Forwarding and QoS Configuration Examples

This section shows examples of how you can use access lists to configure quality of service (QoS), classifying data packets and prioritizing the transmission properties for different classes. Note that QoS is synonymous with class of service (CoS).

Forwarding and QoS Example

This example shows how to configure class of service (CoS) to classify data packets and control how traffic flows out of and in to the interfaces on a vEdge router and on the interface queues. To configure a QoS policy:

1. Map each forwarding class to an output queue.
2. Configure the QoS scheduler for each forwarding class.
3. Group the QoS schedulers into a QoS map.
4. Define an access list to specify match conditions for packet transmission.
5. Apply the access list to a specific interface.
6. Apply the queue map and the rewrite rule to the egress interface.

The sections below show examples of each of these steps.

Map Forwarding Class to Output Queue

This example shows a data policy that classifies incoming traffic by mapping each forwarding class to an output queue. Here, traffic classified as "be" (Best Effort) is mapped to queue 2, traffic classified as "af1" (Assured Forwarding) is mapped to queue 3, and so on.

```
policy
  class-map
    class be queue 2
    class af1 queue 3
    class af2 queue 4
    class af3 queue 5
  !
```

Configure QoS Scheduler for Each Forwarding Class

This example illustrates how to configure the QoS scheduler for each queue to define the importance of data packets. Depending on the priority of the traffic, you assign the bandwidth, buffer level, and random early detection (RED) drop profile associated with the queue. Here, "af3" traffic has higher priority over other traffic classes and so is configured to have 40% bandwidth and 40% buffer. Traffic in class "af2" has 30% bandwidth and 30% buffer; traffic in class "af1" class has 20% bandwidth and 20% buffer and traffic in class "be" has 10% bandwidth and 10% buffer size reflecting the respective priority of the traffic on the network. All traffic classes are configured with a drop profile of RED, meaning that instead of waiting for the queue to be full, packets are dropped randomly based on the thresholds defined.
Group QoS Schedulers into a QoS Map

This example illustrates the grouping of "qos scheduler af1," "qos scheduler af2," and "qos scheduler be" into a single QoS map called "test."

```
policy
  qos-scheduler af1
    class af1
    bandwidth-percent 20
    buffer-percent 20
    drops red-drop
  qos-scheduler af2
    class af2
    bandwidth-percent 30
    buffer-percent 30
    drops red-drop
  qos-scheduler af3
    class af3
    bandwidth-percent 40
    buffer-percent 40
    drops red-drop
  qos-scheduler be
    class be
    bandwidth-percent 10
    buffer-percent 10
    drops red-drop

qos-map test
  qos-scheduler af1
  qos-scheduler af2
  qos-scheduler be
```

Classify Data Packets into Appropriate Class

This example shows how to classify data packets into appropriate forwarding classes based on match conditions. Here "access-list acl1" classifies data packets originating from the host at source address 10.10.10.1 and going to the destination host at 20.20.20.1 into the "be" class. Data packets with a DSCP value of 10 in the IP header field are classified in the "af1" class, TCP packets are classified in the "af3" class, and packets going to destination port 23, which carries Telnet mail traffic, are classified in the "af2" class. All other traffic is dropped.

```
policy
  access-list acl1
    sequence 1
      match
        source-ip 10.10.10.1/32
        destination-ip 20.20.20.1/32
      action accept
        class be
      !
    sequence 2
      match
        dscp 10
      action accept
        class af1
      !
    sequence 3
      match
        protocol 6
      action accept
        class af3
      !```
Apply Access List to Specific Interface

This example illustrates how to apply the access list defined above on the input of a service interface. Here "access-list acl1" is applied on the input of interface ge0/4 in VPN 1.

```
! sequence 4
match
destination-port 23
!
action accept
class af2
!
default-action drop
!
```

Configure Rewrite Rule

This example shows how to configure the rewrite rule to overwrite the DSCP field of the outer IP header. Here the rewrite rule "transport" overwrites the DSCP value for forwarding classes based on the drop profile. Since all classes are configured with RED drop, they can have one of two profiles: high drop or low drop. The rewrite rule is applied only on the egress interface, so on the way out, packets classified as "af1" and a Packet Loss Priority (PLP) level of low are marked with a DSCP value of 3 in the IP header field, while "af1" packets with a PLP level of high are marked with 4. Similarly, "af2" packets with a PLP level of low are marked with a DSCP value of 5, while "af2" packets with a PLP level of high are marked with 6, and so on.

```
policy
 rewrite-rule transport
class af1 low dscp 3
class af1 high dscp 4
class af2 low dscp 5
class af2 high dscp 6
class af3 low dscp 7
class af3 high dscp 8
class be low dscp 1
class be high dscp 2
!
```

Apply the Queue Map and Rewrite Rule on an Interface

This example applies the queue map "test" and the rewrite rule "transport" to the egress interface ge0/0 in VPN 0. (Note that you cannot apply QOS maps to VLAN interfaces, also called subinterfaces.) Queue maps and rewrite rules are applied only on outgoing traffic.

```
vpn 0
 interface ge0/0
 ip address 10.1.15.15/24
 tunnel-interface
 preference 10
 weight 10
 color lte
 allow-service dhcp
 allow-service dns
```
Police Data Packets

This section shows two examples of policing data packets.

The first example illustrates how to configure a policer to rate limit traffic received on an interface. After you configure the policer, include it in an access list. Here "policer p1" is configured to have a maximum traffic rate of 1,000,000 bits per second and a maximum burst-size limit of 15000 bytes. Traffic exceeding these rate limits is dropped. The policer is then included in the access list “acl1,” which is configured to accept all TCP or UDP traffic originating from the host at source 2.2.0.0 and going to the destination host at 10.1.1.0 on port 20 or 100.1.1.0 on port 30. You can use “access-list acl1” on the input or output of the interface to do flow-based policing.

```
policy
policer p1
rate 1000000
burst 15000
exceed drop
!
access-list acl1
sequence 1
match
source-ip 2.2.0.0/16
destination-ip 10.1.1.0/24 100.1.1.0/24
destination-port 20 30
protocol 6 17 23
!
action accept
policer p1
!
!
default-action drop
!
!vpn 1
interface ge0/4
ip address 10.20.24.15/24
no shutdown
access-list acl1 in
!
!
```

You can also apply a policer directly on an inbound or an outbound interface when you want to police all traffic ingressing or egressing this interface:

```
policy
policer p1
rate 1000000
burst 15000
exceed drop
!
!vpn 1
interface ge0/4
ip address 10.20.24.15/24
no shutdown
policer p1 in
!
!
!vpn 2
interface ge0/0
ip address 10.1.15.15/24
```
In the second example, we have a vEdge router with two WAN interfaces in VPN 0. The ge0/0 interface connects to a 30-MB link, and we want to always have 10 MB available for very high priority traffic. When lower-priority traffic bursts exceed 20 MB, we want to redirect that traffic to the second WAN interface, ge0/1.

Implementing this traffic redirection requires two policies:

- You apply an access list to the service-side interface that polices the incoming data traffic.
- You apply a data policy to the ge0/0 WAN interface that directs bursty traffic to the second WAN interface, ge0/1.

For the access list, the configuration snippet belows if for interface ge1/0, in VPN 1. The policer monitors incoming traffic on the interface. When traffic exceeds 20 MB (configured in the **policer burst** command), we change the PLP from low to high (configured by the **policer exceed remark** command). You configure the following on the vEdge router:

```
policy
  policer bursty-traffic
  rate 1000000
  burst 20000
  exceed remark
  access-list policer-bursty-traffic
    sequence 10
      match
        source-ip 56.0.1.0/24
      action accept
  policer bursty-traffic
  default-action accept
vpn 1
interface ge1/0
ip address 56.0.1.14/24
no shutdown
access-list policer-bursty-traffic in
```

To display a count of the packets that have been remarked, issue the **show interface detail** or the **show system statistics** command on the vEdge router. The count is reported in the rx-policer-remark field.

The centralized data policy directs bursty traffic away from the ge0/0 interface (color: internet) to interface ge0/1 (color: red). You apply this data policy to all the routers at a particular site, specifying the direction **from-service** so that the policy is applied only to traffic originating from the service side of the router. You configure the following on the vSmart controller:

```
policy
```

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.1/08Forwarding_and_QoS/03Forwardi...
Additional Information

Forwarding and QoS Overview
Localized Data Policy