switch# show copp status`	（任意） 最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、コピーされたポリシーがコントロール プレーンにアタッチされていないことを確認することもできます。
ステップ 3	**show running-config copp** 例： `switch# show running-config copp`	（任意） コピーされたポリシー設定を含む、実行コンフィギュレーション内の CoPP 設定を表示します。

CoPP の設定の確認

CoPP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	コントロール プレーン ポリシー マップと関連するクラス マップ、および CIR と BC の値を表示します。

コマンド	目的
show policy-map interface control-plane [**class** *class-map* | **module** *slot*]	ポリシーの値と関連するクラスマップ、およびポリシーごとまたはクラスマップごとのドロップが表示されます。また、CoPP ポリシーが適用されている場合は、スケール ファクタ値も表示されます。スケール ファクタ値がデフォルト（1.00）の場合は表示されません。 （注） スケール ファクタは各モジュールでCIR、BC、PIR、BE の値を内部的に変更しますが、その表示では設定された CIR、BC、PIR、BE の値だけが表示されます。モジュールに実際に適用される値は、スケール ファクタに設定値を掛けた値です。
show class-map type control-plane [*class-map-name*]	このクラス マップにバインドされている ACL を含め、コントロール プレーン クラス マップの設定を表示します。

コマンド	目的
show copp diff profile {**strict** | **moderate** | **lenient** | **dense**} [**prior-ver**] **profile** {**strict** | **moderate** | **lenient** | **dense**}	2 つの CoPP ベスト プラクティス ポリシーの違いを表示します。 **prior-ver** オプションを指定しない場合、このコマンドは、現在適用されている 2 つのデフォルトの CoPP のベスト プラクティス ポリシー（現在適用されている厳密なポリシーと現在適用されている中程度のポリシーなど）の差異を表示します。 **prior-ver** オプションを指定した場合、このコマンドは、現在適用されているデフォルトの CoPP ベストプラクティスポリシーと以前に適用したデフォルトの CoPP ベストプラクティスポリシーの違いを表示します（現在適用されている厳密なポリシーと以前適用した緩いポリシーなど）。
show copp profile {**strict** | **moderate** | **lenient** | **dense**}	クラスおよびポリサー値とともに、CoPP ベスト プラクティス ポリシーの詳細を表示します。
show ip access-lists [*acl-name*]	ACL を含むアクセス リストを表示します。**statistics per-entry** コマンドが使用されている場合は、特定のエントリのヒット カウントが表示されます。
show running-config aclmgr [**all**]	実行コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

コマンド	目的
show running-config copp [**all**]	実行コンフィギュレーション内の CoPP 設定を表示します。
show startup-config aclmgr [**all**]	スタートアップ コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、スタートアップコンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

CoPP 設定ステータスの表示

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. switch# **show copp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show copp status**	CoPP 機能の設定ステータスを表示します。

次に、CoPP 設定ステータスを表示する例を示します。

```
switch# show copp status
```

CoPP のモニタリング

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. switch# **show policy-map interface control-plane** [**class***class-map* | **module***slot*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show policy-map interface control-plane** [**class***class-map* | **module***slot*]	適用された CoPP ポリシーの一部であるすべてのクラスに関して、パケットレベルの統計情報を表示します。 統計情報は、OutPackets（コントロールプレーンに対して許可されたパケット）と DropPackets（レート制限によってドロップされたパケット）に関して指定します。 （注） スーパーバイザ 3 または F2e シリーズ モジュールを使用すると、このコマンドの出力でバイト数の表示にレイヤ 3 パケット長が使用されます。M1、M2、または F2 シリーズ モジュールを使用すると、コマンドの出力ではバイト数にレイヤ 2 パケット長が使用されます。

次に、CoPP をモニタする例を示します。

```
switch# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy-default

class-map copp-system-class-igmp (match-any)
match protocol igmp
police cir 1024 kbps , bc 65535 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
class-map copp-system-class-pim-hello (match-any)
match protocol pim
police cir 1024 kbps , bc 4800000 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
....
```

この例では、一致および違反したバイト数の 5 分間の移動平均およびピーク値が **show policy-map interface control-plane** コマンドの出力に表示されます。この例では、5 分間の提起レートは一致および違反したバイト数の 5 分間の移動平均、5 分間の違反レートは違反バイト数の 5 分間の移

動平均です。さらにピーク レートは、起動以降またはカウンタのリセット以降の最高値で、その発生時がタイムスタンプで示されます。

```
module 9:
    conformed 0 bytes,
        5-min offered rate 10 bytes/sec
        peak rate 12 bytes/sec at 12:29:38.654 UTC Sun Jun 30 2013
    violated 0 bytes,
        5-min violate rate 20 bytes/sec
        peak rate 22 bytes/sec at 12:26:22.652 UTC Sun Jun 30 2013
```

SNMP での CoPP のモニタリング

Cisco NX-OS Release 6.2(2) 以降、CoPP はシスコ クラスベースの QoS MIB（cbQoSMIB）をサポートします。CoPP 要素はすべて、SNMP を使用してモニタできるようになりました（ただし変更は不可）。この機能は、コントロール プレーンにアタッチされたポリシーとサブ要素（クラス、一致ルール、セットアクションなど）にのみ適用されます。コントロールプレーンで使用されていないポリシーの要素は、SNMP では見えません。

次の cbQoSMIB テーブルがサポートされます。

- ccbQosServicePolicy
- cbQosInterfacePolicy
- cbQosObjects
- cbQosPolicyMapCfg
- cbQosClassMapCfg
- cbQosMatchStmtCfg
- cbQosPoliceCfg
- cbQosSetCfg

cbQoSMIB テーブルと要素の詳細情報は、次の URL で入手可能です：

- http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.4.1.9.9.166
- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_management/7x/b_6k_System_Mgmt_Config_7x/b_6k_System_Mgmt_Config_7x_chapter_010110.html

CoPP 統計情報のクリア

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. （任意） switch# **show policy-map interface control-plane** [**class** *class-map* | **module** *slot*]
2. switch# **clear copp statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show policy-map interface control-plane** [**class** *class-map* | **module** *slot*]	（任意） 現在適用されている CoPP ポリシーおよびクラスごとの統計情報を表示します。
ステップ 2	switch# **clear copp statistics**	CoPP 統計情報をクリアします。

次に、インターフェース環境で、CoPP 統計情報をクリアする例を示します。

```
switch# show policy-map interface control-plane
switch# clear copp statistics
```

CoPP の設定例

ここでは、CoPP の設定例を示します。

CoPP Configuration Example

The following example shows how to configure CoPP using IP ACLs and MAC ACLs:

```
configure terminal
ip access-list copp-system-acl-igmp
permit igmp any 10.0.0.0/24

ip access-list copp-system-acl-msdp
permit tcp any any eq 639

mac access-list copp-system-acl-arp
permit any any 0x0806

ip access-list copp-system-acl-tacas
permit udp any any eq 49

ip access-list copp-system-acl-gre
permit 47 any any

ip access-list copp-system-acl-ntp
permit udp any 10.0.1.1/23 eq 123

ip access-list copp-system-acl-icmp
permit icmp any any

class-map type control-plane match-any copp-system-class-critical
match access-group name copp-system-acl-igmp
```

```
match access-group name copp-system-acl-msdp

class-map type control-plane match-any copp-system-class-important
match access-group name copp-system-acl-gre

class-map type control-plane match-any copp-system-class-normal
match access-group name copp-system-acl-icmp
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option
match redirect arp-inspect
match redirect dhcp-snoop

policy-map type control-plane copp-system-policy

class copp-system-class-critical
police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class copp-system-class-important
police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class copp-system-class-normal
police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class class-default
police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

control-plane
service-policy input copp-system-policy
```

The following example shows how to create the CoPP class and associate an ACL:

```
class-map type control-plane copp-arp-class
match access-group name copp-arp-acl
```

The following example shows how to add the class to the CoPP policy:

```
policy-map type control-plane copp-system-policy
class copp-arp-class
police pps 500
```

ICMP ping と ARP 要求の分割による CoPP のオーバーフローの防止

一部のサーバでは、アクティブな NIC が集約スイッチにアクセスできることを確認するために、デフォルト ゲートウェイに対する ICMP ping と ARP 要求を使用しています。その結果として CoPP 値が超過すると、CoPP はすべてのネットワークに対してトラフィックのドロップを開始します。正しく機能していないサーバが大量の ICMP ping および ARP 要求を送信すると、ある集約ブロック内にあるすべてのサーバでアクティブな NIC が失われ、NIC の切り替えが開始されます。

使用しているサーバがこのように設定されている場合は、サブネットのサブネットまたはグループに基づいて ICMP ping と ARP 要求を分割することにより、CoPP のオーバーフローを最小限に抑えることができます。その後、サーバで障害が発生して CoPP がオーバーフローした場合でも、スーパーバイザが一部のサブネットワークでのみ ICMP ping と ARP 要求に応答します。

クラスマップまたはポリシーマップの最後のエントリは、指定されていないネットワークでのすべての ICMP ping および ARP 要求を特定する必要があります。これらのカウンタが増えることは、ICMP と ARP の既存の ACL で指定されていない新しいネットワークが追加されたことを意味します。この場合は、ICMP と ARP に関連する ACL を更新する必要があります。

（注） デフォルト CoPP ごとに、ICMP ping は copp-system-p-class-monitoring に、ARP 要求は copp-system-p-class-normal に分類します。

次に、ICMP と ARP 要求を分割して、CoPP のオーバーフローを回避する例を示します。

最初に、アプリケーションの調査の結果に基づいてグループ化するネットワークを識別する新しい ACL を追加します。

```
arp access-list copp-arp-1
statistics per-entry
10 permit ip 10.1.1.0 255.255.255.0 mac any
20 permit ip 10.1.2.0 255.255.255.0 mac any
30 permit ip 10.1.3.0 255.255.255.0 mac any
arp access-list copp-arp-2
statistics per-entry
10 permit ip 10.2.1.0 255.255.255.0 mac any
20 permit ip 10.2.2.0 255.255.255.0 mac any
30 permit ip 10.2.3.0 255.255.255.0 mac any
arp access-list copp-arp-3
statistics per-entry
10 permit ip 10.3.1.0 255.255.255.0 mac any
20 permit ip 10.3.2.0 255.255.255.0 mac any
30 permit ip 10.3.3.0 255.255.255.0 mac any
...
arp access-list copp-arp-10
10 permit ip any any mac any

ip access-list copp-icmp-1
statistics per-entry
10 permit icmp 10.2.1.0 255.255.255.0 any
20 permit icmp 10.2.2.0 255.255.255.0 any
30 permit icmp 10.2.3.0 255.255.255.0 any
ip access-list copp-icmp-2
statistics per-entry
10 permit icmp 10.3.1.0 255.255.255.0 any
10 permit icmp 10.3.2.0 255.255.255.0 any
10 permit icmp 10.3.3.0 255.255.255.0 any
ip access-list copp-icmp-3
statistics per-entry
10 permit icmp 10.4.1.0 255.255.255.0 any
10 permit icmp 10.4.2.0 255.255.255.0 any
10 permit icmp 10.4.3.0 255.255.255.0 any
...
ip access-list copp-icmp-10
10 permit icmp any any
```

CoPP の新しいクラス マップにこれらの ACL を追加します。

```
class-map type control-plane match-any copp-cm-arp-1
 match access-group name copp-arp-1
class-map type control-plane match-any copp-cm-arp-2
 match access-group name copp-arp-2
class-map type control-plane match-any copp-cm-arp-3
 match access-group name copp-arp-3
...
class-map type control-plane match-any copp-cm-arp-10
 match access-group name copp-arp-10# class-map type control-plane match-any copp-cm-icmp-1

 match access-group name copp-icmp-1
class-map type control-plane match-any copp-cm-icmp-2
 match access-group name copp-icmp-2
class-map type control-plane match-any copp-cm-icmp-3
 match access-group name copp-icmp-3
...
class-map type control-plane match-any copp-cm-icmp-10
 match access-group name copp-icmp-10
```

新しいポリシーと先に作成したクラス マップを追加して、CoPP ポリシー マップを変更します。

```
policy-map type control-plane copp-system-p-policy
class copp-cm-icmp-1
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-2
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-3
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-4
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-10
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-1
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-2
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-3
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-4
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-10
      police cir X kbps bc X ms conform transmit violate drop
```

既存のクラス マップから ICMP と ARP を削除します。

```
class-map type control-plane match-any copp-system-p-class-normal
no match protocol arp

class-map type control-plane match-any copp-system-p-class-monitoring
no match access-grp name copp-system-p-acl-icmp
```

セットアップ ユーティリティによるデフォルト CoPP ポリシーの変更または再適用

セットアップ ユーティリティを使用して CoPP のデフォルト ポリシーを再適用する例を次に示します。

（注） Cisco NX-OS Release 5.2 以降では、**copp profile** コマンドを使用して、デフォルト CoPP ポリシーを変更または再適用できます。

```
switch# setup

         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.


*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.


Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

```
Do you want to enforce secure password standard (yes/no)[y]: <CR>

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]: n

  Configure read-write SNMP community string (yes/no) [n]: n

  Enter the switch name : <CR>

  Enable license grace period? (yes/no) [n]: n

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

  Configure the default gateway? (yes/no) [y]: n

  Configure advanced IP options? (yes/no) [n]: <CR>

  Enable the telnet service? (yes/no) [n]: y

  Enable the ssh service? (yes/no) [y]: <CR>

    Type of ssh key you would like to generate (dsa/rsa) : <CR>

  Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L3]: <CR>

  Configure default switchport interface state (shut/noshut) [shut]: <CR>

  Configure best practices CoPP profile (strict/moderate/lenient/dense/skip) [strict]:
strict

  Configure CMP processor on current sup (slot 6)? (yes/no) [y]: n

  Configure CMP processor on redundant sup (slot 5)? (yes/no) [y]: n

The following configuration will be applied:
  password strength-check
  no license grace-period
  no telnet server enable
  no system default switchport
  system default switchport shutdown
  policy-map type control-plane copp-system-p-policy

Would you like to edit the configuration? (yes/no) [n]: <CR>

Use this configuration and save it? (yes/no) [y]: y

switch#
```

CoPP に関する追加情報

ここでは、CoPP の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
ライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
RFC 2698	『A Two Rate Three Color Marker』

CoPP の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *2*：*CoPP* の機能の履歴

機能名	リリース	機能情報
CoPP	6.2(2)	各モジュールの各ポリシーに関する5分間移動平均と一致および違反したバイトカウントのピーク値を表示するための **show policy-map interface control-plane** コマンドの出力が更新されました。
CoPP	6.2(2)	VRRP IPv6 トラフィックをポリシングするための VRRP6 ACL サポートが追加されました。HSRP ACL は制御パケットの正しい宛先アドレスを反映するよう変更されます。
CoPP	6.2(2)	マルチキャスト トラフィックの動作が、異なるクラスにおいて異なるレートでポリシングされることから、3つのクラス（マルチキャスト ホスト、マルチキャスト ルータ、標準）にグループ化され、一定のレートでポリシングされるように変更されました。

機能名	リリース	機能情報
CoPP	6.2(2)	SNMP で CoPP をモニタする機能が追加されました。
CoPP	6.1(1)	FCoE に対する新しいクラスが追加されました。LISP、LISP6 および MAC レイヤ 3 IS-IS ACL が重要なクラスに追加されました。fcoe-fib-miss 一致例外が好ましくないクラスに追加されました。MAC レイヤ 2 トンネル ACL がレイヤ 2 非ポリシー クラスに追加されました。「permit icmp any any 143」ルールが acl-icmp6-msgs ACL に追加されました。
CoPP	6.0(1)	デンスデフォルト CoPP ポリシーが追加されました。
CoPP	6.0(1)	ラインカードごとに CoPP のスケール ファクタを設定する機能が追加されました。
CoPP	5.2(1)	設定ユーティリティを再度実行しないでデフォルト CoPP ポリシーを変更または再適用する機能が追加されました。
CoPP	5.2(1)	CoPP ベストプラクティスポリシーを読み取り専用に変更し、ポリシーを修正するためにコピーする機能が追加されました。

機能名	リリース	機能情報
CoPP	5.2(1)	CoPP ベスト プラクティス ポリシーの詳細を表示する **show copp profile** コマンドと、ポリシー間の違いを表示する **show copp diff profile** コマンドが追加されました。
CoPP	5.2(1)	実行コンフィギュレーションとスタートアップ コンフィギュレーションでユーザ設定 ACL だけを表示する（およびデフォルトの CoPP 設定 ACL を表示しない）ように、**show running-config aclmgr** コマンドと **show startup-config aclmgr** コマンドが変更されました。
CoPP	5.2(1)	**show copp status** コマンドが変更され、CoPP ベスト プラクティス ポリシーのどの部分がコントロール プレーンにアタッチされているかを表示するようになりました。
CoPP	5.2(1)	セットアップ ユーティリティで、ベスト プラクティス CoPP プロファイルの **none** オプションの名前が **skip** に変更されました。
CoPP	5.2(1)	デフォルトのクラス マップが更新され、MPLS LDP、MPLS OAM、MPLS RSVP、DHCP リレー、および OTV-AS のサポートが含まれました。

機能名	リリース	機能情報
コントロール プレーン ポリシー マップ	5.1(1)	ドロップされるパケットのしきい値を指定し、設定したしきい値をドロップ数が超えた場合に syslog を生成する機能が追加されました。
CoPP	5.1(1)	デフォルトのポリシーが更新され、802.1Q サービス クラス（cos）の値が含まれました。
CoPP	5.1(1)	非 IP トラフィック クラスのサポートが追加されました。
CoPP	5.0(2)	デフォルトのポリシーが更新され、ACL HSRP6 のサポートが含まれました。
CoPP	4.2(3)	デフォルトのポリシーが更新され、ACL DHCP のサポートが含まれました。
CoPP	4.2(1)	デフォルトのポリシーが更新され、WCCP および Cisco TrustSec のサポートが含まれました。