Configuring Control Plane Policing

This chapter contains the following sections:

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. You configure packet classifications and rate controlling policies using class-maps and policy-maps.

The following parameters can be used to classify a packet:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 4 protocol

Rate Controlling Mechanisms

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

The policing rate is specified in terms of packets per second (PPS). Each classified flow can be policed individually by specifying a policing rate limit in PPS.

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—Layer 2 and Layer 3 policy which provides a good balance of policing between switched and routed traffic bound to CPU.
- Layer 2—Layer 2 policy which gives more preference to the Layer 2 traffic (eg BPDU) bound to the CPU
- Layer 3—Layer 3 policy which gives more preference to the Layer 3 traffic (eg BGP, RIP, OSPF etc) bound to the CPU

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 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.

You can switch across default, Layer 2 and Layer 3 templates by entering the setup utility again using the setup command.

Default CoPP Policy

This policy is applied to the switch by default. It has the classes with police rates that should suit most network installations. You cannot modify this policy template, but you can modify the CoPP configuration on the device. After you run the setup utility and set up the default CoPP policy profile, all modifications that were made to the CoPP policy will be removed.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
```

```
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 1300
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 1000
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bpdu
    police pps 12000
  class copp-s-cdp
    police pps 400
  class copp-s-lacp
    police pps 400
  class copp-s-lldp
    police pps 200
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
  class copp-ftp
    police pps 100
  class copp-http
    police pps 100
```

This is the default CoPP policy profile for Cisco Nexus 34180YC.

```
sh policy-map int control-plane
        Control Plane

          Service-policy  input: copp-system-p-policy-strict
```

```
class-map copp-system-p-class-l3uc-data (match-any)
  match exception glean
  set cos 1
  police cir 250 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

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-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
  set cos 7
  police cir 19000 pps , bc 128 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-important (match-any)
  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
  set cos 6
  police cir 3000 pps , bc 256 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-openflow (match-any)
  match access-group name copp-system-p-acl-openflow
  set cos 5
  police cir 2000 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-multicast-router (match-any)
  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
  set cos 6
  police cir 3000 pps , bc 128 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-multicast-host (match-any)
  match access-group name copp-system-p-acl-mld
  set cos 1
  police cir 2000 pps , bc 128 packets
```

```
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-l3mc-data (match-any)
  match exception multicast rpf-failure
  match exception multicast dest-miss
  set cos 1
  police cir 3000 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-normal (match-any)
  match access-group name copp-system-p-acl-mac-dot1x
  match protocol arp
  set cos 1
  police cir 1500 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-ndp (match-any)
  match access-group name copp-system-p-acl-ndp
  set cos 6
  police cir 1500 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-normal-dhcp (match-any)
  match access-group name copp-system-p-acl-dhcp
  match access-group name copp-system-p-acl-dhcp6
  set cos 1
  police cir 300 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-normal-dhcp-relay-response (match-any)
  match access-group name copp-system-p-acl-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp6-relay-response
  set cos 1
  police cir 400 pps , bc 64 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-normal-igmp (match-any)
  match access-group name copp-system-p-acl-igmp
  set cos 3
  police cir 6000 pps , bc 64 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-redirect (match-any)
  match access-group name copp-system-p-acl-ptp
  match access-group name copp-system-p-acl-ptp-l2
  match access-group name copp-system-p-acl-ptp-uc
  set cos 1
  police cir 1500 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
```

```
    dropped 0 packets;

class-map copp-system-p-class-exception (match-any)
  match exception ip option
  match exception ip icmp unreachable
  match exception ipv6 option
  match exception ipv6 icmp unreachable
  set cos 1
  police cir 50 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-exception-diag (match-any)
  match exception ttl-failure
  match exception mtu-failure
  set cos 1
  police cir 50 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-management (match-any)
  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
  set cos 2
  police cir 3000 pps , bc 512000 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-monitoring (match-any)
  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
  set cos 1
  police cir 300 pps , bc 128 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-l2-unpoliced (match-any)
  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
```

```
  set cos 7
  police cir 20000 pps , bc 8192 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-undesirable (match-any)
  match access-group name copp-system-p-acl-undesirable
  match exception multicast sg-rpf-failure
  set cos 0
  police cir 15 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-fcoe (match-any)
  match access-group name copp-system-p-acl-mac-fcoe
  set cos 6
  police cir 1500 pps , bc 128 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-nat-flow (match-any)
  match exception nat-flow
  set cos 7
  police cir 100 pps , bc 64 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-l3mcv6-data (match-any)
  match exception multicast ipv6-rpf-failure
  match exception multicast ipv6-dest-miss
  set cos 1
  police cir 3000 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-undesirablev6 (match-any)
  match exception multicast ipv6-sg-rpf-failure
  set cos 0
  police cir 15 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map copp-system-p-class-l2-default (match-any)
  match access-group name copp-system-p-acl-mac-undesirable
  set cos 0
  police cir 50 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;

class-map class-default (match-any)
  set cos 0
  police cir 50 pps , bc 32 packets
  module 1 :
    transmitted 0 packets;
    dropped 0 packets;
```

Layer 2 CoPP Policy

You cannot modify this policy template, but you can modify the CoPP configuration on the device. After you run the setup utility and set up the Layer 2 CoPP policy profile, all modifications that were made to the CoPP policy will be removed.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 1200
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 900
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bpdu
    police pps 12300
  class copp-s-cdp
    police pps 400
  class copp-s-lacp
    police pps 400
  class copp-s-lldp
    police pps 200
  class copp-icmp
    police pps 200
```

```
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
  class copp-ftp
    police pps 100
  class copp-http
    police pps 100
```

Layer 3 CoPP Policy

You cannot modify this policy template, but you can modify the CoPP configuration on the device. After you run the setup utility and set up the Layer 3 CoPP policy profile, all modifications that were made to the CoPP policy will be removed.

This policy has the following configuration:

```
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 4000
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
```

```
class copp-s-pimautorp
  police pps 200
class copp-s-routingProto1
  police pps 4000
class copp-s-arp
  police pps 200
class copp-s-ptp
  police pps 1000
class copp-s-bpdu
  police pps 6000
class copp-s-cdp
  police pps 200
class copp-s-lacp
  police pps 200
class copp-s-lldp
  police pps 200
class copp-icmp
  police pps 200
class copp-telnet
  police pps 500
class copp-ssh
  police pps 500
class copp-snmp
  police pps 500
class copp-ntp
  police pps 100
class copp-tacacsradius
  police pps 400
class copp-stftp
  police pps 400
class copp-ftp
  police pps 100
class copp-http
  police pps 100
```

Static CoPP Classes

The following are the available static CoPP classes:

- **copp-s-default**

  Catch-all CoPP class for traffic when copy-to-CPU is set for the packet and there is no match in other more specific CoPP classes for the packet.

  ```
  class-map copp-s-default (match-any)
        police pps 400
          OutPackets    0
          DropPackets   0
  ```

- **copp-s-l2switched**

  Catch-all CoPP class for Layer 2 traffic if there is no match in other explicit CoPP classes when CPU port is being selected for the packet.

  ```
  class-map copp-s-l2switched (match-any)
        police pps 200
          OutPackets    0
          DropPackets   0
  ```

- **copp-s-l3destmiss**

  Layer 3 traffic with a miss for the lookup in the hardware Layer 3 forwarding table.

```
class-map copp-s-l3destmiss (match-any)
      police pps 100
        OutPackets    0
        DropPackets   0
```

- **copp-s-glean**

  Used in case of Layer 3 traffic to IP address in directly connected subnets with no ARP resolution present for the IP address to trigger ARP resolution in software.

```
class-map copp-s-glean (match-any)
      police pps 500
        OutPackets    0
        DropPackets   0
```

- **copp-s-selfip**

  Default CoPP class for packets that are coming to one of the router interface's IP addresses if there is no match in other more specific CoPP classes.

```
class-map copp-s-selfIp (match-any)
      police pps 500
        OutPackets    4
        DropPackets   0
```

- **copp-s-l3mtufail**

  Layer 3 packets with MTU check fail needing software processing for fragmentation or for generating ICMP message.

```
class-map copp-s-l3mtufail (match-any)
      police pps 100
        OutPackets    0
        DropPackets   0
```

- **copp-s-ttl1**

  Layer 3 packets coming to one of the router's interface IP addresses and with TTL=1.

```
class-map copp-s-ttl1 (match-any)
      police pps 100
        OutPackets    0
        DropPackets   0
```

- **copp-s-ipmsmiss**

  Multicast packets with lookup miss in hardware Layer 3 forwarding table for multicast forwarding lookup. These data packets can trigger the installation of the hardware forwarding table entries for hardware forwarding of multicast packets.

```
class-map copp-s-ipmcmiss (match-any)
      police pps 400
        OutPackets    0
        DropPackets   0
```

- **copp-s-l3slowpath**

  Layer 3 packets that are hitting other packet exception cases that need handing in software. For example, IP option packets.

```
class-map copp-s-l3slowpath (match-any)
      police pps 100
        OutPackets    0
        DropPackets   0
```

- **copp-s-dhcpreq**

CoPP class for DHCP request packets. By default, this class is only used to program the CoPP rate for this class of packets. Copy to CPU is not enabled till DHCP snooping or relay is configured.

```
class-map copp-s-dhcpreq (match-any)
      police pps 300
        OutPackets    0
        DropPackets   0
```

- **copp-s-dai**

  CoPP class for ARP inspection intercepted packets. By default, this class is only used to program the CoPP rate for this class of packets. Copy to CPU is not enabled till the IP ARP inspection feature is configured.

```
class-map copp-s-dai (match-any)
      police pps 300
        OutPackets    0
        DropPackets   0
```

- **copp-s-pimautorp**

  This CoPP class is used to copy PIM auto-rp packets to the CPU (IP multicast groups 224.0.1.39 and 224.0.1.40)

```
class-map copp-s-pimautorp (match-any)
      police pps 200
        OutPackets    0
        DropPackets   0
```

- **copp-s-arp**

  CoPP class for ARP and ND request and reply packets that are being copied to the CPU.

```
class-map copp-s-arp (match-any)
      police pps 200
        OutPackets    0
        DropPackets   0
```

- **copp-s-ptp**

  CoPP class for Precision Time Protocol (PTP) packets.

```
class-map copp-s-ptp (match-any)
      police pps 1000
        OutPackets    0
        DropPackets   0
```

- **copp-s-vxlan**

  This CoPP class is used when the NV overlay feature is configured and when packets are being copied to the CPU for remote peer IP address learning.

```
class-map copp-s-vxlan (match-any)
      police pps 1000
        OutPackets    0
        DropPackets   0
```

- **copp-s-bfd**

  CoPP class for Bidirectional Forwarding Detection (BFD) packets that are being copied to the CPU (Packets with BFD protocol UDP ports, coming to router interface IP address).

```
class-map copp-s-bfd (match-any)
      police pps 600
        OutPackets    0
        DropPackets   0
```

- **copp-s-bpdu**

  CoPP class for BPDU class of packets that are being copied to the CPU. This includes STP, CDP, LLDP, LACP, and UDLD packets).

```
class-map copp-s-bpdu (match-any)
      police pps 15000
        OutPackets    100738
        DropPackets   0
```

- **copp-s-dpss**

  CoPP class that is used for programmability features, OnePK and Openflow, when the policy is configured with punt-to-CPU action. For example, data path service set, OpenFlow punt-to-controller action.

```
class-map copp-s-dpss (match-any)
      police pps 1000
        OutPackets    0
        DropPackets   0
```

- **copp-s-mpls**

  Used for the tap aggregation feature for MPLS label strip action. This class is used to copy the packets to the CPU to learn the MPLS label information and program for the label strip action.

```
class-map copp-s-mpls (match-any)
      police pps 100
        OutPackets    0
        DropPackets   0
```

CoPP Class Maps

Classes within a policy are of two types:

- Static—These classes are part of every policy template and cannot be removed from the policy or CoPP configuration. Static classes would typically contain the traffic which is deemed critical to device operation and is required in the policy.
- Dynamic—These classes can be created, added or removed from a policy. Using dynamic classes, you can create classes/policing for CPU bound traffic (unicast) specific to their requirements.

Note Classes with names copp-s-x are static classes.

ACLs can be associated with both static and dynamic classes.

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).

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 has the following configuration guidelines and limitations:

- The PIM_IGMP class-id is set on the port only when PIM is enabled. Since there is no need to punt IGMP packets to the CPU on the Layer 3 ports when PIM is not enabled, you have to configure feature pim and enable PIM on the port to get the packets on the copp-s-igmp queue.
- Cisco recommends that you choose the default, L2, or L3 policy, depending upon your deployment scenario and later modify the CoPP policies based on observed behavior.
- First generation Nexus 3000 series switches (non -EX/FX/FX2), do not support source-based CoPP. This limitation does not exist for cloud scale ASIC-based Nexus switches
- If you observe +/- 2-5% irregularity in the traffic around 30-40s after the traffic has fully converged after fast-reload, use a higher COPP value for the ARP packets.
- 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.
- The default police packets per second (PPS) value is changed to 900 for **copp-s-bfd** command with **write erase** command and reload.
- 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.
- The Cisco NX-OS software does not support egress CoPP or silent mode. CoPP is supported only on ingress (**service-policy output copp** cannot be applied to the control plane interface).
- The creation of new CoPP policies is not supported.
- When a new CoPP class-map is inserted into the CoPP policy-map with the **insert-before** option, the order of the class-maps is retained in the running-configuration. However, after you run the **write erase** command and reload the switch, the default CoPP policy is applied, and the class-maps are rearranged in the default order. When you copy the file to the running-configuration, it becomes a modify operation

for the existing CoPP policy and the new class-maps are inserted at the end. Similarly, if there is change in the order of default class-maps in the file, it will not be effective. To preserve the order of the class-maps, copy the configuration to startup and reload.

- IPv6 and IPv4 CoPP ACL entries use different TCAM regions. For IPv6 CoPP to work, the IPv6 ACL SUP tcam region (ipv6-sup) needs to be carved to a non- zero size. For more information, see the ACL TCAM Regions and Configuring ACL TCAM Region Sizes topics.
- CoPP can have a maximum of 76 entries for all IPv4 CoPP ACLs, IPv6 CoPP ACLs, and ARP ACLs. The system is programmed with 72 static entries (20 internal, 43 IPv4 ACL, and 9 IPv6 ACL entries). You can configure the remaining 4 entries. If you want to create more entries, you need to delete any unused static CoPP ACEs, and then create your additional entries.
- Cisco Nexus 3000 Series switches drop all the packets when the tunnel is not configured. The packets are also dropped when the tunnel is configured but the tunnel interface is not configured or the tunnel interface is in shut down state.

  Point to Point tunnel (Source and Destination) – Cisco Nexus 3000 Series switches decapsulate all IP-in-IP packets destined to it when the command **feature tunnel** is configured and there is an operational tunnel interface configured with the tunnel source and the destination address that matches the incoming packets' outer source and destination addresses. If there is not a source and destination packet match or if the interface is in shutdown state, the packet is dropped.

  Decapsulate Tunnel (Source only) - Cisco Nexus 3000 Series switches decapsulate all IP-in-IP packets destined to it when the command **feature tunnel** is configured and there is an operational tunnel interface configured with the tunnel source address that matches the incoming packets' outer destination addresses. If there is not a source packet match or if the interface is in shutdown state, the packet is dropped.
- If you use NXAPI over the front panel port, then you must increase the CoPP policy (for http) to allows 3000 PPS traffic, so that there is no packet drop, and the CLIs with a larger output return within the expected time.
- The following limitations apply to Cisco Nexus 34180YC platform:
  - The BC value in the CoPP policy is ignored
  - The transmitted packets to the supervisor moduel are double if the control traffic comes on two pipelines.
  - CIR is in PPS.
  - Default Layer 2 CoPP policies are not supported.
  - Only TTL=1 is supported.

Upgrade Guidelines for CoPP

CoPP has the following upgrade guidelines:

- If you upgrade from a Cisco NX-OS release that does not support the CoPP feature to a release that supports the CoPP feature, CoPP is automatically enabled with the default policy when the switch boots up. You must run the setup script after the upgrade to enable a different policy (default, l3, ,l2). Not configuring CoPP protection can leave your NX-OS device vulnerable to DoS attacks.

- 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 additional classes for new protocols, you must run the setup utility for the new CoPP classes to be available.
- Because the setup script modifies the policing rates corresponding to different flows coming into the CPU, we recommend that you run the setup script during a scheduled maintenance period and not during a time when there is traffic on the device.
- When upgrading from Cisco NX-OS Release 6.x to Cisco NX-OS Release 7.x or 9.2x/9.3x, the default control plane policy may not be applied. To apply CoPP policy, you must perform the following steps:
  1. Back up the configuration on Cisco NX-OS Release 6.x
  2. Write erase the switch
  3. Apply the back up configuration
  4. Proceed with the Cisco NX-OS Release 7.x or 7.x or 9.2x/9.3x upgrade

Configuring CoPP

Configuring 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 IPv4 or 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

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**class-map type control-plane match-any** *class-map-name*
	Example:
	`switch(config)# class-map type control-plane ClassMapA`
	`switch(config-cmap)#`
		Specifies a control plane class map and enters class map configuration mode. 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.

	Command or Action	Purpose
Step 3	(Optional) **match access-group name** *access-list-name* **Example:** `switch(config-cmap)# match access-group name MyAccessList`	Specifies matching for an IP ACL. You can repeat this step to match more than one IP ACL. **Note** The **permit** and **deny** ACL keywords are ignored in the CoPP matching.

Step 4	**exit**
	Example:
	`switch(config-cmap)# exit`
	`switch(config)#`
		Exits class map configuration mode.

Step 5	(Optional) **show class-map type control-plane** [*class-map-name*] **Example:** `switch(config)# show class-map type control-plane`	Displays the control plane class map configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring 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, the default PPS for that class is 0.

You can configure policies for IPv4 or IPv6 packets.

Before you begin

Ensure that you have configured a control plane class map.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**policy-map type control-plane** *policy-map-name* **Example:**	Specifies a control plane policy map and enters the policy map configuration mode. The policy map name is case sensitive.

	Command or Action	Purpose
	`switch(config)# policy-map type control-plane copp-system-policy` `switch(config-pmap)#`	**Note** The name of the policy-map cannot be changed. You can only use the **copp-system-policy** name for the policy-map. The system allows only a single **type control-plane** policy-map to be configured.

Step 3	**class** {*class-map-name* [**insert-before** *class-map-name2*] | **class**}
	Example:
	`switch(config-pmap)# class ClassMapA`
	`switch(config-pmap-c)#`
		Specifies a control plane class map name or the class default and enters control plane class configuration mode.

Step 4	**police** [**pps**] {*pps-value*} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**] **Example:** `switch(config-pmap-c)# police pps 100 bc 10`	Specifies the rate limit in terms of packets per second (PPS) and the committed burst (BC). The PPS range is 0 - 20,000. The default PPS is 0. The BC range is from 0 to 512000000. The default BC size unit is bytes.
Step 5	**police** [**cir**] {*cir-rate* [*rate-type*]} OR **police** [**cir**] {*cir-rate* [*rate-type*]}[**bc**] burst-size [burst-size-type] OR **police** [**cir**] {*cir-rate* [*rate-type*]} **conform transmit** [**violate drop**] **Example:** `switch(config-pmap-c)# police cir 3400 kbps bc 200 kbytes`	You can specify the BC and conform action for the same CIR. The conform action options are as follows: • drop—Drops the packet. • transmit—Transmits the packet.

Step 6	**exit**
	Example:
	`switch(config-pmap-c)# exit`
	`switch(config-pmap)#`
		Exits policy map class configuration mode.

Step 7	**exit**
	Example:
	`switch(config-pmap)# exit`
	`switch(config)#`
		Exits policy map configuration mode.

Step 8	(Optional) **show policy-map type control-plane** [**expand**] [**name** *class-map-name*] **Example:** `switch(config)# show policy-map type control-plane`	Displays the control plane policy map configuration.
Step 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring the Control Plane Service Policy

Before you begin

Configure a control plane policy map.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**control-plane**
	Example:
	`switch(config) # control-plane`
	`switch(config-cp)#`
		Enters control plane configuration mode.

Step 3	[**no**] **service-policy input** *policy-map-name* **Example:** `switch(config-cp)# service-policy input copp-system-policy`	Specifies a policy map for the input traffic.

Step 4	**exit**
	Example:
	`switch(config-cp)# exit`
	`switch(config)#`
		Exits control plane configuration mode.

Step 5	(Optional) **show running-config copp** [**all**] **Example:** `switch(config)# show running-config copp`	Displays the CoPP configuration.
Step 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

CoPP Show Commands

To display CoPP configuration information, enter one of the following show commands:

Command	Purpose
show ip access-lists [*acl-name*]	Displays all IPv4 ACLs configured in the system, including the CoPP ACLs.

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 ipv6 access-lists	Displays all of the IPv6 ACLs configured on the device, including the CoPP IPv6 ACLs.
show arp access-lists	Displays all of the ARP ACLs configured on the device, including the CoPP ARP ACLs.
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	Displays the control plane policy map with associated class maps and PPS values.
show running-config copp [**all**]	Displays the CoPP configuration in the running configuration.
show running-config aclmgr [**all**]	Displays the user-configured access control lists (ACLs) in the running configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
show startup-config copp [**all**]	Displays the CoPP configuration in the startup configuration.
show startup-config aclmgr [**all**]	Displays the user-configured access control lists (ACLs) in the startup configuration. The **all** option displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

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-policy-default

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


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

service-policy input: copp-system-policy
class-map copp-s-selfIp (match-any)
 police pps 500
 OutPackets 268
 DropPackets 0
```

Disabling and Reenabling the Rate Limit on CoPP Classes

To transfer data at speeds higher than what is regulated by CoPP, you can disable the default rate limit on CoPP classes and set the rate to the maximum value allowed on the device. Although the packets are now directed to the CPU at the maximum possible rate, the rate of processing of these packets depends on the CPU capability. After data transfer, you must ensure that you reenable the rate limit on CoPP classes.

Important Disabling the rate limit on CoPP classes can make the CPU vulnerable to overwhelming traffic.

Before you begin

Ensure that the CPU is protected and that excessive external traffic is not directed at device interfaces, the supervisor module or the CPU.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**copp rate-limit disable** **Example:** `switch(config)# copp rate-limit disable`	Disables the default packets per second sent to the CPU and allows the maximum possible packet rate to the CPU on each queue. **Important** After you run this command, a warning appears to notify you that the CoPP rate-limit is disabled for all classes. Hence, the CPU is vulnerable to traffic attacks. Run the **no copp rate-limit disable** command as soon as possible.
Step 3	(Optional) **show policy-map interface control-plane** **Example:** `switch(config)# 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).
Step 4	**no copp rate-limit disable** **Example:** `switch(config)# no copp rate-limit disable`	Resets the rate limit of the packets sent to the CPU on each queue to the default value.

	Command or Action	Purpose
Step 5	**exit** **Example:** `switch(config)# exit`	Exits global configuration mode.

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
```

CoPP Configuration Examples

Creating an IP ACL

```
ip access-list  copp-sample-acl
permit udp any any eq 3333
permit udp any any eq 4444
```

The following example shows how to modify the CoPP Policy to drop all IP-in-IP (Protocol 4) packets immediately if there is not an operational tunnel that matches the incoming packet. Create copp-s-ipinip before the default copp-s-selfip policy as displayed in the following example.

```
ip access-list copp-s-ipinip
10 permit 4 any any
class-map type control-plane match-any copp-s-ipinip
match access-group name copp-s-ipinip
policy-map type control-plane copp-system-policy
class copp-s-ipinip
police pps 0
class copp-s-selfIp
police pps 500
class copp-s-default
police pps 400
```

Creating a Sample CoPP Class with an Associated IP ACL

The following example shows how to create a new CoPP class and associated ACL:

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

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

```
policy-map type control-plane copp-system-policy
Class copp-sample-class
 Police pps 100
```

The following example shows how to modify the PPS for an existing class (copp-s-bpdu):

```
policy-map type control-plane copp-system-policy
 Class copp-s-bpdu
 Police pps <new_pps_value>
```

Creating a Dynamic Class (IPv6 ACL)

The following example shows how to create an IPv6 ACL

```
ipv6 access-list  copp-system-acl-eigrp6
10 permit 88 any ff02::a/128
```

Associating an ACL with an Existing or New CoPP Class

The following example shows how to associate an ACL with an existing or new CoPP class:

```
class-map type control-plane copp-s-eigrp
match access-grp name copp-system-acl-eigrp6
```

Adding a Class to a CoPP Policy

The following example shows how to add a class to a CoPP policy, if the class has not already been added:

```
policy-map type control-plane copp-system-policy
class copp-s-eigrp
police pps 100
```

Creating an ARP ACL-Based Dynamic Class

ARP ACLs use ARP TCAM. The default size of this TCAM is 0. Before ARP ACLs can be used with CoPP, this TCAM needs to be carved for a non-zero size.

```
hardware profile tcam region arpacl 128
copy running-config startup-config
reload
```

Creating an ARP ACL

```
arp access-list copp-arp-acl
permit ip 20.1.1.1 255.255.255.0 mac any
```

The procedure to associate an ARP ACLs with a class, and adding that class to the CoPP policy, is the same as the procedure for IP ACLs.

Creating a CoPP Class and Associating an ARP ACL

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

Removing a Class from a CoPP Policy

```
policy-map type control-plane copp-system-policy
   no class-abc
```

Removing a Class from the System

```
no class-map type control-plane copp-abc
```

Using the insert-before option to see if a packet matches multiple classes and the priority needs to be assigned to one of them

```
policy-map type control-plan copp-system-policy
class copp-ping insert-before copp-icmp
```

Sample CoPP Configuration

The following example shows a sample CoPP configuration with ACLs, classes, policies, and individual class policing:

```
IP access list copp-system-acl-eigrp
        10 permit eigrp any 224.0.0.10/32
IP access list copp-system-acl-icmp
        10 permit icmp any any
IP access list copp-system-acl-igmp
        10 permit igmp any any
IP access list copp-system-acl-ntp
        10 permit udp any any eq ntp
        20 permit udp any eq ntp any
IP access list copp-system-acl-pimreg
        10 permit pim any any
IP access list copp-system-acl-ping
        10 permit icmp any any echo
        20 permit icmp any any echo-reply
IP access list copp-system-acl-routingproto1
        10 permit tcp any gt 1024 any eq bgp
        20 permit tcp any eq bgp any gt 1024
        30 permit udp any 224.0.0.0/24 eq rip
        40 permit tcp any gt 1024 any eq 639
        50 permit tcp any eq 639 any gt 1024
        70 permit ospf any any
        80 permit ospf any 224.0.0.5/32
        90 permit ospf any 224.0.0.6/32
IP access list copp-system-acl-routingproto2
        10 permit udp any 224.0.0.0/24 eq 1985
        20 permit 112 any 224.0.0.0/24
IP access list copp-system-acl-snmp
        10 permit udp any any eq snmp
        20 permit udp any any eq snmptrap
IP access list copp-system-acl-ssh
        10 permit tcp any any eq 22
        20 permit tcp any eq 22 any
IP access list copp-system-acl-stftp
        10 permit udp any any eq tftp
        20 permit udp any any eq 1758
        30 permit udp any eq tftp any
        40 permit udp any eq 1758 any
        50 permit tcp any any eq 115
        60 permit tcp any eq 115 any
IP access list copp-system-acl-tacacsradius
        10 permit tcp any any eq tacacs
```

```
        20 permit tcp any eq tacacs any
        30 permit udp any any eq 1812
        40 permit udp any any eq 1813
        50 permit udp any any eq 1645
        60 permit udp any any eq 1646
        70 permit udp any eq 1812 any
        80 permit udp any eq 1813 any
        90 permit udp any eq 1645 any
        100 permit udp any eq 1646 any
IP access list copp-system-acl-telnet
        10 permit tcp any any eq telnet
        20 permit tcp any any eq 107
        30 permit tcp any eq telnet any
        40 permit tcp any eq 107 any
IP access list copp-system-dhcp-relay
        10 permit udp any eq bootps any eq bootps
IP access list test
        statistics per-entry
        10 permit ip 1.2.3.4/32 5.6.7.8/32 [match=0]
        20 permit udp 11.22.33.44/32 any [match=0]
        30 deny udp 1.1.1.1/32 any [match=0]

IPv6 access list copp-system-acl-dhcpc6
        10 permit udp any any eq 546
IPv6 access list copp-system-acl-dhcps6
        10 permit udp any ff02::1:2/128 eq 547
        20 permit udp any ff05::1:3/128 eq 547
IPv6 access list copp-system-acl-eigrp6
        10 permit 88 any ff02::a/128
IPv6 access list copp-system-acl-v6routingProto2
        10 permit udp any ff02::66/128 eq 2029
        20 permit udp any ff02::fb/128 eq 5353
IPv6 access list copp-system-acl-v6routingproto1
        10 permit 89 any ff02::5/128
        20 permit 89 any ff02::6/128
        30 permit udp any ff02::9/128 eq 521

class-map type control-plane match-any copp-icmp
  match access-group name copp-system-acl-icmp
class-map type control-plane match-any copp-ntp
  match access-group name copp-system-acl-ntp
class-map type control-plane match-any copp-s-arp
class-map type control-plane match-any copp-s-bfd
class-map type control-plane match-any copp-s-bpdu
class-map type control-plane match-any copp-s-dai
class-map type control-plane match-any copp-s-default
class-map type control-plane match-any copp-s-dhcpreq
  match access-group name copp-system-acl-dhcps6
class-map type control-plane match-any copp-s-dhcpresp
  match access-group name copp-system-acl-dhcpc6
  match access-group name copp-system-dhcp-relay
class-map type control-plane match-any copp-s-eigrp
  match access-group name copp-system-acl-eigrp
  match access-group name copp-system-acl-eigrp6
class-map type control-plane match-any copp-s-glean
class-map type control-plane match-any copp-s-igmp
  match access-group name copp-system-acl-igmp
class-map type control-plane match-any copp-s-ipmcmiss
class-map type control-plane match-any copp-s-l2switched
class-map type control-plane match-any copp-s-l3destmiss
class-map type control-plane match-any copp-s-l3mtufail
class-map type control-plane match-any copp-s-l3slowpath
class-map type control-plane match-any copp-s-pimautorp
class-map type control-plane match-any copp-s-pimreg
```

```
  match access-group name copp-system-acl-pimreg
class-map type control-plane match-any copp-s-ping
  match access-group name copp-system-acl-ping
class-map type control-plane match-any copp-s-ptp
class-map type control-plane match-any copp-s-routingProto1
  match access-group name copp-system-acl-routingproto1
  match access-group name copp-system-acl-v6routingproto1
class-map type control-plane match-any copp-s-routingProto2
  match access-group name copp-system-acl-routingproto2
class-map type control-plane match-any copp-s-selfIp
class-map type control-plane match-any copp-s-ttl1
class-map type control-plane match-any copp-s-v6routingProto2
  match access-group name copp-system-acl-v6routingProto2
class-map type control-plane match-any copp-snmp
  match access-group name copp-system-acl-snmp
class-map type control-plane match-any copp-ssh
  match access-group name copp-system-acl-ssh
class-map type control-plane match-any copp-stftp
  match access-group name copp-system-acl-stftp
class-map type control-plane match-any copp-tacacsradius
  match access-group name copp-system-acl-tacacsradius
class-map type control-plane match-any copp-telnet
  match access-group name copp-system-acl-telnet
policy-map type control-plane copp-system-policy
  class copp-s-selfIp
    police pps 500
  class copp-s-default
    police pps 400
  class copp-s-l2switched
    police pps 200
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-l3slowpath
    police pps 100
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-dai
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-routingProto2
    police pps 1300
  class copp-s-v6routingProto2
    police pps 1300
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto1
    police pps 1000
```

```
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bfd
    police pps 350
  class copp-s-bpdu
    police pps 12000
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
control-plane
  service-policy input copp-system-policy
```

Example: 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

  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 : switch

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

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

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

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

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

  Configure CoPP System Policy Profile ( default / l2 / l3 ) [default]: l2

The following configuration will be applied:
  switchname switch
  telnet server enable
  no ssh server enable
  policy-map type control-plane copp-system-policy ( l2 )

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

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

[########################################] 100%
```

Preventing CoPP Overflow by Splitting ICMP Pings

Note This section applies only to Cisco Nexus 3000 Series switches and Cisco Nexus 3100 Series switches in N3K mode.

Some servers use ICMP pings to the default gateway to verify that the active NIC still has access to the aggregation switch. As a result, if the CoPP values are exceeded, CoPP starts dropping traffic for all networks. One malfunctioning server can send out thousands of ICMP pings, causing all servers in one aggregation block to lose their active NIC and start swapping NICs.

If your server is configured as such, you can minimize the CoPP overflow by splitting the ICMP pings based on subnets or groups of subnets. Then if a server malfunctions and overflows CoPP, the supervisor answers the ICMP pings only on some subnetworks.

The last entry in the class map or policy map should identify all of the ICMP pings in the networks that are not specified. If these counters increase, it means that a new network was added that was not specified in the existing ACLs for ICMP. In this case, you would need to update the ACLs related to ICMP.

Note Per the default CoPP, ICMP pings fall under copp-system-p-class-monitoring.

The following example shows how to prevent CoPP overflow by splitting ICMP pings.

First, add the new ACLs that identify the networks you want to group together based on the findings of the investigations of the applications:

```
ip access-list copp-icmp-1
statistics per-entry
10 permit icmp 10.2.1.0 255.255.255.0 any
20 permit icmp 10.2.2.0 255.255.255.0 any
30 permit icmp 10.2.3.0 255.255.255.0 any
ip access-list copp-icmp-2
statistics per-entry
10 permit icmp 10.3.1.0 255.255.255.0 any
10 permit icmp 10.3.2.0 255.255.255.0 any
```

```
10 permit icmp 10.3.3.0 255.255.255.0 any
ip access-list copp-icmp-3
statistics per-entry
10 permit icmp 10.4.1.0 255.255.255.0 any
10 permit icmp 10.4.2.0 255.255.255.0 any
10 permit icmp 10.4.3.0 255.255.255.0 any
...
ip access-list copp-icmp-10
10 permit icmp any any
```

Add these ACLs to the new class maps for CoPP:

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

Modify the CoPP policy map by adding new policies with the above created class maps:

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

Delete ICMP from the existing class maps:

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

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	