Configuring Control Plane Policing

This chapter describes how to configure control plane policing (CoPP) on a Cisco NX-OS device.

This chapter includes the following sections:

Information About CoPP

Control plane policing (CoPP) protects the control plane and separates it from the data plane, thereby ensuring 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 route processor 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. Attacks on the supervisor module can be of various types such as DoS that generates IP traffic streams to the control plane at a very high rate. These attacks force the control plane to spend a large amount of time in handling these packets and prevents 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 setting appropriate control plane protection.

Control Plane Protection

To protect the control plane, the Cisco NX-OS device segregates different packets destined to the control plane into different classes. Once these classes are identified, the Cisco NX-OS device polices or marks down packets, which ensure 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, then 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 like 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 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. The following parameters that can be used for classifying a packet:

- Source IP address
- Destination IP address
- Source MAC address
- Destination MAC address
- VLAN
- Source port
- Destination port
- Exception cause

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. Two mechanisms control the rate of traffic to the supervisor module. One is called policing and the other is called rate limiting.

Using hardware policers, you can define separate actions for traffic that conforms to, exceeds, or violates certain conditions. The 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 or a percentage of the link rate.
Peak information rate (PIR)	Desired bandwidth, specified as a bit rate or a percentage of the link rate.
Committed burst (BC)	Size of a traffic burst that can exceed the CIR within a given unit of time and not impact scheduling
Extended burst (BE)	Size that a traffic burst can reach before all traffic exceeds the PIR.

In addition, you can set separate actions such as transmit or drop for conform, exceed, and violate traffic.

For more information on policing parameters, see the Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 4.2.

Default Policing Policies

When you bring up your Cisco NX-OS device for the first time, the Cisco NX-OS software installs the default copp-system-policy policy to protect the supervisor module from DoS attacks. You can set the level of protection by choosing one of the following CoPP policy options from the initial setup utility:

- Strict—This policy is 1 rate and 2 color and has a BC value of 250 ms (except for the important class, which has a value of 1000 ms).
- Moderate—This policy is 1 rate and 2 color and has a BC value of 310 ms (except for the important class, which has a value of 1250 ms). These values are 25 percent greater than the strict policy.
- Lenient—This policy is 1 rate and 2 color and has a BC value of 375 ms (except for the important class, which has a value of 1500 ms). These values are 50 percent greater than the strict policy.
- None—No control plane policy is applied.

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

The 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. The default CoPP policy does not change when you upgrade the Cisco NX-OS software on your device.

Caution Selecting the none option and not subsequently configuring CoPP protection can leave your Cisco NX-OS device vulnerable to DoS attacks.

You can reassign the CoPP default policy by entering the setup utility again using the **setup** command from the CLI prompt. Any changes you have made to the CoPP configuration are lost.

If you are using a CoPP default policy, we recommend that you reapply the CoPP default policy using the **setup** command after you upgrade to Cisco NX-OS Release 4.2(1) or later.

Related Topics

- Changing or Reapplying the Default CoPP Policy, page 21

Default Class Maps

The copp-system-class-exception class has the following configuration:

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

The copp-system-class-critical class has the following configuration:

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

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

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



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

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

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

ip access-list copp-system-acl-pim
    permit pim any 224.0.0.0/24
    permit udp any any eq pim-auto-rp
    permit ahp any 224.0.0.13/32

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

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

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



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



class-map type control-plane match-any copp-system-class-critical
    match access-group name copp-system-acl-igmp
    match access-group name copp-system-acl-msdp
    match access-group name copp-system-acl-bgp
    match access-group name copp-system-acl-eigrp
    match access-group name copp-system-acl-rip

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

```
    match access-group name copp-system-acl-pim
    match access-group name copp-system-acl-bgp6
    match access-group name copp-system-acl-ospf6
    match access-group name copp-system-acl-pim6
    match access-group name copp-system-acl-vpc
    match access-group name copp-system-acl-mac-l2pt
    match access-group name copp-system-acl-mac-otv-isis

    match access-group name copp-system-acl-mac-fabricpath-isis
```

The copp-system-class-important class has the following configuration:

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



ip access-list copp-system-acl-vrrp
    permit 112 any 224.0.0.0/24

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

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

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

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

ip access-list copp-system-acl-wccp
    permit udp any any eq 2048
    permit udp any eq 2048 any eq 2048



class-map type control-plane match-any copp-system-class-important
    match access-group name copp-system-acl-hsrp
    match access-group name copp-system-acl-vrrp
    match access-group name copp-system-acl-glbp
    match access-group name copp-system-acl-pim-reg
    match access-group name copp-system-acl-icmp6-msgs
    match access-group name copp-system-acl-cts
    match access-group name copp-system-acl-wccp
    match access-group name copp-system-acl-mac-lldp
    match access-group name copp-system-acl-mac-flow-control
```

The copp-system-class-management class has the following configuration:

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

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

```
    permit udp any eq 1646 any

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

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

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

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

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

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

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

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

ipv6 access-list copp-system-acl-radius6
    permit udp any any eq 1812
    permit udp any any eq 1813
    permit udp any any eq 1645
    permit udp any any eq 1646
    permit udp any eq 1812 any
    permit udp any eq 1813 any
    permit udp any eq 1645 any
    permit udp any eq 1646 any

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

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

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

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

class-map type control-plane match-any copp-system-class-management
    match access-group name copp-system-acl-tacacs
    match access-group name copp-system-acl-radius
```

```
    match access-group name copp-system-acl-ntp
    match access-group name copp-system-acl-ftp
    match access-group name copp-system-acl-tftp
    match access-group name copp-system-acl-sftp
    match access-group name copp-system-acl-ssh
    match access-group name copp-system-acl-snmp
    match access-group name copp-system-acl-telnet
    match access-group name copp-system-acl-tacacs6
    match access-group name copp-system-acl-radius6
    match access-group name copp-system-acl-ntp6
    match access-group name copp-system-acl-tftp6
    match access-group name copp-system-acl-ssh6
    match access-group name copp-system-acl-telnet6
```

The copp-system-class-normal class has the following configuration:

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



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

The copp-system-class-redirect class has the following configuration:

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

The copp-system-class-monitoring class has the following configuration:

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

ip access-list copp-system-acl-traceroute
    permit icmp any any ttl-exceeded
    permit icmp any any port-unreachable

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

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

The copp-system-class-l2-unpoliced class has the following configuration:

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

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

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

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

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

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

The copp-system-class-l2-default class has the following configuration:

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

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

The copp-system-class-undesirable class has the following configuration:

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

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

The copp-system-acl-mac access lists have the following configuration:

```
mac access-list copp-system-acl-mac-cdp-udld-vtp
  permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-acl-mac-cfsoe
  permit any 0180.c200.000e 0000.0000.0000 0x8843
mac access-list copp-system-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-acl-mac-flow-control
  permit any 0180.c200.0001 0000.0000.0000 0x8808
mac access-list copp-system-acl-mac-gold
  permit any any 0x3737
mac access-list copp-system-acl-mac-l2mp-isis
  permit any 0180.c200.0015 0000.0000.0000
  permit any 0180.c200.0014 0000.0000.0000
mac access-list copp-system-acl-mac-l2pt
  permit any 0100.0ccd.cdd0 0000.0000.0000
mac access-list copp-system-acl-mac-lacp
  permit any 0180.c200.0002 0000.0000.0000 0x8809
mac access-list copp-system-acl-mac-lldp
  permit any 0180.c200.000c 0000.0000.0000 0x88cc
mac access-list copp-system-acl-mac-stp
  permit any 0100.0ccc.cccd 0000.0000.0000
  permit any 0180.c200.0000 0000.0000.0000
mac access-list copp-system-acl-mac-undesirable
  permit any any
```

Strict Default CoPP Policy

The strict CoPP policy has the following configuration:

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

    class copp-system-class-exception

        police cir 360 kbps bc 250 ms conform transmit violate drop

    class copp-system-class-critical
```

```
        police cir 39600 kbps bc 250 ms conform transmit violate drop
    class copp-system-class-important
        police cir 1060 kbps bc 1000 ms conform transmit violate drop
    class copp-system-class-management
        police cir 10000 kbps bc 250 ms conform transmit violate drop
    class copp-system-class-normal
        police cir 680 kbps bc 250 ms conform transmit violate drop
    class copp-system-class-redirect
        police cir 280 kbps bc 250 ms conform transmit violate drop
    class copp-system-class-monitoring
        police cir 130 kbps bc 1000 ms conform transmit violate drop
    class copp-system-class-l2-unpoliced
        police cir 8 gbps bc 5 mbytes conform transmit violate transmit
    class copp-system-class-l2-default
        police cir 100 kbps bc 250 ms conform transmit violate drop
    class copp-system-class-undesirable
        police cir 32 kbps bc 250 ms conform drop violate drop
    class class-default
        police cir 100 kbps bc 250 ms conform transmit violate drop
```

Moderate Default CoPP Policy

The moderate CoPP policy has the following configuration:

```
policy-map type control-plane copp-system-policy
    class copp-system-class-exception
        police cir 360 kbps bc 310 ms conform transmit violate drop
    class copp-system-class-critical
        police cir 39600 kbps bc 310 ms conform transmit violate drop
    class copp-system-class-important
        police cir 1060 kbps bc 1250 ms conform transmit violate drop
    class copp-system-class-management
        police cir 10000 kbps bc 310 ms conform transmit violate drop
    class copp-system-class-normal
        police cir 680 kbps bc 310 ms conform transmit violate drop
    class copp-system-class-redirect
        police cir 280 kbps bc 310 ms conform transmit violate drop
    class copp-system-class-monitoring
        police cir 130 kbps bc 1250 ms conform transmit violate drop
```

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

    class copp-system-class-l2-default
        police cir 100 kbps bc 310 ms conform transmit violate drop

    class copp-system-class-undesirable

        police cir 32 kbps bc 310 ms conform drop violate drop

    class class-default

        police cir 100 kbps bc 310 ms conform transmit violate drop
```

Lenient Default CoPP Policy

The lenient CoPP policy has the following configuration:

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

    class copp-system-class-exception

        police cir 360 kbps bc 375 ms conform transmit violate drop

    class copp-system-class-critical

        police cir 39600 kbps bc 375 ms conform transmit violate drop

    class copp-system-class-important

        police cir 1060 kbps bc 1500 ms conform transmit violate drop

    class copp-system-class-management

        police cir 10000 kbps bc 375 ms conform transmit violate drop

    class copp-system-class-normal

        police cir 680 kbps bc 375 ms conform transmit violate drop

    class copp-system-class-redirect

        police cir 280 kbps bc 375 ms conform transmit violate drop

    class copp-system-class-monitoring

        police cir 130 kbps bc 1500 ms conform transmit violate drop

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

    class copp-system-class-l2-default
        police cir 100 kbps bc 375 ms conform transmit violate drop

    class copp-system-class-undesirable

        police cir 32 kbps bc 375 ms conform drop violate drop

    class class-default

        police cir 100 kbps bc 375 ms conform transmit violate drop
```

Modular QoS Command-Line Interface

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

The MQC structure consists of the following high-level steps:

SUMMARY STEPS

1. Define a traffic class using the **class-map** command. A traffic class is used to classify traffic.
2. Create a traffic policy using the **policy-map** command. A traffic policy (policy map) contains a traffic class and one or more CoPP features that will be applied to the traffic class. The CoPP features in the traffic policy determine how to treat the classified traffic.
3. Attach the traffic policy (policy map) to the control plane using the **control-plane** and **service-policy** commands.

DETAILED STEPS

Step 1 Define a traffic class using the **class-map** command. A traffic class is used to classify traffic.

Step 2 Create a traffic policy using the **policy-map** command. A traffic policy (policy map) contains a traffic class and one or more CoPP features that will be applied to the traffic class. The CoPP features in the traffic policy determine how to treat the classified traffic.

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

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. To limit traffic on the mgmt0 interface, use ACLs.

Related Topics

- Configuring IP ACLs
- Configuring MAC ACLs

Virtualization Support for CoPP

You can configure CoPP only in the default virtual device context (VDC), but the CoPP configuration applies to all VDCs on the Cisco NX-OS device. For more information on VDCs, see the Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.2.

Licensing Requirements for CoPP

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	CoPP requires no 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 an explanation of the Cisco NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2*.

Guidelines and Limitations for CoPP

CoPP has the following configuration guidelines and limitations:

- Cisco recommends that you use the strict default CoPP policy initially and then later modify the CoPP policies 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 modify the CoPP policies.
- All the traffic that you do not specify in the other class maps is put into the last class, the default class. Monitor the drops in this class and investigate if these drops are based on traffic that you do not want or the result of a feature that was not configured and you need to add.
- You must use the setup utility to change or reapply the default copp-system-policy policy. You can access the setup utility using the **setup** command in the CLI.
- After you have configured CoPP, delete anything that is not being used, such as old class maps and unused routing protocols.
- You can use the **statistics per-entry** command in the ACL configuration mode to start logging hit counts per ACL entry.
- You must ensure that the CoPP policy does not filter critical traffic such as routing protocols or interactive access to the device. Filtering this traffic could prevent remote access to the Cisco NX-OS device and require a console connection.
- 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).
- You can use the access control entry (ACE) hit counters in the hardware only for ACL logic. Use the software ACE hit counters and the **show access-lists** and **show policy-map type control-plane** commands to evaluate CPU traffic.
- The Cisco NX-OS device hardware performs CoPP on a per-forwarding-engine basis. CoPP does not support distributed policing. Therefore, you should choose rates so that the aggregate traffic does not overwhelm the supervisor module.
- To get a more granular view of traffic that reaches the supervisor and might be dropped by CoPP, you can use the NetFlow feature on SVIs. To do so, compare the ACL hit counts by the values listed in the NetFlow table.

•
• The following rules apply for Cisco NX-OS Release 4.2(6):

CoPP supports non-IP and IP traffic classes.
L2PT, OTV-ISIS, and FabricPath-ISIS packets are classified under the copp-system-class-critical policy.
LLDP and flow-control packets are classified under the copp-system-class-important policy.
Dot1x packets are classified under the copp-system-class-normal policy.
STP, CDP, UDLD, VTP, LACP, GOLD, and CFSoE packets are classified under the copp-system-class-l2-unpoliced policy. These packets are only classified; they are not policed. The corresponding policer simply displays the statistics. These packets are always forwarded to the supervisor.
The rest of the non-IP traffic is classified under the copp-system-class-l2-default policy.
IP traffic not matching any of the copp classes is classified under the class-default policy.

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 1: Default CoPP Parameters Settings

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

Configuring CoPP

This section describes how to configure 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 both IP version 4 (IPv4) and IP version 6 (IPv6) packets.

Before You Begin

Ensure that you are in the default VDC.

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

SUMMARY STEPS

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

DETAILED STEPS

	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-all** | **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.

Step 3	**match access-group name** *access-list-name* **Example:** `switch(config-cmap)# match access-group name MyAccessList`	(Optional) 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 control plane policing matching.
Step 4	**match exception** {**ip** | **ipv6**} **icmp redirect** **Example:** `switch(config-cmap)# match exception ip icmp redirect`	(Optional) Specifies matching for IPv4 or IPv6 ICMP redirect exception packets.

	Command or Action	Purpose
Step 5	**match exception** {**ip** | **ipv6**} **icmp unreachable** **Example:** `switch(config-cmap)# match exception ip icmp unreachable`	(Optional) Specifies matching for IPv4 or IPv6 ICMP unreachable exception packets.
Step 6	**match exception** {**ip** | **ipv6**} **option** **Example:** `switch(config-cmap)# match exception ip option`	(Optional) Specifies matching for IPv4 or IPv6 option exception packets.
Step 7	**match protocol arp** **Example:** `switch(config-cmap)# match protocol arp`	Specifies matching for IP Address Resolution Protocol (ARP) packets.
Step 8	**match redirect arp-inspect** **Example:** `switch(config-cmap)# match redirect arp-inspect`	(Optional) Specifies matching for ARP inspection redirected packets.
Step 9	**match redirect dhcp-snoop** **Example:** `switch(config-cmap)# match redirect dhcp-snoop`	(Optional) Specifies matching for Dynamic Host Configuration Protocol (DHCP) snooping redirected packets.

Step 10	**exit**
	
	Example:
	`switch(config-cmap)# exit`
	`switch(config)#`
		Exits class map configuration mode.

Step 11	**show class-map type control-plane** [*class-map-name*] **Example:** `switch(config)# show class-map type control-plane`	(Optional) Displays the control plane class map configuration.
Step 12	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring a Control Plane Policy Map

You must configure a policy map for CoPP, which include policing parameters. If you do not configure a policer for a class, then the default policer conform action is drop. The Cisco NX-OS software supports 1-rate 2-color and 2-rate 3-color policing.

Before You Begin

Ensure that you are in the default VDC.

Ensure that you have configured a control plane class map.

SUMMARY STEPS

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

DETAILED STEPS

	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:
	`switch(config)# policy-map type control-plane ClassMapA`
	`switch(config-pmap)#`
		Specifies a control plane policy map and enters policy map configuration mode. The policy map name can have a maximum of 64 characters and is case sensitive.

Step 3	**class** {*class-map-name* [**insert-before** *class-map-name2*]	**class-default**}
		
		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.
			
			Note The class-default class map is always at the end of the class map list for a policy map.

	Command or Action	Purpose
Step 4	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] | **percent** *percent*} **Example:** `switch(config-pmap-c)# police cir 52000`	Specifies the committed information rate (CIR). The rate range is from 0 to 80000000000. The default CIR unit is bps.
Step 5	**police** [**cir**] {cir-rate [**bps** | **gbps** | **kbps** | **mbps** | **pps**] | **percent** *percent*} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**] **Example:** `switch(config-pmap-c)# police cir 52000 bc 1000`	Specifies the CIR with the committed burst (BC). The CIR range is from 0 to 80000000000 and the BC range is from 0 to 512000000. The default CIR unit is bps and the default BC size unit is **bytes**.
Step 6	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] | **percent** *percent*} **conform** {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}] **Example:** `switch(config-pmap-c)# police cir 52000 conform transmit exceed drop`	Specifies the CIR with the conform action. The CIR range is from 0 to 80000000000. The default rate unit is bps. The range for the *cos-value* and *prec-value* arguments is from 0 to 7. The range for the *dscp-value* argument is from 0 to 63. The options are as follows: • **drop**—Drops the packet. • **set-cos-transmit**—Sets the class of service (CoS) value. • **set-dscp-transmit**—Sets the differentiated services code point value. • **set-prec-transmit**—Sets the precedence value. • **transmit**—Transmits the packet. • **set dscp dscp table cir-markdown-map**—Sets the exceed action to the CIR markdown map. • **set dscp dscp table pir-markdown-map**—Sets the violate action to the PIR markdown map. **Note** You can specify the BC and conform action for the same CIR.
Step 7	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] | **percent** *percent*} **pir** *pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]] **Example:** `switch(config-pmap-c)# police cir 52000 pir 78000 be 2000`	Specifies the CIR with the peak information rate (PIR). The CIR range is from 0 to 80000000000 and the PIR range is from 1 to 80000000000. You can optionally set an extended burst (BE) size. The BE range is from 1 to 512000000. The default CIR unit is bps, the default PIR unit is **bps**, and the default BE size unit is **bytes**. **Note** You can specify the BC, conform action, and PIR for the same CIR.

	Command or Action	Purpose
Step 8	**set cos** [**inner**] *cos-value* **Example:** `switch(config-pmap-c)# set cos 1`	(Optional) Specifies the 802.1Q class of service (CoS) value. Use the inner keyword in a Q-in-Q environment. The range is from 0 to 7. The default value is 0.
Step 9	**set dscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**} **Example:** `switch(config-pmap-c)# set dscp 10`	(Optional) Specifies the differentiated services code point value in IPv4 and IPv6 packets. Use the **tunnel** keyword to set tunnel encapsulation. The range is from 0 to 63. The default value is 0.
Step 10	**set precedence** [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**} **Example:** `switch(config-pmap-c)# set precedence 2`	(Optional) Specifies the precedence value in IPv4 and IPv6 packets. Use the **tunnel** keyword to set tunnel encapsulation. The range is from 0 to 7. The default value is 0.

Step 11	**exit**
	
	Example:
	`switch(config-pmap-c)# exit`
	`switch(config-pmap)#`
		Exits policy map class configuration mode.

Step 12	**exit**
	
	Example:
	`switch(config-pmap)# exit`
	`switch(config)#`
		Exits policy map configuration mode.

Step 13	**show policy-map type control-plane** [**expand**] [**name** *class-map-name*] **Example:** `switch(config)# show policy-map type control-plane`	(Optional) Displays the control plane policy map configuration.
Step 14	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Related Topics

- Configuring a Control Plane Class Map, page 14

Configuring the Control Plane Service Policy

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

Before You Begin

Ensure that you are in the default VDC.

Ensure that you have configured a control plan policy map.

SUMMARY STEPS

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

DETAILED STEPS

	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	**service-policy input** *policy-map-name* **Example:** `switch(config-cp)# service-policy input PolicyMapA`	Specifies a policy map for the input traffic. Repeat this step if you have more than one policy map. Use the **no service-policy input** *policy-map-name* command to remove the policy from the control plane.

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

Step 5	**show running-config copp** [**all**] **Example:** `switch(config)# show running-config copp`	(Optional) Displays the CoPP configuration.
Step 6	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Related Topics

- Configuring a Control Plane Policy Map, page 16

Changing or Reapplying the Default CoPP Policy

You can change to a different default CoPP policy using the setup utility. You can also reapply the same CoPP default policy.

Before You Begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. **setup**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**setup** **Example:** `switch# setup`	Enters the setup utility.

Related Topics

- Changing or Reapplying the Default CoPP Policy, page 24

Displaying the CoPP Configuration Status

You can display the CoPP feature configuration status information.

Before You Begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. **show copp status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show copp status** **Example:** `switch# show copp status`	Displays CoPP feature configuration status information.

Monitoring CoPP

You can monitor CoPP.

Before You Begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. **show policy-map interface control-plane**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show policy-map interface control-plane** **Example:** `switch# show policy-map interface control-plane`	Displays control plane statistics.

Clearing the CoPP Statistics

You can clear the CoPP statistics.

Before You Begin

Ensure that you are in the default VDC.

SUMMARY STEPS

1. (Optional) **show policy-map interface control-plane**
2. **clear copp statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show policy-map interface control-plane** **Example:** `switch# show policy-map interface control-plane`	(Optional) Displays control plane statistics.
Step 2	**clear copp statistics** **Example:** `switch# clear copp statistics`	Clears the CoPP statistics.

Verifying the CoPP Configuration

To display CoPP configuration information, perform one of the following tasks:

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 ip access-lists [*acl-name*]	Displays the access lists, including the ACLs. If the **statistics per-entry** command is used, it also displays hit counts for specific entries.
show policy-map interface control-plane	Displays the policy values with associated class maps. It also displays drops per policy or class map.
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	Displays the control plane policy map with associated class maps and CIR and BC values.
show running-config copp [**all**]	Displays the CoPP configuration in the running configuration.
show startup-config copp	Displays the CoPP configuration in the startup configuration.

For detailed information about the fields in the output from these commands, see the Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.2.

Configuration Examples for CoPP

This section includes example CoPP configurations.

CoPP Configuration Example

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Changing or Reapplying the Default CoPP Policy

This following example shows how to change or reapply the default CoPP policy using the setup utility:

```
switch# setup

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

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


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


Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
```

```
to skip the remaining dialogs.

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

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

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

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

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

  Enter the switch name : <CR>

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

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

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

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

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

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

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

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

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

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

  Configure best practices CoPP profile (strict/moderate/lenient/none) [strict]: strict

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

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

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

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

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

switch#
```

Using CoPP to Enable a VTY Access Class

Cisco NX-OS currently does not offer the ability to set an access class on VTYs in the same way that Cisco IOS does. However, you can use a CoPP policy to achieve the equivalent of a VTY access class.

To do so, you must explicitly define ACLs used in the CoPP policy to match allowed traffic (and police that to a given rate) as well as define CoPP policies to match denied traffic and drop that traffic. CoPP is different from ACLs in that you cannot use "deny ip any any" as a policy. Rather, you must use "permit" to match the undesired traffic and then use the policer to "drop" that traffic.

The following example shows how to permit access from the 30.30.30.0/24 subnet in order to deploy CoPP to provide the equivalent of a VTY access class. This example explicitly allows

Telnet/SSH/SNMP/NTP/RADIUS/TACACS+ inbound from 30.30.30/24 and anything outbound from the switch to 30.30.30.0/24.

```
ip access-list copp-system-acl-allow
  10 remark ### ALLOW TELNET from 30.30.30.0/24
  20 permit tcp 30.30.30.0/24 any eq telnet
  30 permit tcp 30.30.30.0/24 any eq 107
  40 remark ### ALLOW SSH from 30.30.30.0/24
  50 permit tcp 30.30.30.0/24 any eq 22
  60 remark ### ALLOW SNMP from 30.30.30.0/24
  70 permit udp 30.30.30.0/24 any eq snmp
  80 remark ### ALLOW TACACS from 30.30.30.0/24
  90 permit tcp 30.30.30.0/24 any eq tacacs
  100 remark ### ALLOW RADIUS from 30.30.30.0/24
  110 permit udp 30.30.30.0/24 any eq 1812
  120 permit udp 30.30.30.0/24 any eq 1813
  130 permit udp 30.30.30.0/24 any eq 1645
  140 permit udp 30.30.30.0/24 any eq 1646
  150 permit udp 30.30.30.0/24 eq 1812 any
  160 permit udp 30.30.30.0/24 eq 1813 any
  170 permit udp 30.30.30.0/24 eq 1645 any
  180 permit udp 30.30.30.0/24 eq 1646 any
  190 remark ### ALLOW NTP from 30.30.30.0/24
  200 permit udp 30.30.30.0/24 any eq ntp
  210 remark ### ALLOW ALL OUTBOUND traffic TO 30.30.30.0/24
  220 permit ip any 30.30.30.0/24
  statistics  # keep statistics on matches
ip access-list copp-system-acl-deny
  10 remark ### this is a catch-all to match any other traffic
  20 permit ip any any
  statistics  # keep statistics on matches
class-map type control-plane match-any copp-system-class-management-allow
  match access-group name copp-system-acl-allow
class-map type control-plane match-any copp-system-class-management-deny
  match access-group name copp-system-acl-deny
policy-map type control-plane copp-system-policy
    class copp-system-class-management-allow
        police cir 60000 kbps bc 250 ms conform transmit violate drop
    class copp-system-class-management-deny
        police cir 60000 kbps bc 250 ms conform drop violate drop
control-plane
  service-policy input copp-system-policy
```

Preventing CoPP Overflow by Splitting ICMP Pings and ARP Requests

Some servers use ICMP pings and ARP requests 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 and ARP requests, 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 and ARP requests based on subnets or groups of subnets. Then if a server malfunctions and overflows CoPP, the supervisor answers the ICMP pings and ARP requests only on some subnetworks.

The last entry in the class map or policy map should identify all of the ICMP pings and ARP requests 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 and ARP. In this case, you would need to update the ACLs related to ICMP and ARP.

Note Per the default CoPP, ICMP pings fall under copp-system-class-monitoring, and ARP requests fall under copp-system-class-normal.

The following example shows how to prevent CoPP overflow by splitting ICMP and ARP requests.

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

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

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

Add these ACLs to the new class maps for CoPP:

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

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

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

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

```
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-4
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-10
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-1
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-2
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-3
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-4
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-10
      police cir X kbps bc X ms conform transmit violate drop
```

Delete ICMP and ARP from the existing class maps:

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

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

Additional References for CoPP

This section provides additional information related to implementing CoPP.

Related Documents

Related Topic	Document Title
Licensing	*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2*
Command reference	Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.2

Standards

Standards	Title
RFC 2698	A Two Rate Three Color Marker

Feature History for CoPP

This table lists the release history for this feature.

Table 2: Feature History for CoPP

Feature Name	Releases	Feature Information
CoPP	4.2(6)	Updated the default policies with support for MAC access

Feature Name	Releases	Feature Information
		lists and Layer 2 default and unpoliced classes. Also modified existing class maps to include support for ACL MAC L2PT, FabricPath, LLDP, flow control, and dot1x.
CoPP	4.2(3)	Updated the default policies with support for ACL DHCP.
CoPP	4.2(1)	Updated the default policies with support for WCCP and Cisco TrustSec.