Configuring Control Plane Policing

This chapter contains the following sections:

- Information About CoPP, on page 1
- Control Plane Protection, on page 2
- CoPP Policy Templates, on page 6
- CoPP and the Management Interface, on page 11
- Licensing Requirements for CoPP, on page 11
- Guidelines and Limitations for CoPP, on page 11
- Default Settings for CoPP, on page 12
- Configuring CoPP, on page 13
- Verifying the CoPP Configuration, on page 14
- Displaying the CoPP Configuration Status, on page 15
- Monitoring CoPP, on page 15
- Clearing the CoPP Statistics, on page 17
- Additional References for CoPP, on page 17
- Feature History for CoPP, on page 17

Information 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 destined to any of the IP addresses of the router or Layer 3 switch. 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, which can be perpetrated either inadvertently or maliciously, typically involve high rates of traffic destined to the supervisor module or CPU itself.

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. For example, excessive traffic to the supervisor module could overload and slow down the performance of the entire Cisco NX-OS device. Another example is a DoS attack on the supervisor module that could generate IP traffic streams to the control plane at a very high rate, forcing the control plane to spend a large amount of time in handling these packets and preventing the control plane from processing genuine traffic.

Examples of DoS attacks are as follows:

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

These attacks can impact the device performance and have the following 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, such as the memory and buffers
- 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 different packets destined for the control plane into different classes. Once these classes are identified, the Cisco NX-OS device polices the packets, which ensures that the supervisor module is not overwhelmed.

Control Plane 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.

Redirected packets
Packets that are redirected to the supervisor module. Features such as Dynamic Host Configuration Protocol (DHCP) snooping or dynamic Address Resolution Protocol (ARP) inspection redirect some packets 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 to different classes and provides a mechanism to individually control the rate at which the supervisor module receives these packets.

Classification for CoPP

For effective protection, the Cisco NX-OS device classifies the packets that reach the supervisor modules to allow you to apply different rate controlling policies based on the type of the packet. For example, you might want to be less strict with a protocol packet such as Hello messages but more strict with a packet that is sent to the supervisor module because the IP option is set.

Rate Controlling Mechanisms

Once the packets are classified, the Cisco NX-OS device has two different mechanisms to control the rate at which packets arrive at the supervisor module: policing and rate limiting.

Using hardware policers, you can define separate actions for traffic that conforms to or violates certain conditions. These actions can transmit the packet, mark down the packet, or drop the packet.

You can configure the following parameters for policing:

Committed information rate (CIR)
Desired bandwidth, specified as a bit rate.

Committed burst (BC)
Size of a traffic burst that can exceed the CIR within a given unit of time and not impact scheduling.

CoPP Class Maps

The following table shows the available class maps and their configurations.

Table 1: Class Map Configurations and Descriptions

Class Map	Configuration	Description
class-map type control-plane match-any copp-system-class-arp	match protocol arp match protocol nd	Class matches all ARP packets. Class matches all ARP packets and ND (NA, NS, RA, and RS) packets.
class-map type control-plane match-any copp-system-class-bgp	match protocol bgp	Class matches all BGP packets.
class-map type control-plane match-any copp-system-class-bridging	match protocol bridging	Class matches all STP and RSTP frames.
class-map type control-plane match-any copp-system-class-cdp	match protocol cdp	Class matches all CDP frames.
class-map type control-plane match-any copp-system-class-default	match protocol default	Class matches all frames. Used for the default policer.
class-map type control-plane match-any copp-system-class-dhcp	match protocol dhcp	Class matches all IPv4 DHCP packets Class matches all both IPv4 DHCP packets.
class-map type control-plane match-any copp-system-class-eigrp	match protocol eigrp match protocol eigrp6	Class matches all IPv4 EIGRP packets. Class matches both IPv4 and IPv6 EIGRP packets.
class-map type control-plane match-any copp-system-class-exception	match protocol exception	Class matches all IP packets that are treated as exception packets (except TTL exception, IP Fragment exception and Same Interface exception packets) for IP routing purposes, such as packets with a Martian destination address or with an MTU failure.
class-map type control-plane match-any copp-system-class-excp-ip-frag	match protocol ip_frag	Class matches all IP packets that are fragments. (These packets are treated as exception packets from an IP routing perspective).
class-map type control-plane match-any copp-system-class-excp-same-if	match protocol same-if	Class matches all IP packets that are treated as exception packets for IP routing. The packets are matched because they are received from the interface where their destination is supposed to be.

Class Map	Configuration	Description
class-map type control-plane match-any copp-system-class-excp-ttl	match protocol ttl	Class matches all packets that are treated as TTL exception packets (when TTL is 0) from a IP routing perspective.
class-map type control-plane match-any copp-system-class-fip	match protocol fip	Class matches all packets belonging to the FCoE Initialization Protocol.
class-map type control-plane match-any copp-system-class-glean	match protocol glean	
class-map type control-plane match-any copp-system-class-hsrp-vrrp	match protocol hsrp_vrrp match protocol hsrp6	Class matches HSRP and VRRP packets. Class matches IPv4 HSRP, VRRP and IPv6 HSRP packets
class-map type control-plane match-any copp-system-class-icmp-echo	match protocol icmp_echo	Class matches all ICMP Echo (Ping) packets.
class-map type control-plane match-any copp-system-class-igmp	match protocol igmp	Class matches all IGMP packets.
class-map type control-plane match-any copp-system-class-isis	match protocol isis_dce	
class-map type control-plane match-any copp-system-class-l3dest-miss	match protocol unicast	Class matches all unicast routed packets that did not find a destination in the FIB.
class-map type control-plane match-any copp-system-class-lacp	match protocol lacp	Class matches all Link Aggregation Control Protocol (LACP) frames.
class-map type control-plane match-any copp-system-class-lldp	match protocol lldp_dcx	Class matches all LLDP frames.
class-map type control-plane match-any copp-system-class-mcast-last-hop	match protocol mcast_last_hop	Class matches all IP multicast last hop packets.
class-map type control-plane match-any copp-system-class-mcast-miss	match protocol multicast	Class matches all IP multicast frames that could not be routed because they did not have an entry in the FIB.
class-map type control-plane match-any copp-system-class-mgmt	match protocol mgmt	Class matches all management-related frames, such as SNMP, HTTP, NTP, Telnet, and SSH.
class-map type control-plane match-any copp-system-class-msdp	match protocol msdp	Class matches MSDP packets.

Class Map	Configuration	Description
class-map type control-plane match-any copp-system-class-ospf	match protocol ospf match protocol ospfv3	Class matches OSPF and OSPFv3 Protocol packets.
class-map type control-plane match-any copp-system-class-pim-hello	match protocol pim	Class matches all PIM Hello packets.
class-map type control-plane match-any copp-system-class-pim-register	match protocol reg	Class matches all PIM Register packets.
class-map type control-plane match-any copp-system-class-rip	match protocol rip	Class matches all RIP packets.
class-map type control-plane match-any copp-system-class-rpf-fail	match protocol rpf_fail	Class matches all RPF failure packets.
class-map type control-plane match-any copp-system-class-udld	match protocol udld	Class matches all UDLD frames.

CoPP Policy Templates

When you bring up your Cisco NX-OS device for the first time, the Cisco NX-OS software installs the default copp-system-policy to protect the supervisor module from DoS attacks. You can choose the CoPP policy template for your deployment scenario by specifying CoPP policy options from the initial setup utility:

- Default CoPP Policy (copp-system-policy-default)
- Scaled Layer 2 CoPP Policy (copp-system-policy-scaled-l2)
- Scaled Layer 3 CoPP Policy (copp-system-policy-scaled-l3)
- Customized CoPP Policy (copp-system-policy-customized)

If you do not select an option or choose not to execute the setup utility, the Cisco NX-OS software applies the Default policing. Cisco recommends starting with the default policy and later modifying the CoPP policies as required.

The default copp-system-policy-default policy has optimized values suitable for basic device operations.

You can change which CoPP policy is used by using the **service-policy input** *policy-name* command in the control plane configuration mode.

Default CoPP Policy

The copp-system-policy-default policy is applied to the switch by default. It has the classes with policer rates that should suit most network installations. You cannot modify this policy or the class maps associated with it. In addition, you cannot modify the class map configurations in this policy.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy-default
    class copp-system-class-igmp
      police cir 1024 kbps bc 65535 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 1024 kbps bc 3600000 bytes
    class copp-system-class-dhcp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-mgmt
      police cir 12000 kbps bc 4800000 bytes
    class copp-system-class-lacp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-lldp
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-udld
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-isis
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-msdp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-cdp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-fip
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bgp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-eigrp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-exception
      police cir 64 kbps bc 4800000 bytes
    class copp-system-class-glean
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-hsrp-vrrp
      police cir 1024 kbps bc 256000 bytes
    class copp-system-class-icmp-echo
      police cir 64 kbps bc 3600000 bytes
    class copp-system-class-ospf
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-pim-register
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-rip
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-l3dest-miss
      police cir 64 kbps bc 256000 bytes
    class copp-system-class-mcast-miss
      police cir 256 kbps bc 3200000 bytes
    class copp-system-class-excp-ip-frag
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-same-if
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-ttl
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-default
      police cir 512 kbps bc 6400000 bytes
```

Scaled Layer 2 CoPP Policy

The copp-system-policy-scaled policy has most classes with policer rates that are same as the default policy. However, it has higher policer rates for IGMP and ISIS. You cannot modify this policy or the class maps associated with it. In addition, you cannot modify the class map configurations in this policy.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy-scaled-l2
    class copp-system-class-igmp
      police cir 4096 kbps bc 264000 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 1024 kbps bc 3600000 bytes
    class copp-system-class-dhcp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-mgmt
      police cir 12000 kbps bc 4800000 bytes
    class copp-system-class-lacp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-lldp
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-udld
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-isis
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-msdp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-cdp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-fip
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bgp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-eigrp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-exception
      police cir 64 kbps bc 4800000 bytes
    class copp-system-class-glean
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-hsrp-vrrp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-icmp-echo
      police cir 64 kbps bc 3600000 bytes
    class copp-system-class-ospf
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-pim-register
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-rip
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-l3dest-miss
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-mcast-miss
      police cir 256 kbps bc 3200000 bytes
    class copp-system-class-excp-ip-frag
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-same-if
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-excp-ttl
```

```
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-default
      police cir 512 kbps bc 6400000 bytes
```

Scaled Layer 3 CoPP Policy

The copp-system-policy-scaled-l3 policy has most classes with policer rates that are same as the default policy. However, it has higher policer rates for IGMP, ICMP Echo, ISIS, Mcast-miss, and Glean related classes. You cannot modify this policy or the class maps associated with it. In addition, you cannot modify the class map configurations in this policy.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy-scaled-l3
    class copp-system-class-igmp
      police cir 4096 kbps bc 264000 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 4000 kbps bc 3600000 bytes
    class copp-system-class-dhcp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-mgmt
      police cir 12000 kbps bc 4800000 bytes
    class copp-system-class-lacp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-lldp
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-udld
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-isis
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-msdp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-cdp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-fip
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bgp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-eigrp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-exception
      police cir 64 kbps bc 4800000 bytes
    class copp-system-class-glean
      police cir 4000 kbps bc 4800000 bytes
    class copp-system-class-hsrp-vrrp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-icmp-echo
      police cir 4000 kbps bc 3600000 bytes
    class copp-system-class-ospf
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-pim-register
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-rip
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-l3dest-miss
      police cir 64 kbps bc 3200000 bytes
    class copp-system-class-mcast-miss
```

```
  police cir 4000 kbps bc 3200000 bytes
class copp-system-class-excp-ip-frag
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-same-if
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-ttl
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-default
  police cir 512 kbps bc 6400000 bytes
```

Customizable CoPP Policy

The copp-system-policy-customized policy is configured identically to the default policy, but can be customized for different class map information rates and burst sizes.

You cannot add or delete any of the class maps configured in this policy.

Important This policy is meant for advanced users. We recommend that you use extreme caution when configuring this policy and test it extensively before deploying it in your production network.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy-customized
    class copp-system-class-igmp
      police cir 1024 kbps bc 65535 bytes
    class copp-system-class-pim-hello
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bridging
      police cir 20000 kbps bc 4800000 bytes
    class copp-system-class-arp
      police cir 1024 kbps bc 3600000 bytes
    class copp-system-class-dhcp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-mgmt
      police cir 12000 kbps bc 4800000 bytes
    class copp-system-class-lacp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-lldp
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-udld
      police cir 2048 kbps bc 4800000 bytes
    class copp-system-class-isis
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-msdp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-cdp
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-fip
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-bgp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-eigrp
      police cir 9600 kbps bc 4800000 bytes
    class copp-system-class-exception
      police cir 64 kbps bc 4800000 bytes
    class copp-system-class-glean
      police cir 1024 kbps bc 4800000 bytes
    class copp-system-class-hsrp-vrrp
```

```
  police cir 1024 kbps bc 4800000 bytes
class copp-system-class-icmp-echo
  police cir 64 kbps bc 3600000 bytes
class copp-system-class-ospf
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-pim-register
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-rip
  police cir 9600 kbps bc 4800000 bytes
class copp-system-class-l3dest-miss
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-mcast-miss
  police cir 256 kbps bc 3200000 bytes
class copp-system-class-excp-ip-frag
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-same-if
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-excp-ttl
  police cir 64 kbps bc 3200000 bytes
class copp-system-class-default
  police cir 512 kbps bc 6400000 bytes
```

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.

Licensing Requirements for CoPP

This feature does not require a license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Guidelines and Limitations for CoPP

- CoPP is a feature that is enabled by default in the switch. You cannot enable or disable CoPP.
- Only one control-plane policy can be applied at a time.
- Removing a CoPP policy applies the default CoPP policy. In this way, a CoPP policy is always applied.
- You cannot add or delete any classes or policies.
- You cannot change the order of the classes or remove a class from any policy.
- You cannot modify the default, the Scaled Layer-2, or the Scaled Layer 3 policies. However, you can modify the information rate and burst size of the classes in the customized policy.
- The customized policy configuration is the same as the default policy configuration, unless the customized policy has been modified.

- When upgrading from a previous release, the default CoPP policy is enabled by default on the switch.
- After modifying the customized policy or changing the applied policy, the statistical counters are reset.
- After you perform an ISSU, the statistical counters are reset.
- Cisco recommends that you use the default CoPP policy initially and then later determine which of the CoPP policies to use based on the data center and application requirements.
- Customizing CoPP is an ongoing process. CoPP must be configured according to the protocols and features used in your specific environment as well as the supervisor features that are required by the server environment. As these protocols and features change, CoPP must be modified.
- Cisco recommends 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 use a different CoPP policy or modify the customized CoPP policy.
- All the traffic that you do not specify in the other class maps is put into the last class, the default class.
- 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).
- When a packet meets multiple exception conditions, CoPP matches the packet based on the order in which the CoPP ACLs are configured and match it only against a single class. This is an expected CoPP behavior.
- The copp-system-class-exception matches all IP data packets that are treated as exception packets (except TTL exception, IP Fragment exception and Same Interface exception packets) since the hardware itself is not capable of processing them. Control packets with ip-options are supposed to be caught by the respective protocol class and the protocol stack running on the switch is usually able to process them.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Default Settings for CoPP

This table lists the default settings for CoPP parameters.

Table 2: Default CoPP Parameters Settings

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

Configuring CoPP

Applying a CoPP Policy to the Switch

You can apply one of the following CoPP policies to the switch:

- Default CoPP Policy (copp-system-policy-default).
- Scaled Layer 2 CoPP Policy (copp-system-policy-scaled-l2).
- Scaled Layer 3 CoPP Policy (copp-system-policy-scaled-l3).
- Customized CoPP Policy (copp-system-policy-customized).

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config) # **control-plane**	Enters control-plane mode.
Step 3	switch(config-cp) # **service-policy input** *policy-map-name*	Applies the specified CoPP policy map. The *policy-map-name* can be copp-system-policy-default, copp-system-policy-scaled-l2, copp-system-policy-scaled-l3, or copp-system-policy-customized.
Step 4	switch(config-cp) # **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to apply a CoPP policy to the device:

```
switch# configure terminal
switch(config)# control-plane
switch(config-cp) # service-policy input copp-system-policy-default
switch(config-cp) # copy running-config startup-config
```

Modifying the Customized CoPP Policy

You can only modify the information rates and burst sizes of the class maps configured in this policy.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **policy-map type control-plane copp-system-policy-customized**	Enters configuration mode for the customized CoPP policy.
Step 3	switch(config-pmap)# **class** *class-map-name*	Specifies one of the 28 predefined class-maps listed in any CoPP predefined policy.
Step 4	switch(config-pmap-c)# **police cir** *rate-value* **kbps bc** *buffer-size* **bytes**	Configures the committed information rate (CIR) and committed burst size (BC). The range for cir is from 1 to 20480. The range for bc is from 1500 to 6400000.
Step 5	switch(config-pmap-c) # **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to modify the customized CoPP policy:

```
switch(config)# policy-map type control-plane copp-system-policy-customized
switch(config-pmap)# class copp-system-class-bridging
switch(config-pmap-c)# police cir 10000 kbps bc 2400000 bytes
```

Verifying the CoPP Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	Displays the control plane policy map with associated class maps.
show policy-map interface control-plane	Displays the policy values with associated class maps and drops per policy or class map.
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.

Displaying the CoPP Configuration Status

Procedure

	Command or Action	Purpose
Step 1	switch# **show copp status**	Displays the configuration status for the CoPP feature.

Example

This example shows how to display the CoPP configuration status:

```
switch# show copp status
```

Monitoring CoPP

Procedure

	Command or Action	Purpose
Step 1	switch# **show policy-map interface control-plane**	Displays packet-level statistics for all classes that are part of the applied CoPP policy. 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)
      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-rise
      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-rise6
    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-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
    set cos 7
    police cir 36000 kbps bc 250 ms
      conform action: transmit
      violate action: drop
    module 12:
      conformed 0 bytes,
        5-min offered rate 0 bytes/sec
        peak rate 0 bytes/sec
      violated 0 bytes,
        5-min violate rate 0 bytes/sec
        peak rate 0 bytes/sec
    module 14:
      conformed 0 bytes,
        5-min offered rate 0 bytes/sec
        peak rate 0 bytes/sec
      violated 0 bytes,
        5-min violate rate 0 bytes/sec
        peak rate 0 bytes/sec

  class-map copp-system-p-class-important (match-any)
    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-opflex
    match access-group name copp-system-p-acl-mac-lldp
    match access-group name copp-system-p-acl-mac-mvrp
    match access-group name copp-system-p-acl-mac-flow-control
    set cos 6
    police cir 1400 kbps bc 1500 ms
      conform action: transmit
      violate action: drop
    module 12:
      conformed 0 bytes,
        5-min offered rate 0 bytes/sec
        peak rate 0 bytes/sec
      violated 0 bytes,
        5-min violate rate 0 bytes/sec
        peak rate 0 bytes/sec
    module 14:
      conformed 0 bytes,
        5-min offered rate 0 bytes/sec
        peak rate 0 bytes/sec
      violated 0 bytes,
        5-min violate rate 0 bytes/sec
        peak rate 0 bytes/sec
....
```

Clearing the CoPP Statistics

Procedure

	Command or Action	Purpose
Step 1	(Optional) switch# **show policy-map interface control-plane**	Displays the currently applied CoPP policy and per-class statistics.
Step 2	switch# **clear copp statistics**	Clears the CoPP statistics.

Example

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

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

Additional References for CoPP

This section provides additional information related to implementing CoPP.

Related Documents

Related Topic	Document Title
Licensing	*Cisco NX-OS Licensing Guide*
Command reference	

Feature History for CoPP

Table 3: Feature History for CoPP

Feature Name	Feature Information
CoPP	Introduced in 5.1(3)N1(1)
CoPP	Additional IPv6 support in 5.2(1)N1(1)