**Discovery 26: Configure Control Plane Policing**

**Introduction**

Through this discovery, you will learn how to configure a CoPP policy. CoPP allows you to use the MQC (Modular QoS CLI) framework to permit, deny, or rate-limit traffic that goes to the route processor. For this discovery, you will police OSPF, VRRP, ICMP, and Telnet traffic being sent to R1’s control plane.

The discovery is prepared with the devices that are represented in the topology diagram and configured according to the information in the Job Aids section. R1 and R2 are running OSPFv2 and VRRP. PC1 will be used to generate ICMP traffic and establish a Telnet session with R1.

Your configuration tasks are as follows:

* Configure and verify CoPP on R1 to police OSPF, VRRP, ICMP, and Telnet traffic.

**Task 1: Configure and Verify CoPP on R1**

**CoPP Configuration**

To configure Control Plane Policing, you must complete the following tasks:

* Create ACLs that will identify the control plane traffic that needs to be policed by CoPP. The definition of these ACLs is one of the most critical steps in the CoPP process. MQC uses these ACLs to define the traffic classes, which in turn become the object of the policy actions (policing).
* Create traffic classes that describe valid control plane traffic (ACL permit statements). You can configure as many traffic classes as you need, depending on the required granularity of your policy.
* Create a traffic policy that will permit, deny, or rate-limit the configured traffic classes and therefore conserve process layer resources, or even act as a device firewall by hiding most device resources from the network.
* Apply the configured traffic policy to the control plane.

**Activity**

**Step 1:** On R1, configure the following ACLs. These ACLs will be used to identify traffic going to the router’s management and control plane and that will be policed by CoPP

| **ACL Name** | **Protocol** | **Source IP Address** | **Destination IP Address** | **Destination Port** |
| --- | --- | --- | --- | --- |
| COPP-ICMP | ICMP | ANY | ANY | -- |
| COPP-TELNET | TCP | ANY | ANY | 23 |
| COPP-OSPF | OSPF | ANY | ANY | -- |
| COPP-VRRP | 112 (VRRP) | ANY | Host 224.0.0.18 | -- |

On R1, enter the following commands:

R1(config)# ip access-list extended COPP-ICMP

R1(config-ext-nacl)# permit icmp any any

R1(config-ext-nacl)# ip access-list extended COPP-TELNET

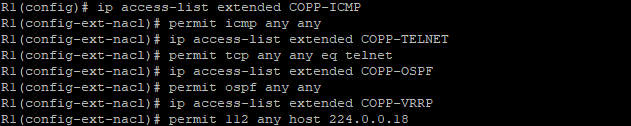
R1(config-ext-nacl)# permit tcp any any eq telnet

R1(config-ext-nacl)# ip access-list extended COPP-OSPF

R1(config-ext-nacl)# permit ospf any any

R1(config-ext-nacl)# ip access-list extended COPP-VRRP

R1(config-ext-nacl)# permit 112 any host 224.0.0.18



The COPP-ICMP ACL will match any ICMP packets sent to the router, the COPP-TELNET ACL will match any Telnet sessions initiated with the router, the COPP-OSPF ACL will match any OSPF packets it receives, and the COPP-VRRP ACL will match any multicast VRRP messages received by R1. Notice the use of protocol number 112 in the VRRP ACL. VRRP messages are neither UDP nor TCP. Instead, VRPP was assigned protocol number 112 by IANA, in the same way that EIGRP was assigned number 88 and OSPF was assigned number 89. Also, VRRP uses the multicast address 224.0.0.18 to transmit messages on the local segment.

Note that a DENY statement in the ACL will still forward packets to the control plane but the packets will not be policed. This is useful when certain trusted hosts should have unfettered access to a device’s control plane, for example for Telnet or SSH.

**Step 2:** On R1, configure the following class maps. The class maps will be used to classify traffic for CoPP.

| **Class Map Name** | **Match** |
| --- | --- |
| COPP-MAP-ICMP | ACL Name: COPP-ICMP |
| COPP-MAP-TELNET | ACL Name: COPP-TELNET |
| COPP-MAP-OSPF | ACL Name: COPP-OSPF |
| COPP-MAP-VRRP | ACL Name: COPP-VRRP |

On R1, enter the following commands:

R1(config)# class-map COPP-MAP-ICMP

R1(config-cmap)# match access-group name COPP-ICMP

R1(config-cmap)# class-map COPP-MAP-TELNET

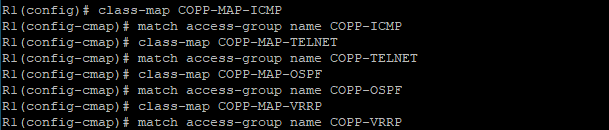
R1(config-cmap)# match access-group name COPP-TELNET

R1(config-cmap)# class-map COPP-MAP-OSPF

R1(config-cmap)# match access-group name COPP-OSPF

R1(config-cmap)# class-map COPP-MAP-VRRP

R1(config-cmap)# match access-group name COPP-VRRP



Each class map is associated with the appropriate ACL for CoPP traffic classification.

**Step 3:** On R1, configure a policy map with the name ROUTER-COPP-POLICY. This policy map will be used to apply Control Plane Policing actions to the traffic classes already configured.

| **Class Name** | **Action** |
| --- | --- |
| COPP-MAP-ICMP | Police to 8 kbps, conform action transmit, exceed action drop |
| COPP-MAP-TELNET | Police to 100 kbps, conform action transmit, exceed action drop |
| COPP-MAP-OSPF | Police to 300 kbps, conform action transmit, exceed action drop |
| COPP-MAP-VRRP | Police to 50 kbps, conform action transmit, exceed action drop |
| Class-default | Police to 12 kbps, conform action transmit, exceed action transmit |

On R1, enter the following commands:

R1(config)# policy-map ROUTER-COPP-POLICY

R1(config-pmap)# class COPP-MAP-ICMP

R1(config-pmap-c)# police 8000 conform-action transmit exceed-action drop

R1(config-pmap-c)# exit

R1(config-pmap)# class COPP-MAP-TELNET

R1(config-pmap-c)# police 100000 conform-action transmit exceed-action drop

R1(config-pmap-c)# exit R1(config-pmap)# class COPP-MAP-OSPF

R1(config-pmap-c)# police 300000 conform-action transmit exceed-action drop

R1(config-pmap-c)# exit

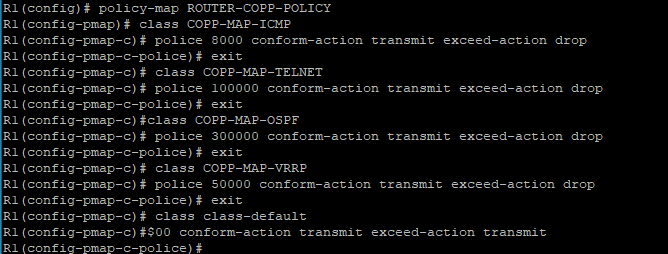
R1(config-pmap)# class COPP-MAP-VRRP

R1(config-pmap-c)# police 50000 conform-action transmit exceed-action drop

R1(config-pmap-c)# exit

R1(config-pmap)# class class-default

R1(config-pmap-c)# police 12000 conform-action transmit exceed-action transmit



The ICMP class map is policed to 8000 bps to allow easy testing of the CoPP policy in the next steps. Notice that a new class map is included at the end of the policy map. The class-default class map is automatically placed at the end of the policy map. Match criteria cannot be configured for class-default because it automatically includes an implied match for all packets. By the nature of CoPP matching mechanisms, certain traffic types will always end up falling into the default class. This includes traffic such as Layer 2 keepalives and non-IP traffic such as certain IS-IS packets. Because these traffic types are required to maintain the network control plane, class-default should never be policed with both conform and exceed being set with an action of drop. It is also generally considered best practice never to rate-limit the class-default class. It is done here simply to serve as an example.

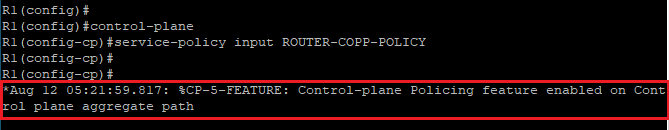
**Step 4:** On R1, apply the CoPP policy map to the control plane.

On R1, enter the following commands:

R1(config)# control-plane

R1(config-cp)# service-policy input ROUTER-COPP-POLICY

R1(config-cp)#

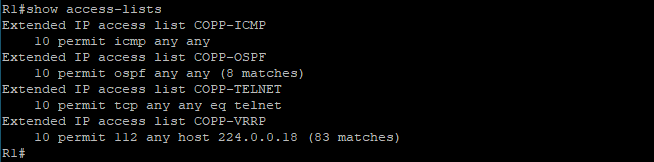


The policy map is applied to the control plane virtual interface in the inbound direction. Only traffic destined for the device’s route processor will be affected by the CoPP policy.

**Step 5:** On R1, verify the CoPP configuration.

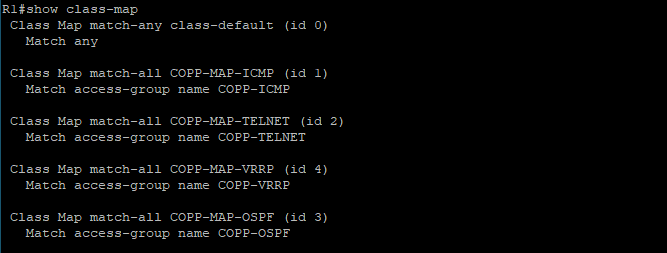
On R1, enter the following commands:

R1# show access-lists



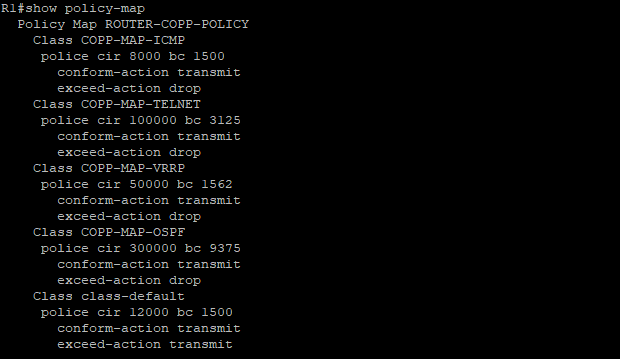
Within a few moments of the CoPP policy being applied, you should already see ACL matches for OSPF and VRRP packets (hellos) since those two protocols were preconfigured on R1 and R2. There will be no matches yet for ICMP or Telnet traffic. You will generate that traffic from PC1 in the next step.

R1# show class-map



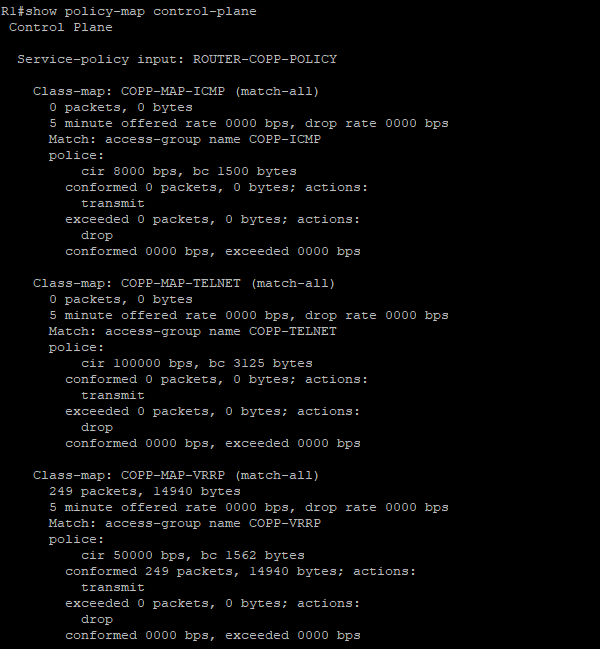
The only class maps configured are those used for CoPP. Notice the match any statement under the class-default class map. This match statement was automatically added when the class map was included in the policy map configuration.

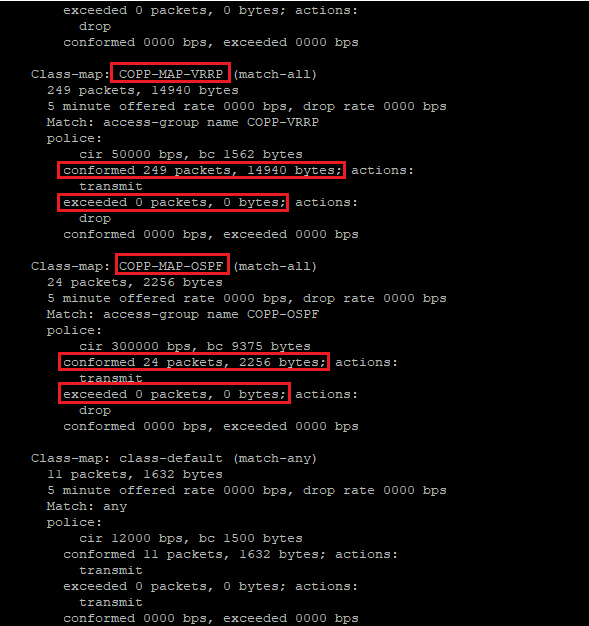
R1# show policy-map



The policy map shows the policing rates that were configured for each class map, including the class-default class map.

R1# show policy-map control-plane



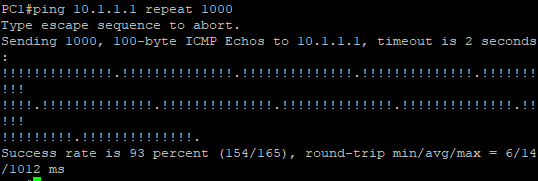


This is the most useful command for verifying CoPP functionality. Notice the OSPF and VRRP packets that conform to the policing rule. Since no packets exceeded the defined rates for the OSPF and VRRP class maps, all packets were transmitted to the control plane for processing. Note that your packet count will naturally vary from the example above.

**Step 6:** From PC1, use the command ping 10.1.1.1 repeat 1000 to simulate a DoS attack on R1’s control plane.

On PC1, enter the following command:

PC1# ping 10.1.1.1 repeat 1000

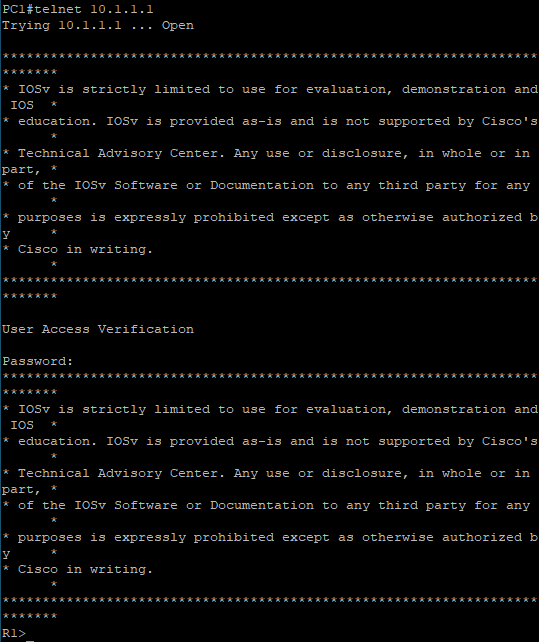


Use the CTRL+SHIFT+6 break sequence to abort the pings after a few seconds. Notice the failed pings as indicated by the period symbol (.) among the exclamation marks. This is an indication the PC1 did not receive an echo-reply ICMP message from R1.

**Step 7:** From PC1, Telnet to R1 using the telnet 10.1.1.1 command. Enter the password (root@123) when prompted.

On PC1, enter the following command:

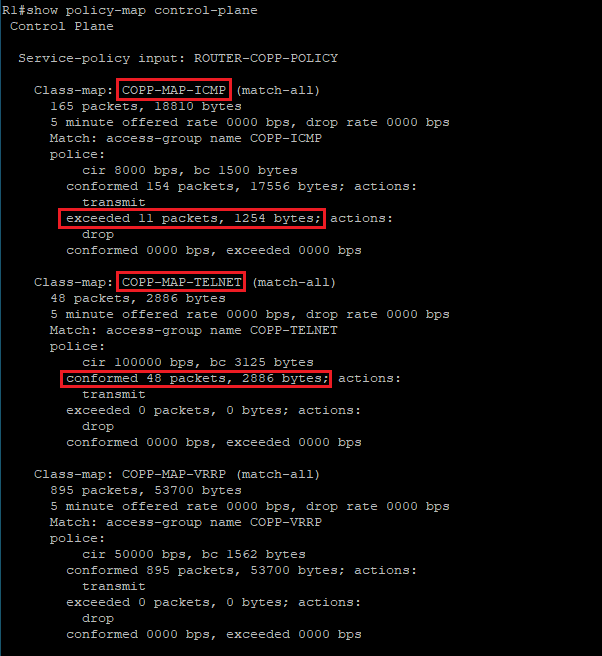
PC1# telnet 10.1.1.1

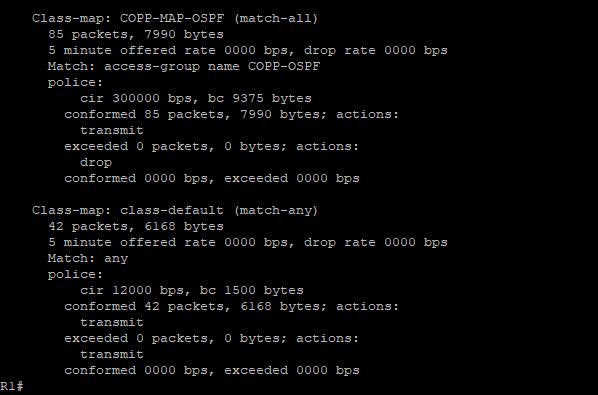


**Step 8:** On R1, use the show policy-map control-plane command to investigate CoPP policing of ICMP and Telnet packets.

On R1, enter the following command:

R1# show policy-map control-plane





The output confirms that some ICMP packets were dropped because they temporarily exceeded the allowed data rate. Obviously, some echo-request messages were successfully transmitted to the control plane and the router replied to PC1 with an icmp-reply message.

The output also shows that all Telnet packets were successfully transmitted to the control plane, with no packets exceeding the configured data rate.

Finally, notice that there is a substantial number of packets that are being matched to the class-default class map. One possible solution to help identify the source of these packets would be to create a “catch-all” class. This new class map would be required to collect any remaining traffic that has not matched any other class and that is destined for the device’s control plane. This “catch-all” class prevents these packets from ending up in class-default. For example, an ACL called COPP-CATCH-ALL could be defined as follows:

R1(config)# ip access-list extended COPP-CATCH-ALL

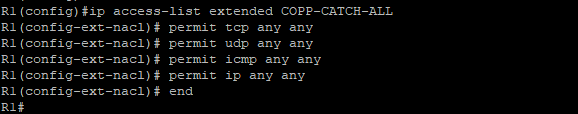
R1(config-ext-nacl)# permit tcp any any

R1(config-ext-nacl)# permit udp any any

R1(config-ext-nacl)# permit icmp any any

R1(config-ext-nacl)# permit ip any any

R1(config-ext-nacl)# end



This ACL could then be matched to a class map called COPP-MAP-CATCH-ALL which could be policed to 50 kbps with a conform action of transmit and an exceed action of drop.

Frequent use of the clear access-list counters command and show access-list command would be useful in tuning all CoPP ACLs. These commands help identify traffic matching each ACL. By being especially aware of traffic matching the new COPP-CATCH-ALL ACL, you be able to identify all previously unmatched traffic. Traffic falling into this class should be investigated to determine if it (1) is legitimate receive-traffic that should have previously been classified (that is, was overlooked in the other ACLs); (2) is attack traffic that should be dropped; or (3) is legitimate transit traffic and acceptable for the new “catch-all” ACL.