Configuring Control-Plane Policing

This chapter describes how to configure Control-Plane Policing (CoPP) on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as the Cisco CG-OS router).

This chapter includes the following sections:

Information About CoPP

To prevent the Cisco CG-OS router from Denial of Service (DoS) attacks, the system employs control-plane policing (CoPP or CPP). CoPP increases security on the router by protecting the system from unnecessary or DoS traffic and gives priority to important control-plane and management traffic.

To protect the control plane against DoS attacks and to restrict specific flows, there should be a flexible way to police different classes of traffic destined to the CPU.

For information on deploying CoPP:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

For information on CoPP best practices:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

CoPP can protect the control and management planes and ensure routing stability, accessibility, and packet delivery. CoPP uses a dedicated control-plane configuration through Cisco Modular QoS CLI (MQC) to provide filtering and rate-limiting capabilities for control-plane packets. (See Using Modular CLI in the *Cisco 1000 Series Connected Grid Routers QoS Software Configuration Guide.*) CoPP policy can be used to protect the CPU from DoS attacks by restricting SYNC packets, FIN packets, and IP fragments.

CoPP manager (Coppmgr) is the part of CG-OS that processes control-plane configuration commands. Because CoPP uses MQC, it must interact with the Access Control List (ACL) manager for the ACLs, and the QoS manager for the class maps.

When a CoPP policy refers to a QoS class map, the QoS manager sends the changes in the class map to the clients that use the policy. Similarly, when an ACL, referenced by CoPP policy, changes, the CG-OS software sends that change to the client by employing the ACL manager.

Key Concepts

CoPP involves the following actions:

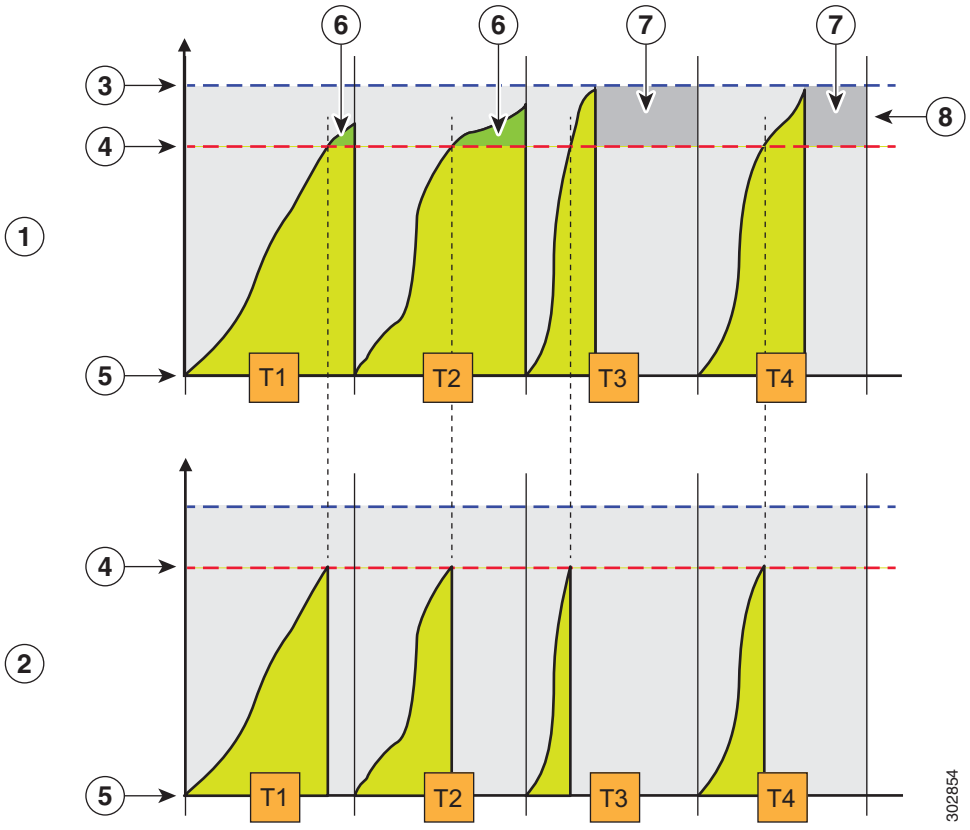
Rate—Defines the amount of traffic sent by the Cisco CG-OS router in a given interval.

Policing—The process of limiting traffic to a prescribed rate. Allows the definition of a rate and a burst. The router does not forward any further traffic for a given interval after the specified amount has passed through the interface.

Burst—Defines the amount of traffic that can be held in the queue for future transmission. Traffic in excess of the burst can be either dropped or have its priority setting reduced.

Figure 10-1 demonstrates that committed information rate (CIR) [4] and burst rate [3] are integral to policing. While the traffic allowed within the time window is at the rate of committed information rate, traffic is only dropped after the burst rate is reached.

Figure 10-1 QoS Policing



1	QoS with burst	**2**	QoS without burst (Cisco CG-OS router)
3	Burst rate (maximum bytes)	**4**	CIR (bytes)
5	Zero (bytes)	**6**	Actual burst
7	No traffic received	**8**	Burst rate
T	Sampling window		

The CG-OS router does not have a burst rate [8]. The sampling window duration [T*x*] is in seconds. The CIR [4] is in packets per second. The router drops packets that exceed the CIR setting [7]. The router does not support additional actions such as marking traffic.

In Figure 10-1, at 5-second intervals, the router allows for the committed number of packets [4] for the specified flow and drops additional packets. The committed number of packets [4] is calculated by multiplying by 5 the committed information rate provided in the input.

Prerequisites

Refer to the Before You Begin paragraph at the beginning of each section for prerequisites.

Guidelines and Limitations

The Cisco CG-OS router supports a limited set of the policing parameters for CoPP.

The router supports the following commands shown in bold:

```
router(config)# policy-map type control-plane copp_policy
router(config-pmap)# class copp_class
router(config-pmap-c)# police ?
<CR>
cir         Specify committed information rate
<CR>
router(config-pmap-c)# police cir ?
  <1-100000>  Committed Information Rate in pps
router(config-pmap-c)# police cir 50 ?
<CR>
pps            Packets per second
```

The CG-OS router does not support the following CoPP policing parameters when defining a policy map and class-map at the (config-pmap-c)# prompt:

- <1-512000000>–Defines the committed burst size in bytes
- bc–Specifies committed burst
- bps–Specifies bits per second
- conform–Specifies a conform action
- gbps–Specifies gigabits per second
- kbps–Specifies kilobits per second
- mbps–Specifies kilobits per second

- pir–Specifies a peak information rate

Default Settings

Table 10-1 Default Settings

Parameters	Default
class-map type control-plane	match-any

Configuring CoPP

This section includes the following topics:

Configuring an ACL

A CoPP policy protects the CPU from DoS attacks by restricting synchronization (sync) packets, finish (FIN) packets and IP fragments.

This section provides details on configuring an ACL for CoPP.

See Configuring IP ACLs in this guide for more information on configuring ACLs on the Cisco CG-OS router.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip access-list default_copp_acl**	Creates or accesses the IP ACL, named default_copp_acl, and enters IP ACL configuration mode.
Step 3	**permit tcp any any syn**	Defines the traffic match conditions that the router permits for synchronization.

	Command	Purpose
Step 4	**permit tcp any any fin**	Defines the traffic match conditions that the router permits for finish packets.
Step 5	**permit ip any any fragments**	Defines the traffic match conditions that the router permits for IP packets.

EXAMPLE

This example shows how to create the ACL, default_copp_acl, and define ACL permits.

```
router# configure terminal
router(config-acl)# ip access-list default_copp_acl
router(config-acl)# permit tcp any any syn
router(config-acl)# permit tcp any any fin
router(config-acl)# permit ip any any fragments
```

Configuring a Class Map

Create a class map for the control-plane and classify traffic based on the ACL.

See Configuring Priority Queuing in the *Cisco 1000 Series Connected Grid Routers QoS Software Configuration Guide* for more information on configuring class maps on the Cisco CG-OS router.

BEFORE YOU BEGIN

Configure an ACL. *See* Configuring an ACL.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**class-map type control-plane match-any default_copp_class**	Creates or accesses the class-map for the control-plane, and then enters class-map qos mode.
Step 3	**match access-group name default_copp_acl**	Creates or accesses the traffic class by matching packets based on the *acl-name*, default_copp_acl. The system ignores permit and deny ACL keywords in the matching.

EXAMPLE

This example shows how to create the class-map for the control-plane.

```
router# configure terminal
router(config)# class-map type control-plane match-any default_copp_class
router(config-cmap)# match access-group name default_copp_acl
```

Configuring a Policy Map

Configure a policy map for the control-plane and define a policing action within a subordinate class map.

See Configuring Priority Queuing in the Cisco 1000 Series Connected Grid Routers QoS Software Configuration Guide for more information on configuring policy maps on the Cisco CG-OS router.

BEFORE YOU BEGIN

See Guidelines and Limitations for a summary of supported policing commands.

Create a class map. (*See* Configuring a Class Map.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**policy-map type control-plane default_copp_policy**	Creates or accesses the policy map and then enters policy-map mode for the policy-map name that you specify. Policy-map names can contain alphabetic, hyphen, or underscore characters, are case sensitive, and can be up to 40 characters.
Step 3	**class copp_class**	Configures the class map and then enters the class-map qos mode.
Step 4	**police cir** *value* **pps**	Specifies the CIR policing rate in packets per second (pps). *value*–1 to 100000 **Note** The router drops packets that exceed the CIR setting.

EXAMPLE

This example shows how to define a policing action for the control-plane policy map.

```
router# configure terminal
router(config)# policy-map type control-plane default_copp_policy
router(config-pmap)# class copp_class
router(config-pmap-c)# police cir 50 pps
```

Configuring the Control-Plane

Apply the policy map created in Configuring a Policy Map to the control-plane.

BEFORE YOU BEGIN

Create a policy map. (See Configuring a Policy Map.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**control-plane**	Enters the control plane configuration mode.
Step 3	**service-policy input default_copp_policy**	Applies the defined policy to incoming packets on the control plane.

EXAMPLE

This example shows how to apply a policy map to the control-plane.

```
router# configure terminal
router(config)# control-plane
router(config)# service-policy input default_copp_policy
```

Verifying Configuration

To display information about the CoPP configuration, enter any or all of the following commands:

Command	Purpose
show ip traffic	Displays details on processed IP traffic. **Note** In the display, the COPP Drop field refers to the number of dropped packets due to control-plane policing.
show policy-map interface control-plane	Displays the configuration details for the policing policy defined on the control plane.

show commands

show ip traffic

To see whether CoPP has initiated policing to drop packets, enter the **show ip traffic** command.

```
router# show ip traffic

IP Software Processed Traffic Statistics
----------------------------------------
Transmission and reception:
  Packets received: 680962, sent: 26263, consumed: 457,
  Forwarded, unicast: 2027, multicast: 0, Label: 0
Opts:
  end: 0, nop: 0, basic security: 0, loose source route: 0
  timestamp: 0, record route: 0
  strict source route: 0, alert: 0,
  other: 0
Errors:
  Bad checksum: 0, packet too small: 0, bad version: 0,
  Bad header length: 0, bad packet length: 0, bad destination: 0,
  Bad ttl: 0, could not forward: 3826, no buffer dropped: 0,
  Bad encapsulation: 46045, no route: 0, non-existent protocol: 0
  Bad options: 0
  Stateful Restart Recovery: 0,  MBUF pull up fail: 0
  Bad context id: 0, rpf drops: 0
  Ingress Drop (ifmgr init): 0,
  Ingress Drop (invalid filter): 0
  Ingress Drop (Invalid L2 msg): 0
  ACL Filter Drops :
       Ingress - 0
       Egree -   0
       Directed Broadcast - 0
  COPP Drop : 90,               <-- CoPP drop packets
```

```
Fragmentation/reassembly:
  Fragments received: 10, fragments sent: 0, fragments created: 0,
  Fragments dropped: 9, packets with DF: 0, packets reassembled: 0,
```

show policy-map interface control-plane

To review configuration details for the policing policy defined on the control plane, enter the **show policy-map interface control-plane** command:

```
router# show policy-map interface control-plane
Control Plane
  service-policy  input: copp_policy
    class-map copp_class match-any
      match access-group name copp_acl
      police cir 2000 pps <-- Committed Information Rate (CIR)
```

Configuration Example

This example shows how to configure an IP ACL named default_copp_a, create a control-plane policy map with a class map that specifies policing as an action, and apply that policy map to the control-plane.

```
router# configure terminal
router(config-acl)# ip access-list default_copp_acl
router(config-acl)# permit tcp any any syn
router(config-acl)# permit tcp any any fin
router(config-acl)# permit ip any any fragments
router(config-acl)# exit
router(config)# class-map control-plane match-any default_copp_class
router(config-cmap)# match access-group name default_copp_acl
router(config-cmap)# exit
router(config)# policy-map type control-plane default_copp_policy
router(config-pmap)# class copp_class
router(config-pmap-c)# police cir 50 pps
router(config-pmap-c)# exit
router(config)# control-plane
router(config)# service-policy input default_copp_policy
router(config)# copy running-config startup-config
```

Feature History

Feature Name	Release	Feature Information
Control-Plane Policing	Cisco CG-OS Release CG2(1)	Initial support of the feature on the CGR 1000 Series Routers.