

Configure Control Plane Policing

This chapter describes how to configure Control Plane Policing on Cisco NX-OS devices.

- About CoPP, on page 1
- CoPP configuration guidelines, on page 15
- Default settings for CoPP, on page 20
- Configuring CoPP, on page 21
- Protocol ACL filtering added for egress CoPP, on page 28
- Copp configuration verification commands, on page 31
- Display the CoPP configuration status, on page 33
- Monitor CoPP, on page 33
- Monitoring CoPP with SNMP, on page 34
- Clear the CoPP statistics, on page 34
- Configuration examples for CoPP, on page 35
- Additional references for CoPP, on page 38

About CoPP

Control Plane Policing (CoPP) protects the control plane and separates it from the data plane, which ensures network stability, reachability, and packet delivery.

This feature allows a policy map to be applied to the control plane. This policy map looks like a normal QoS policy and is applied to all traffic entering the switch from a non-management port. A common attack vector for network devices is the denial-of-service (DoS) attack, where excessive traffic is directed at the device interfaces.

The Cisco NX-OS device provides CoPP to prevent DoS attacks from impacting performance. Such attacks, whether inadvertent or malicious, typically involve high rates of traffic directed to the supervisor module or CPU.

The supervisor module divides the traffic that it manages into three functional components or planes:

- Data plane—Handles all the data traffic. The basic functionality of a Cisco NX-OS device is to forward packets from one interface to another. The packets that are not meant for the switch itself are called the transit packets. These packets are handled by the data plane.
- Control plane—Handles all routing protocol control traffic. These protocols, such as the Border Gateway Protocol (BGP) and the Open Shortest Path First (OSPF) Protocol, send control packets between devices. These packets are destined to router addresses and are called control plane packets.

- Management plane—Runs the components meant for Cisco NX-OS device management purposes such as the command-line interface (CLI) and Simple Network Management Protocol (SNMP).

The supervisor module has both the management plane and control plane and is critical to the operation of the network. Any disruption or attacks to the supervisor module will result in serious network outages. Excessive traffic to the supervisor module could overload and slow down the performance of the entire Cisco NX-OS device. Additionally, a DoS attack on the supervisor module could generate IP traffic streams to the control plane at a very high rate. This would force the control plane to spend significant time handling these packets and prevent it from processing genuine traffic.

Examples of DoS attacks include:

- Internet Control Message Protocol (ICMP) echo requests
- IP fragments
- TCP SYN flooding

These attacks can impact the device performance and have these negative effects:

- reduced service quality (such as poor voice, video, or critical applications traffic)
- high route processor or switch processor CPU utilization
- route flaps due to loss of routing protocol updates or keepalives
- unstable Layer 2 topology
- slow or unresponsive interactive sessions with the CLI
- processor resource exhaustion, including memory and buffer depletion
- indiscriminate drops of incoming packets



Caution It is important to ensure that you protect the supervisor module from accidental or malicious attacks by configuring control plane protection.

Control plane protection

To protect the control plane, the Cisco NX-OS device segregates packets destined for the control plane into separate classes. After these classes are identified, the Cisco NX-OS device polices the packets to prevent the supervisor module from being overwhelmed.

Control plan packet types

Different types of packets can reach the control plane.

- Receive packets: packets that have the destination address of a router. The destination address can be a Layer 2 address (such as a router MAC address) or a Layer 3 address (such as the IP address of a router interface). These packets include router updates and keepalive messages. Multicast packets can also be in this category where packets are sent to multicast addresses that are used by a router.

- Exception packets: packets that need special handling by the supervisor module. For example, if a destination address is not present in the Forwarding Information Base (FIB) and results in a miss, the supervisor module sends an ICMP unreachable packet back to the sender. Another example is a packet with IP options set.

  These exceptions are possible from line cards only:

  - match exception ip option
  - match exception ipv6 option
  - match exception ttl-failure

  These exceptions are possible from fabric modules only:

  - match exception ipv6 icmp unreachable
  - match exception ip icmp unreachable

  These exceptions are possible from line cards and fabric modules:

  - match exception mtu-failure

- Redirected packets: packets that are redirected to the supervisor module.
- Glean packets: if a Layer 2 MAC address for a destination IP address is not present in the FIB, the supervisor module receives the packet and sends an ARP request to the host.

All of these different packets could be maliciously used to attack the control plane and overwhelm the Cisco NX-OS device. CoPP classifies these packets into different classes and provides a mechanism to control the rate at which the supervisor module receives each packet.

Classification for CoPP

To ensure effective protection, the device classifies packets that reach the supervisor modules. This classification allows you to apply different rate control policies based on the packet type. For example, you might be less strict with protocol packets such as Hello messages and more strict with packets sent to the supervisor module due to specific IP options. You configure packet classifications and rate control policies using class maps and policy maps.

Egress CoPP

Beginning with Cisco NX-OS Release 10.2(3)F, egress CoPP is supported on the Nexus 93180YC-FX, Nexus 93240YC-FX2, Nexus 93360YC-FX2, Nexus 9336C-FX2, Nexus 9336C-FX2-E, Nexus 93180YC-FX3, N9K-C9316D-GX, N9K-C93600CD-GX, Nexus 9364C-GX, N9K-C9332D-GX2B CloudScale switches.

Egress CoPP can be applied on top of custom/default CoPP policy.

Rate controlling mechanisms

Once the packets are classified, the device has mechanisms to control how quickly packets reach the supervisor module. The two primary mechanisms are policing and rate limiting.

Using hardware policers, you can define actions for traffic based on whether it meets specific conditions. These actions include transmitting, marking down, or dropping the packet.

You can configure these parameters for policing:

- Committed information rate (CIR): Desired bandwidth, specified as a bit rate or a percentage of the link rate.
- Committed burst (BC): Size of a traffic burst that can exceed the CIR within a given unit of time and not impact scheduling.

In addition, you can configure separate actions, such as transmit or drop, for traffic that conforms or violates policy.

For more information on policing parameters, see the *Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*.

Dynamic and static CoPP ACLs

CoPP access control lists (ACLs) are classified as either dynamic or static. Cisco Nexus 9300 and 9500 Series switches use only dynamic CoPP ACLs.

Dynamic CoPP ACLs work only for Forwarding Information Base (FIB)-based supervisor redirected packets. Static CoPP ACLs work for ACL-based supervisor redirected packets. Dynamic CoPP ACLs are supported for myIP and link-local multicast traffic. Static CoPP ACLs are supported for all other types of traffic.

Static CoPP ACLs are identified by a substring. Any ACL that has one of these substrings is categorized as a static CoPP ACL.

MAC-based static CoPP ACL substrings:

- acl-mac-cdp-udld-vtp
- acl-mac-cfsoe
- acl-mac-dot1x
- acl-mac-l2-tunnel
- acl-mac-l3-isis
- acl-mac-lacp
- acl-mac-lldp
- acl-mac-sdp-srp
- acl-mac-stp

Dynamic and static CoPP ACLs:

- acl-mac-undesirable

Protocol-based static CoPP ACL substrings:

- acl-dhcp
- acl-dhcp-relay-response
- acl-dhcp6
- acl-dhcp6-relay-response
- acl-ptp

Multicast-based static CoPP ACL substrings:

- acl-igmp

For more information on static CoPP ACLs, see CoPP configuration guidelines, on page 15 .

Default policing policies

When you start your Cisco NX-OS device for the first time, the software installs the default copp-system-p-policy-strict policy. This policy protects the supervisor module from DoS attacks. You can set the protection level by choosing a CoPP policy option from the initial setup utility:

- **Strict**—This policy is 1 rate and 2 color.
- **Moderate**—This policy is 1 rate and 2 color. The important class burst size is greater than that of the strict policy but less than that of the lenient policy.
- **Lenient**—This policy is 1 rate and 2 color. The important class burst size is greater than that of the moderate policy but less than that of the dense policy.
- **Dense**—This policy is 1 rate and 2 color. The policer CIR values are lower than those in the strict policy.
- **Skip**—No control plane policy is applied. (Cisco does not recommend using the Skip option, as it may impact the network control plane.

If you do not select an option or do not run the setup utility, the software applies strict policing. We recommend that you start with the strict policy and later modify the CoPP policies as required.

Note Strict policing is not applied by default when using POAP, so you must configure a CoPP policy.

The copp-system-p-policy policy has optimized values suitable for basic device operations. You must add specific class and access-control list (ACL) rules that meet your DoS protection requirements. The default CoPP policy does not change when you upgrade the software.

Caution If you select the skip option and do not configure CoPP protection, your Cisco NX-OS device can be vulnerable to DoS attacks.

You can reassign the default CoPP policy by runnign the **setup** command at the CLI prompt or by using the **copp profile** command.

Related Topics

Change or reapply the default CoPP policy, on page 27

Default class maps

The copp-system-class-critical class uses this configuration.

```
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-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-ospf6
  match access-group name copp-system-p-acl-eigrp6
  match access-group name copp-system-p-acl-auto-rp
  match access-group name copp-system-p-acl-mac-l3-isis
```

The copp-system-class-exception class uses this configuration.

```
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
```

The copp-system-class-exception-diag class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-exception-diag
  match exception ttl-failure
  match exception mtu-failure
```

The copp-system-class-important class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-important
  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-hsrp6
  match access-group name copp-system-p-acl-vrrp6
  match access-group name copp-system-p-acl-mac-lldp
```

The copp-system-class-l2-default class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-l2-default
  match access-group name copp-system-p-acl-mac-undesirable
```

The copp-system-class-l2-unpoliced class uses this configuration.

```
class-map type control-plane match-any 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
```

The copp-system-class-l3mc-data class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-l3mc-data
  match exception multicast rpf-failure
  match exception multicast dest-miss
```

The copp-system-class-l3uc-data class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-l3uc-data
  match exception glean
```

The copp-system-class-management class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-management
  match access-group name copp-system-p-acl-ftp
  match access-group name copp-system-p-acl-ntp
  match access-group name copp-system-p-acl-ssh
  match access-group name copp-system-p-acl-http
  match access-group name copp-system-p-acl-ntp6
  match access-group name copp-system-p-acl-sftp
  match access-group name copp-system-p-acl-snmp
  match access-group name copp-system-p-acl-ssh6
```

```
  match access-group name copp-system-p-acl-tftp
  match access-group name copp-system-p-acl-https
  match access-group name copp-system-p-acl-snmp6
  match access-group name copp-system-p-acl-tftp6
  match access-group name copp-system-p-acl-radius
  match access-group name copp-system-p-acl-tacacs
  match access-group name copp-system-p-acl-telnet
  match access-group name copp-system-p-acl-radius6
  match access-group name copp-system-p-acl-tacacs6
  match access-group name copp-system-p-acl-telnet6
```

The copp-system-class-monitoring class uses this configuration.

```
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-icmp6
  match access-group name copp-system-p-acl-traceroute
```

The copp-system-class-multicast-host class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-multicast-host
  match access-group name copp-system-p-acl-mld
```

The copp-system-class-multicast-router class uses this configuration.

```
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
```

The copp-system-class-nat-flow class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-nat-flow
  match exception nat-flow
```

The copp-system-class-ndp class uses this configuration.

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

The copp-system-class-normal class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-normal
  match access-group name copp-system-p-acl-mac-dot1x
  match protocol arp
```

The copp-system-class-normal-dhcp class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-normal-dhcp
  match access-group name copp-system-p-acl-dhcp
  match access-group name copp-system-p-acl-dhcp6
```

The copp-system-class-normal-dhcp-relay-response class uses this configuration.

```
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
  match access-group name copp-system-p-acl-dhcp6-relay-response
```

The copp-system-class-normal-igmp class uses this configuration.

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

The copp-system-class-redirect class uses this configuration.

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

The copp-system-class-undesirable class uses this configuration.

```
class-map type control-plane match-any copp-system-p-class-undesirable
  match access-group name copp-system-p-acl-undesirable
  match exception multicast sg-rpf-failure
```

The copp-system-class-fcoe class uses this configuration.

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

Strict default CoPP policy

On Nexus CloudScale switches, the strict CoPP policy has the following configuration:

```
switch#show policy-map type control-plane name copp-system-p-policy-strict
  policy-map type control-plane copp-system-p-policy-strict
    class copp-system-p-class-l3uc-data
      set cos 1
      police cir 800 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-critical
      set cos 7
      police cir 36000 kbps bc 1280000 bytes conform transmit violate drop
    class copp-system-p-class-important
      set cos 6
      police cir 2500 kbps bc 1280000 bytes conform transmit violate drop
    class copp-system-p-class-openflow
      set cos 5
      police cir 1000 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-multicast-router
      set cos 6
      police cir 2600 kbps bc 128000 bytes conform transmit violate drop
    class copp-system-p-class-multicast-host
      set cos 1
      police cir 1000 kbps bc 128000 bytes conform transmit violate drop
    class copp-system-p-class-l3mc-data
      set cos 1
      police cir 2400 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-normal
      set cos 1
      police cir 2200 kbps bc 128000 bytes conform transmit violate drop
    class copp-system-p-class-ndp
      set cos 6
      police cir 1400 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-normal-dhcp
      set cos 1
      police cir 1300 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-normal-dhcp-relay-response
      set cos 1
      police cir 1500 kbps bc 64000 bytes conform transmit violate drop
    class copp-system-p-class-normal-igmp
      set cos 3
      police cir 3000 kbps bc 64000 bytes conform transmit violate drop
    class copp-system-p-class-redirect
      set cos 1
      police cir 1800 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-exception
      set cos 1
      police cir 150 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-exception-diag
      set cos 1
      police cir 150 kbps bc 32000 bytes conform transmit violate drop
```

```
    class copp-system-p-class-management
      set cos 2
      police cir 36000 kbps bc 512000 bytes conform transmit violate drop
    class copp-system-p-class-monitoring
      set cos 1
      police cir 360 kbps bc 128000 bytes conform transmit violate drop
    class copp-system-p-class-l2-unpoliced
      set cos 7
      police cir 50 mbps bc 8192000 bytes conform transmit violate drop
    class copp-system-p-class-undesirable
      set cos 0
      police cir 200 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-fcoe
      set cos 6
      police cir 30000 kbps bc 825000 bytes conform transmit violate drop
    class copp-system-p-class-nat-flow
      set cos 7
      police cir 800 kbps bc 64000 bytes conform transmit violate drop
    class copp-system-p-class-l3mcv6-data
      set cos 1
      police cir 2400 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-undesirablev6
      set cos 0
      police cir 200 kbps bc 32000 bytes conform transmit violate drop
    class copp-system-p-class-l2-default
      set cos 0
      police cir 400 kbps bc 32000 bytes conform transmit violate drop
    class class-default
      set cos 0
      police cir 400 kbps bc 32000 bytes conform transmit violate drop
```

On Nexus Silicon One switches, the strict CoPP policy has the following configuration:

```
switch#show policy-map type control-plane name copp-system-p-policy-strict
  policy-map type control-plane copp-system-p-policy-strict
    class copp-system-p-class-l3uc-data
      set cos 1
      police cir 250 pps bc 256 packets conform transmit violate drop
    class copp-system-p-class-critical
      set cos 7
      police cir 19000 pps bc 1024 packets conform transmit violate drop
    class copp-system-p-class-important
      set cos 6
      police cir 6000 pps bc 1024 packets conform transmit violate drop
    class copp-system-p-class-openflow
      set cos 5
      police cir 2000 pps bc 256 packets conform transmit violate drop
    class copp-system-p-class-multicast-router
      set cos 6
      police cir 3000 pps bc 1024 packets conform transmit violate drop
    class copp-system-p-class-multicast-host
      set cos 1
      police cir 2000 pps bc 1024 packets conform transmit violate drop
    class copp-system-p-class-l3mc-data
      set cos 1
      police cir 3000 pps bc 1024 packets conform transmit violate drop
    class copp-system-p-class-normal
      set cos 1
      police cir 2500 pps bc 512 packets conform transmit violate drop
    class copp-system-p-class-ndp
      set cos 6
      police cir 1500 pps bc 512 packets conform transmit violate drop
    class copp-system-p-class-normal-dhcp
      set cos 1
      police cir 750 pps bc 256 packets conform transmit violate drop
```

```
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 750 pps bc 512 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 6000 pps bc 512 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 125 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 125 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 5000 pps bc 1024 packets conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 375 pps bc 1024 packets conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 64000 pps bc 16384 packets conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 125 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 1000 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 125 pps bc 256 packets conform transmit violate drop
  class copp-system-p-class-l3mcv6-data
    set cos 1
    police cir 3000 pps bc 1024 packets conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0
    police cir 125 pps bc 256 packets conform transmit violate drop
  class class-default
    set cos 0
    police cir 125 pps bc 256 packets conform transmit violate drop
```



Note The values in the examples are for reference only. Actual CoPP rates may vary based on the switches deployed.

Moderate default CoPP policy

On Cisco Nexus 9300 and 9500 Series switches, the moderate CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-p-policy-moderate
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 192 packets conform transmit violate drop
```

```
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 2000 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1500 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1500 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 300 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 400 pps bc 96 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 6000 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 300 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 20000 pps bc 8192 packets conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 15 pps bc 48 packets conform transmit violate drop
  class copp-system-p-class-fcoe
    set cos 6
    police cir 1500 pps bc 192 packets conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 100 pps bc 64 packets conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0
    police cir 50 pps bc 48 packets conform transmit violate drop
  class class-default
    set cos 0
    police cir 50 pps bc 48 packets conform transmit violate drop
```

Lenient default CoPP policy

On Cisco Nexus 9300 and 9500 Series switches, the lenient CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-p-policy-lenient
  class copp-system-p-class-l3uc-data
```

```
  set cos 1
  police cir 250 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-critical
  set cos 7
  police cir 19000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-important
  set cos 6
  police cir 3000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-multicast-router
  set cos 6
  police cir 3000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-management
  set cos 2
  police cir 3000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-multicast-host
  set cos 1
  police cir 2000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-l3mc-data
  set cos 1
  police cir 3000 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal
  set cos 1
  police cir 1500 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-ndp
  set cos 6
  police cir 1500 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 300 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 400 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 6000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 1500 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 50 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 50 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 300 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-fcoe
  set cos 6
  police cir 1500 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 50 pps bc 64 packets conform transmit violate drop
class class-default
```

```
    set cos 0
    police cir 50 pps bc 64 packets conform transmit violate drop
```

Dense default CoPP policy

On Cisco Nexus 9300 and 9500 Series switches, the dense CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 2500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 2
    police cir 1000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 1200 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 750 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 1
    police cir 750 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 150 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 2500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 50 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 20000 pps bc 8192 packets conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 15 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-fcoe
    set cos 6
```

```
  police cir 750 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop
```

Packets per second credit limit

The aggregate packets per second (PPS) for a given policy (sum of PPS of each class part of the policy) is capped by an upper PPS Credit Limit (PCL). If an increase in PPS of a given class causes a PCL exceed, the configuration is rejected. To increase the desired PPS, the additional PPS beyond PCL should be decreased from other class(es).

Modular QoS Command-Line interface

CoPP uses the Modular Quality of Service Command-Line Interface (MQC). MQC is a CLI structure that allows you to define a traffic class. You can also create a traffic policy (policy map) and attach the traffic policy to an interface. The traffic policy contains the CoPP feature, which is applied to the traffic class.

Procedure

Step 1 Define a traffic class using the **class-map** command.

Example:

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

A traffic class is used to classify traffic. This example shows how to create a new class-map called copp-sample-class:

Step 2 Create a traffic policy using the **policy-map** command.

A traffic policy (policy map) contains a traffic class and one or more CoPP features that will be applied to the traffic class. The CoPP features in the traffic policy specify how to treat the classified traffic.

Step 3 Attach the traffic policy (policy map) to the control plane using the **control-plane** and **service-policy** commands.

Example:

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

This example shows how to attach the policy map to the control plane:

Note
The copp-system-policy is always configured and applied. There is no need to use this command explicitly.

Copp and the management interface

The Cisco NX-OS device supports only hardware-based CoPP, which does not support the management interface (mgmt0). The out-of-band mgmt0 interface connects directly to the CPU and does not pass through the in-band traffic hardware where CoPP is implemented.

On the mgmt0 interface, ACLs can be configured to give or deny access to a particular type of traffic.

Related Topics

Configure IP ACLs
Configuring MAC ACLs

CoPP configuration guidelines

Use this reference to review copp configuration guidelines.

A CoPP policy is a set of configuration rules that

- manage control plane traffic by classifying and policing traffic to the CPU,
- enforce protections against unwanted or excessive control traffic, and
- ensure critical management or routing functions are preserved on the device.

CoPP has these configuration guidelines and limitations:

- We recommend that you use the strict default CoPP policy initially and then later modify the CoPP policies that are based on the data center and application requirements.
- Customizing CoPP is an ongoing process. You must configure CoPP for the protocols and features used in your environment and the supervisor features required by the server environment. As protocols and features change, modify CoPP accordingly.
- We recommend that you continuously monitor CoPP. If drops occur, determine if CoPP dropped traffic unintentionally or in response to a malfunction or attack. In either event, analyze the situation and evaluate the need to modify the CoPP policies.
- All traffic not specified in other class maps is placed in the default class. Monitor drops in this class and investigate whether they result from unwanted traffic or from a feature that needs to be configured.
- All broadcast traffic is sent through CoPP logic to determine which packets, such as ARP and DHCP, must be redirected with an access control list (ACL) to the router processor. Broadcast traffic that does not need to be redirected is matched against CoPP logic. Both conforming and violated packets are counted in the hardware but are not sent to the CPU. Broadcast traffic that must be sent to the CPU and that which does not must be separated into different classes.
- After you have configured CoPP, delete anything that is not being used, such as old class maps and unused routing protocols.
- Ensure that the CoPP policy does not filter critical traffic, such as routing protocols or interactive access. Filtering this traffic could prevent remote access and require a console connection.
- Perform CoPP policy parameter changes only during a maintenance window. Modifying the CIR or committed burst (BC) value of an existing CoPP policy class while the switch is carrying production traffic can cause a transient disruption to LACP, port-channel, and vPC operation.

Switch specific limitations

- CoPP processing comprises of 2 stages: In the first stage, the actual packet size is reused in each class policy, however when the packet enters the second stage, an internal header of 44 bytes is added. This causes an alteration in the conform or violation policies of all the CoPP classes. This limitation is applicable to Cisco Nexus 9300-FX, Nexus 9300-FX2, and 9300-GX platform switches.
- First-generation Cisco Nexus 9000 Series switches (non - FX/FX2), do not support source-based CoPP. This limitation does not exist for cloud scale ASIC-based Cisco Nexus switches.
- The **match-all** option is not supported in CoPP class-map and it always defaults to the **match-any** option.
- The Cisco NX-OS software does not support egress CoPP or silent mode. CoPP is supported only on ingress (you cannot use the **service-policy output copp** command to the control plane interface).
- Cloudscale IPv6 link-local BGP support requires carving > 512 ing-sup TCAM region (this requires a reload to take effect).
- To avoid traffic loss during traffic impact, configure the CoPP class normal CIR value to 2200 kbps on Cisco Nexus 9300 GX/FX/FX2/FX3, 9504-FM-G, and 9508-FM-G switches and X9716D-GX line cards.
- Beginning with Cisco NX-OS Release 10.3(2)F, source IP based filtering in CoPP is supported on Cisco Nexus 9504 and 9508 modular chassis with R/RX line cards.



Note For IPv6, source IP based filtering is supported up to 24b MSB.

- On the Silicon one switches, there are no IPv6-specific CoPP classes. Consequently, the existing CoPP classes (l3mc-data and undesirable) are applied to both IPv4 and IPv6 traffic.

Configuration limitations

- You can use the access control entry (ACE) hit counters in the hardware only for ACL logic. Use the software ACE hit counters and the **show access-lists** and **show policy-map type control-plane** commands to evaluate CPU traffic.
- The Cisco NX-OS device hardware performs CoPP on a per-forwarding-engine basis. CoPP does not support distributed policing. Therefore, you should choose rates so that the aggregate traffic does not overwhelm the supervisor module.
- If multiple flows map to the same class, individual flow statistics will not be available.
- You cannot disable CoPP. If you attempt to disable it, packets are rate limited at 50 packets per seconds .
- Skip CoPP policy option has been removed from the Cisco NX-OS initial setup utility because using it can impact the control plane of the network.

Static CoPP ACLs limitations

- These guidelines and limitations apply to static CoPP ACLs:
  - Static CoPP ACLs can be remapped to a different CoPP class.

- Access control entries (ACEs) cannot be modified or removed for static CoPP ACLs.
- If a CoPP ACL has a static ACL substring, it maps to that type of traffic. For example, if the ACL includes the acl-mac-stp substring, STP traffic classifies to the class map for that ACL.
- Static CoPP ACLs take priority over dynamic CoPP ACLs, regardless of their position in the CoPP policy, the order in which they are configured, and how they appear in the output of the **show policy-map type control-plane** command.
- You must have static CoPP ACLs in the CoPP policy. Otherwise, the CoPP policy is rejected.

Protocol ACL filtering feature support and limitations

- Beginning with Cisco Nexus Release 9.2(2), Cisco Nexus 9300-FX Series switches and Cisco Nexus 9500 platform switches support protocol ACL filtering. In this release, IPv6 ACL is not supported.
- Beginning with Cisco NX-OS Release 9.2(3), IPv6 ACL is supported for dynamic CoPP on the Cisco Nexus 9300-FX Series switches, and Cisco Nexus 9500 platform switches.
- The protocol ACL filtering for egress CoPP has the following limitations:
  - Once the egress CoPP ACL is defined, you cannot add or remove an existing rule. This is applicable for all class-maps and policy-maps attached to the egress CoPP ACLs.
  - You cannot override the existing egress CoPP with a new policy. You must remove the existing egress CoPP before you add a new policy.
  - The deny action is not applicable.
  - Every entry is programmed in TCAM and uses a different TCAM space if two MAC or IP ACLs with the same entries are created and bound to either the same or a different class-map.
  - The maximum TCAM carving supported for the egress CoPP is 128 entries (24 entries are reserved and the remaining 104 entries are for egress CoPP, which are all double wide), which can be any of 52 (Ipv4, mac, Ipv6) entries.
  - Policer can be used to drop the traffic completely, with cir and burst as 0.
  - SNMP MIB is not supported.

CoPP ACL feature support and limitations

- When a packet meets multiple exception conditions, CoPP matches the packet based on the order in which the CoPP ACLs are configured and matches it only against a single class. This is an expected CoPP behavior.

  Beginning with Cisco NX-OS Release 9.3(4), the UC FIB MISS exception is counted against the CoPP class (copp-system-p-class-exception). Therefore, if a packet has both, the TTL (accounted user class copp-system-p-class-exception-diag) and the UC FIM MISS exceptions, it is accounted against the UC FIB MISS exception. This behavior occurs because the order of the CoPP classes where the copp-system-p-class-exception class has an order higher than the copp-system-p-class-exception-diag class. For NX-OS releases earlier to NX-OS Release 9.3(4), the UC FIB MISS exception was not explicitly handled by the CoPP rules.

- Beginning with Cisco NX-OS Release 10.1(2), CoPP is supported on the Cisco Nexus X9624D-R2 line cards and 9508-FM-R2 switches.
- Beginning with Cisco NX-OS Release 10.1(2), CoPP is supported on the Cisco Nexus 9364D-GX2A and 9332D-GX2B switches.
- Beginning with Cisco NX-OS Release 10.4(1)F, CoPP ACL is supported on the Cisco Nexus 9332D-H2R switches.
- Beginning with Cisco NX-OS Release 10.4(2)F, CoPP ACL is supported on the Cisco Nexus 93400LD-H1, and 93108TC-FX3 switches.
- Beginning with Cisco Nexus Release 10.4(3)F, CoPP ACL is supported on the Cisco Nexus 9364C-H1 switches.
- On Cisco Nexus 9336C-SE1 switches, zero CIR is not supported under custom CoPP or hardware rate-limiter. When a user configures zero CIR, it is set to the minimum possible value in the hardware.

ISSU limitations

- If you upgrade from a Cisco NX-OS release that supports the CoPP feature to a Cisco NX-OS release that supports the CoPP feature with other classes for new protocols, you must either run the setup utility using the **setup** command or use the **copp profile** command for the new CoPP classes to be available.
- Before you downgrade from a Cisco NX-OS release that supports the CoPP feature to an earlier Cisco NX-OS release that supports the CoPP feature, you should verify compatibility using the **show incompatibility nxos bootflash:** *filename* command. If an incompatibility exists, disable any features that are incompatible with the downgrade image before downgrading the software.
- If there are changes in the CoPP profile in the target image of a non-disruptive upgrade operation, then a reload is required in the target image, post upgrade, for those changes to take effect.

Copp guidelines and limitations for Cisco Nexus 9800 series switches

- Beginning with Cisco NX-OS Release 10.3(1)F , CoPP ACL is supported on Cisco Nexus 9808 switches.
  - Beginning with Cisco NX-OS Release 10.4(1)F, CoPP ACL is supported on Cisco Nexus X98900CD-A and X9836DM-A line cards with Cisco Nexus 9808 switches.
- Beginning with Cisco NX-OS Release 10.4(1)F, CoPP ACL is supported on Cisco Nexus 9804 switches, and Cisco Nexus X98900CD-A and X9836DM-A line cards.
- Cisco Nexus 9808 /9804 switches have the following limitations for SUP CoPP ACL support:
  - Policer rate is in multiples of 161 PPS at Stage-1.
  - There is no shaper in Stage 0.
  - Stage-2 output is at LC/Module level, and Stage-3 output is at SUP/CPU level.
  - Fabrics/FMs are not involved in in-band path.
  - CoPP policy for Stage-1, Stage-2, and Stage-3 are in PPS.
  - CoPP Stage3 stats gets reset to zero after system switchover.
  - Only policer rate changes are supported in Custom CoPP.

CoPP guidelines and limitations for Cisco Nexus 9364E-SG2 switches

- Beginning with Cisco NX-OS Release 10.5(3)F, on the Cisco Nexus 9364E-SG2-Q and 9364E-SG2-O switches, Custom CoPP is supported.
- User-defined MAC access lists and source MAC addresses (SMACs) are not supported within Custom CoPP. However, MAC ACLs with well-known destination MAC addresses (DMACs) from the default profile are supported.
- All Bridge Protocol Data Units (BPDUs) are mapped to a single policer; therefore, distinct policing configurations for protocols such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and Spanning Tree Protocol (STP) are not supported.
- CoPP Consistency checker is not supported for Custom CoPP.
- Only a single burst value of 126 packets is supported.
- Destination IP match does not support IPv4 or IPv6 link-local multicast addresses.
- Custom Copp functionalities and limitations:
  - You can modify the policer rates for the copy of inbuilt classes.
  - You can create fully user-defined CoPP classes with user-defined match criteria and policer rates.
  - You can configure policer rates in packets per second (PPS) only.
  - At least one IPv4 ACL must be present in the Custom CoPP configuration.
  - You can create up to 28 class maps in a CoPP policy.
  - Custom CoPP scale limit (unidimensional) - Maximum number of TCAM entries :
    - IPv4 - 360
    - IPv6 – 180
  - IPv4 and IPv6 ACLs of link-local multicast entries like OSPF, RIP, EIGRP, and AUTO-RP should be added within the same CoPP class. Similarly, IPv4 and IPv6 ACLs for HSRP and VRRP must also be in the same CoPP class as in the default CoPP profile. Additionally, the ACL name for link-local multicast entries should include the string from the default CoPP policy, such as "acl-ospf" or "acl-eigrp".

Guidelines and limitations for CoPP on Cisco Nexus 9336C-SE1 switches

- Policer rates are specified in packets per second (PPS).
- Destination IP-based access-list matching is not supported in Custom CoPP.
- User-defined MAC access lists are not supported; only built-in MAC ACLs can be used.
- A maximum of 28 class maps can be configured under a Custom CoPP policy.
- Custom CoPP supports maximum 360 IPv4 (uni-dimensional) and 180 IPv6 (uni-dimensional) TCAM entries.
- The CoPP Consistency Checker is not supported for Custom CoPP.

- Zero Committed Information Rate (CIR) is not supported. If zero CIR is configured, the hardware sets it to the minimum possible value.

Guidelines and limitations for CoPP on Cisco N9300 smart switches

Beginning with Cisco NX-OS Release 10.6(2)F, Cisco N9324C-SE1U and Cisco N9348Y2C6D-SE1U switches support custom CoPP with these capabilities

- Policer rates are specified in packets per second (PPS).
- Destination IP-based access-list matching is not supported in Custom CoPP.
- User-defined MAC access lists are not supported; only built-in MAC ACLs can be used.
- A maximum of 28 class maps can be configured under a Custom CoPP policy.
- Custom CoPP supports maximum 360 IPv4 (uni-dimensional) and 180 IPv6 (uni-dimensional) TCAM entries.
- The CoPP Consistency Checker is not supported for Custom CoPP.
- Zero Committed Information Rate (CIR) is not supported. If zero CIR is configured, the hardware sets it to the minimum possible value.

Guidelines and limitations for CoPP on Cisco Nexus 9164E-NS4-O switches:

Beginning with Cisco NX-OS Release 10.6(2n), Cisco Nexus 9164E-NS4-O switches support CoPP with these capabilities:

- Policer rates are specified in packets per second (PPS).
- Only Committed Information Rate (CIR) and Burst Size (BC) parameters can be modified when using Custom CoPP.
- The CoPP consistency checker is not supported for Custom CoPP.
- In-band packets are not classified into high or low-priority queues based on the Class of Service (CoS) value of the CoPP class.
- Each IPv4 and IPv6 ACE is accounted as a single unit in resource utilization output.
- The output of the **show system internal access-list sup-redirect-stats** command is limited to displaying permit counts for MTU exceptions, TTL failures, FIB misses, and Glean entries.
- Configuring a CIR of zero may result in packet leakage when the **clear copp statistics** command is executed.

Default settings for CoPP

Use this reference to review the default settings for CoPP.

This table lists the default settings for CoPP parameters.

Table 1: Default CoPP parameters settings

Parameters	Default
Default policy	Strict
Default policy	9 policy entries **Note** The maximum number of supported policies with associated class maps is 128.
Scale factor value	1.00

Configuring CoPP

This section describes how to configure CoPP.

Configure a control plane class map

You must configure control plane class maps for control plane policies.

You can classify traffic by matching packets based on existing ACLs. The permit and deny ACL keywords are ignored in the matching.

You can configure policies for IP version 4 (IPv4) and IP version 6 (IPv6) packets.

Before you begin

Ensure that you have configured the IP ACLs if you want to use ACE hit counters in the class maps.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Specify a control plane class map and enters class map configuration mode.

Example:

```
switch(config)#class-map type control-plane ClassMapA
switch(config-cmap)#
```

The default class matching is match-any. The name can be a maximum of 64 characters long and is case sensitive.

Note
You cannot use class-default, match-all, or match-any as class map names.

Step 3 (Optional) Specify matching for an IP ACL.

Example:

```
switch(config-cmap)#match access-group name MyAccessList
```

Note
The permit and deny ACL keywords are ignored in the CoPP matching.

Step 4 (Optional) Specify matching for IPv4 or IPv6 ICMP redirect exception packets.

Example:

```
switch(config-cmap)#match exception ip icmp redirect
```

Step 5 (Optional) Specify matching for IPv4 or IPv6 ICMP unreachable exception packets.

Example:

```
switch(config-cmap)#match exception ip icmp unreachable
```

Step 6 (Optional) Specify matching for IPv4 or IPv6 option exception packets.

Example:

```
switch(config-cmap)#match exception ip option
```

Step 7 Specify matching for IP Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP) packets.

Example:

```
switch(config-cmap)#match protocol arp
```

Step 8 Complete the remaining control plane class map steps.

a) Exit class map configuration mode.

Example:

```
switch(config-cmap)#exit
switch(config)#
```

b) (Optional) Display the control plane class map configuration.

Example:

```
switch#show class-map type control-plane
```

c) (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Configure a control plane policy map

You must configure a policy map for CoPP, which includes policing parameters. If you do not configure a policer for a class, this default is configured:

- 50 packets per second (pps) with a burst of 32 packets (for Cisco Nexus 9300 and 9500 Series switches)
- 150 kilobits per second (kbps) with a burst of 32,000 bytes

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Specify a control plane policy map to enter policy map configuration mode.

Example:

```
switch(config)#policy-map type control-plane ClassMapA
switch(config-pmap)#
```

The policy map name can have a maximum of 64 characters and is case sensitive.

Step 3 Specify a control plane class map name or the class-default to enter control plane class configuration mode.

Example:

```
switch(config-pmap)#class ClassMapA
switch(config-pmap-c)#
```

The class-default class map is always at the end of the class map list for a policy map.

Enter one of the following commands:

- **police** [**cir**] {*cir-rate* [*rate-type*]}
- **police** [**cir**] {*cir-rate* [*rate-type*]} [**bc**] *burst-size* [*burst-size-type*]
- **police** [**cir**] {*cir-rate* [*rate-type*]]} **conform transmit** [**violate drop**]

Example:

```
switch(config-pmap-c)#police cir 52000 bc 1000 packets
```

Example:

```
switch(config-pmap-c)#police cir 3400 kbps bc 200 kbytes
```

Specifies the committed information rate (CIR). The rate range is as follows:

- 0 1 to 268435456 pps (for Cisco Nexus 9300 and 9500 Series switches)
- 0 to 80000000000 bps/gbps/kbps/mbps

Note
The CIR rate range starts with 0. In previous releases, the CIR rate range starts with 1. A value of 0 drops the packet.

The committed burst (BC) range is as follows:

- 1 to 1073741 packets (for Cisco Nexus 9300 and 9500 Series switches)
- 1 to 512000000 bytes/kbytes/mbytes

The **conform transmit** action transmits the packet.

Note
You can specify the BC and conform action for the same CIR.

Step 4 (Optional) Specify the threshold value for dropped packets and generates a syslog if the drop count exceeds the configured threshold.

Example:

```
switch(config-pmap-c)#logging drop threshold 100
```

The range for the *drop-count* argument is from 1 to 8000000000 bytes. The range for the *syslog-level* argument is from 1 to 7, and the default level is 4.

Step 5 (Optional) Specify the 802.1Q class of service (CoS) value.

Example:

```
switch(config-pmap-c)#set cos 1
```

The range is from 0 to 7. The default value is 0.

Step 6 Exit the policy map class configuration mode and policy map configuration mode.

Example:

```
switch(config-pmap-c)#exit
switch(config-pmap)#exit
switch(config)#
```

Step 7 (Optional) Display the control plane policy map configuration.

Example:

```
switch#show policy-map type control-plane
```

Step 8 (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Configure a control plane class map, on page 21

Configure the control plane service policy

You can configure one or more policy maps for the CoPP service policy.

Note When you try to change the CoPP policy and apply a custom CoPP policy, it is configured in the hardware as non-atomic, and the following system message appears:

```
This operation can cause disruption of control traffic. Proceed (y/n)?  [no]y
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT24-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT23-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT21-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT25-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT26-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT22-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT4-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
```

Before you begin

Ensure that you have configured a control plane policy map.

Procedure

Step 1 Enters global configuration mode and then, enter control plane configuration mode.

Example:

```
switch#configure terminal
switch(config)#control-plane
switch(config-cp)#
```

Step 2 Specifies a policy map for the input traffic.

Example:

```
switch(config-cp)#service-policy input PolicyMapA
```

Repeat this step if you have more than one policy map.

You cannot disable CoPP. If you enter the **no** form of this command, packets are rate limited at 50 packets per seconds .

Step 3 Exit control plane configuration mode.

Example:

```
switch(config-cp)#exit
switch(config)#
```

Step 4 (Optional) Display the CoPP configuration.

Example:

```
switch#show running-config copp
```

Step 5 (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Related Topics

Configure a control plane policy map, on page 22

Configure the CoPP scale factor per line card

You can configure the CoPP scale factor per line card.

The scale factor configuration is used to scale the policer rate of the applied CoPP policy for a particular line card. The accepted value is from 0.10 to 2.00. You can increase or reduce the policer rate for a particular line card without changing the current CoPP policy. The changes are effective immediately, so you do not need to reapply the CoPP policy.

Procedure

Step 1 Enters global configuration mode and then enter the control plane configuration mode.

Example:

```
switch#configure terminal
switch(config)#control-plane
switch(config-cp)#
```

Step 2 Configure the policer rate per line card.

Example:

```
switch(config-cp)#scale-factor 1.10 module 1-2
```

The allowed scale factor value is from 0.10 to 2.00. When the scale factor value is configured, the policing values are multiplied by the corresponding scale factor value of the module, and it is programmed in the particular module.

To revert to the default scale factor value of 1.00, use the **no scale-factor** *value* **module** *multiple-module-range* command, or explicitly set the default scale factor value to 1.00 using the **scale-factor 1 module** *multiple-module-range* command.

Step 3 (Optional) Display the applied scale factor values when a CoPP policy is applied.

Example:

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

Step 4 (Optional) Copy the running configuration to the startup configuration.

Example:

```
switch#copy running-config startup-config
```

Change or reapply the default CoPP policy

You can change to a different default CoPP policy, or you can reapply the same default CoPP policy.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch#configure terminal
switch(config)#
```

Step 2 Apply the CoPP best practice policy.

Example:

```
switch(config)#copp profile moderate
```

You cannot disable CoPP. If you enter the **no** form of this command, packets are rate limited at 50 packets per seconds .

Step 3 (Optional) Display the CoPP status, including the last configuration operation and its status.

Example:

```
switch#show copp status
```

This command also enables you to verify that the CoPP best practice policy is attached to the control plane.

Step 4 (Optional) Display the CoPP configuration in the running configuration.

Example:

```
switch#show running-config copp
```

Related Topics

Changing or reapplying the default CoPP policy using the setup utility, on page 36

Copying the CoPP best practice policy

The CoPP best practice policy is read-only. If you want to modify its configuration, you must copy it.

Procedure

Step 1 Create a copy of the CoPP best practice policy.

Example:

```
switch#copp copy profile strict prefix abc
```

CoPP renames all class maps and policy maps with the specified prefix or suffix.

Step 2 (Optional) Display the CoPP status, including the last configuration operation and its status.

Example:

```
switch#show copp status
```

This command also enables you to verify that the copied policy is not attached to the control plane.

Step 3 (Optional) Display the CoPP configuration in the running configuration, including the copied policy configuration.

Example:

```
switch#show running-config copp
```

Protocol ACL filtering added for egress CoPP

The protocol ACL filtering for egress CoPP enables the NX-OS swtich to filter all traffic to control plane based on the host MAC, IPv4, and IPv6 address.

Configure ARP ACL filtering for egress CoPP

Before you begin

Ensure that you have configured a control plane policy map.

Procedure

Step 1 Enters global configuration mode and configure the size of the CoPP TCAM region.

Example:

```
switch#hardware access-list tcam region erg-copp 128
```

Step 2 Copy the running configuration to the startup configuration and reload the device.

Example:

```
switch#copy running-config startup-config
switch#reload
```

Note
The new size values are effective only after you enter **copy running-config startup-config** + **reload** or reload all line card modules.

Step 3 Enter the AMC ACL configuration sub-mode.

Example:

```
switch#configure terminal
switch#(config)#mac access-list mac-foo-1
switch(config-mac-acl)#
```

Step 4 Specify a control plane class map and enters class map configuration mode.

Example:

```
switch(config)#class-map type control-plane match-any c-map2
switch(config-cmap)#match access-group name IP-foo-1
```

The default class matching is match-any. The name can be a maximum of 64 characters long and is case-sensitive.

Step 5 Specify a control plane policy map and enters policy map configuration mode.

Example:

```
switch(config)#policy-map type control-plane PolicyMap1
switch(config-pmap)#
```

The policy map name can have a maximum of 64 characters and is case-sensitive.

Step 6 Specify a control plane class map name or the class default and enters control plane class configuration mode.

Example:

```
switch(config-pmap)#class c-map2
switch(config-pmap-c)#
```

The class-default class map is always at the end of the class map list for a policy map.

Enter one of these commands:

- **police** [**cir**] {*cir-rate* [*rate-type*]}
- **police** [**cir**] {*cir-rate* [*rate-type*]} [**bc**] *burst-size* [*burst-size-type*]
- **police** [**cir**] {*cir-rate* [*rate-type*]]} **conform transmit** [**violate drop**]

Example:

```
switch(config-pmap-c)#police cir 52000 bc 1000 packets
```

Specifies the committed information rate (CIR). The rate range is as follows:

The committed burst (BC) range is as follows:

Step 7 Enter the control plane dynamic configuration mode.

Example:

```
switch(config)#control-plane dynamic
switch(config-cp-dyn)#
```

Step 8 Specify a policy map for the input traffic.

Example:

```
switch(config-cp-dyn)#service-policy-dynamic input PolicyMap1
```

Configure IP ACL filtering for egress CoPP

Before you begin

Ensure that you have configured a control plane policy map.

Procedure

Step 1 Configure the size of the egress CoPP TCAM region.

Example:

```
switch#hardware access-list tcam region erg-copp 128
```

Step 2 Copy the running configuration to the startup configuration and reload the device.

Example:

```
switch#copy running-config startup-config
switch#reload
```

Note
The new size values are effective only after you enter **copy running-config startup-config** + **reload** or reload all line card modules.

Step 3 **ip access-list IP-foo-1**

Example:

```
switch#configure terminal
switch(config)#ip access-list IP-foo-1
switch(config-acl)#
```

Step 4 **permit tcp access-list IP-foo-1** *eq bgp*

Example:

```
switch(config-acl)#10 permit tcp 10.1.1.1/32 10.1.1.2/32 eq bgp
```

Step 5 Specify a control plane class map and enters class map configuration mode.

Example:

```
switch(config)#class-map type control-plane match-any c-map2
switch(config-cmap)#
```

The default class matching is match-any. The name can be a maximum of 64 characters long and is case sensitive.

Step 6 **match access-group name** *access-list-name*

Example:

```
switch(config-cmap)#match access-group name IP-foo-1
```

Step 7 Specify a control plane policy map and enters policy map configuration mode. The policy map name can have a maximum of 64 characters and is case sensitive.

Example:

```
switch(config)#policy-map type control-plane ClassMapA
switch(config-pmap)#
```

Step 8 Specify a control plane class map name or the class default and enters control plane class configuration mode.

Example:

```
switch(config-pmap)#class ClassMap2
switch(config-pmap-c)#
```

The class-default class map is always at the end of the class map list for a policy map.

Enter one of these commands.

- **police** [**cir**] {*cir-rate* [*rate-type*]}
- **police** [**cir**] {*cir-rate* [*rate-type*]} [**bc**] *burst-size* [*burst-size-type*]
- **police** [**cir**] {*cir-rate* [*rate-type*]]} **conform transmit** [**violate drop**]

Example:

```
switch(config-pmap-c)#police cir 52000 bc 1000 packets
```

Example:

```
switch(config-pmap-c)#police cir 3400 kbps bc 200 kbytes
```

Specifies the committed information rate (CIR). The rate range is as follows:

The committed burst (BC) range is as follows:

Step 9 Enter the control plane dynamic configuration mode and specify a policy map for the input traffic.

Example:

```
switch(config)#control-plane dynamic
switch(config-cp-dyn)#service-policy-dynamic input PolicyMap1
```

Copp configuration verification commands

Use this reference to verify the Copp configuration.

To display CoPP configuration information, use one of these tasks.

Table 2: Copp configuration verification commands

Command	Purpose
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	isplays the control plane policy map with associated class maps and CIR and BC values.
show policy-map interface control-plane	Displays the policy values with associated class maps and the number of drops for each policy or class map. When a CoPP policy is applied, the display includes scale factor values. If the scale factor value is set to the default (1.00), it is omitted from the display. **Note** The scale factor modifies the CIR and BC values internally for each module. The display only shows the configured CIR and BC values, while the actual value applied on a module is calculated by multiplying the scale factor with the configured value.

Command	Purpose
show class-map type control-plane [*class-map-name*]	Displays the control plane class map configuration, including the ACLs that are bound to this class map.
show copp diff profile {**strict** | **moderate** | **lenient** | **dense** } [**prior-ver**] **profile** {**strict** | **moderate** | **lenient** | **dense** } **show copp diff profile**	Displays the difference between two CoPP best practice policies. If you do not include the **prior-ver** option, this command displays the difference between two currently applied default CoPP best practice policies, such as the currently applied strict and currently applied moderate policies. When you include the prior-ver option, this command displays the difference between a currently applied default CoPP best practice policy and a previously applied default CoPP best practice policy (such as the currently applied strict and the previously applied lenient policies).
show copp profile {**strict** | **moderate** | **lenient** | **dense** }	Displays the details of the CoPP best practice policy, along with the classes and policer values.
show running-config aclmgr [**all**]	Displays the user-configured access control lists (ACLs) in the running configuration. Using the **all** keyword shows both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show running-config copp [**all**]	Displays the CoPP configuration stored in the running configuration.
show startup-config aclmgr [**all**]	Displays the user-configured access control lists (ACLs) in the startup configuration. Using the **all** keyword shows both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

Display the CoPP configuration status

Procedure

Display the configuration status for the CoPP feature.

Example:

```
switch#show copp status
```

Copp consistency checker

Beginning with Cisco NX-OS Release 10.5(2)F, the CoPP consistency checker ensures the consistency of all SUP-related ACLs across the Software, HAL, and Hardware layers. This feature is supported on Cisco Nexus 9300-FX3, GX, GX2, HX, 9808, and 9804 series switches.



Note Beginning with Cisco NX-OS Release 10.5(3)F, the **show consistency-checker copp extended module** command is deprecated. For more information on the CoPP consistency checker, see the *Consistency Checker Commands* section in the *Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 10.5(x)*.

Procedure

Perform a CoPP consistency check.

Example:

```
switch#show consistency-checker copp extended module 1 brief
switch#show consistency-checker copp extended module 2 detail
```

brief – displays the structured output of the consistency checker in brief format.

detail – displays the structured output of the consistency checker in detail format.

Monitor CoPP

Procedure

Display packet-level statistics for all classes that are part of the applied CoPP policy.

Example:

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

Statistics are specified in terms of OutPackets (packets admitted to the control plane) and DropPackets (packets dropped because of rate limiting).

Example:

This example shows how to monitor CoPP:

```
switch#show policy-map interface control-plane
Control Plane
Service-policy  input: copp-system-p-policy-strict
class-map copp-system-p-class-critical (match-any)
set cos 7
police cir 19000 pps , bc 128 packets
module 4 :
transmitted 373977 packets;
dropped 0 packets;
```

Monitoring CoPP with SNMP

Beginning with Cisco Nexus Release 9.2(3), CoPP supports the Cisco class-based QoS MIB (cbQoSMIB). You can now monitor all CoPP elements using SNMP, but you cannot modify them. This feature applies only to policies and their subelements—such as classes, match rules, and set actions—attached to the control plane. You cannot view elements of policies that are not in service on the control plane through SNMP.

These cbQoSMIB tables are supported:

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

Note SNMP MIB is not supported for Dynamic CoPP.

Clear the CoPP statistics

To clear the CoPP statistics, perform these steps.

Procedure

Step 1 (Optional) Display the currently applied CoPP policy and per-class statistics.

Example:

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

Step 2 Clear the CoPP statistics.

Example:

```
switch#clear copp statistics
```

Note
On Cisco Nexus 9800 Series switches with N9K-X9836DM-A and N9K-X98900CD-A line cards, as well as N9K-C9232E-B1, 9364E-SG2, and N9324C-SE1U switches, the **clear copp statistics** command clears the CoPP statistics for all policers, except for the **hardware rate-limiter** policers.

Example:

This example shows how to clear the CoPP statistics for your installation:

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

Configuration examples for CoPP

This section includes example CoPP configurations.

Copp configuration example

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

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

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

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

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

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

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

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

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

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

class-map type control-plane match-any copp-system-p-class-normal
 match access-group name copp-system-p-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-p-policy
 class copp-system-p-class-critical
  police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit exceed
transmit violate drop
 class copp-system-p-class-important
  police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit exceed
transmit violate drop
 class copp-system-p-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-p-policy
```

Create CoPP class and associate ACL:

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

Add the class to the CoPP policy:

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

The following example shows to customize COPP limit:

```
copp copy profile strict suffix CUSTOMIZED-COPP
policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
 class copp-class-redirect-CUSTOMIZED-COPP
  police cir 1500 mbps bc 125 mbytes conform transmit violate drop
control-plane
 service-policy input copp-policy-strict-CUSTOMIZED-COPP
```

Changing or reapplying the default CoPP policy using the setup utility

The following example shows how to change or reapply the default CoPP policy using the setup utility.

```
switch# setup
---- Basic System Configuration Dialog ----

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#
```

Changing CoPP policy limit

The following example shows to change CoPP limit to set PTP state stable across PTP interfaces.

```
copp copy profile strict suffix CUSTOMIZED-COPP

policy-map type control-plane copp-policy-strict-CUSTOMIZED-COPP
  class copp-class-redirect-CUSTOMIZED-COPP
    police cir 1500 mbps bc 125 mbytes conform transmit violate drop

control-plane
  service-policy input copp-policy-strict-CUSTOMIZED-COPP
```

Additional references for CoPP

This section offers more information about implementing CoPP.

Related Documents

Table 3: Related documents

Related Topic	Document title
Licensing	*Cisco NX-OS Licensing Guide*

Standards

Table 4: Standards

Standards	Title
RFC 2698	A Two Rate Three Color Marker