

Forwarding and QoS

Forwarding is the transmitting of data packets from one router to another.

Quality of Service (QoS) is synonymous with class of service (CoS). You can enable QoS with localized data policies, which control the flow of data traffic into and out of the interfaces of edge devices.

- Cisco Catalyst SD-WAN Forwarding and QoS Overview, on page 1
- How QoS Works, on page 2
- Limitations for Forwarding on Cisco IOS XE Catalyst SD-WAN Devices, on page 3
- Workflow to Configure QoS Using Cisco SD-WAN Manager, on page 4
- Forwarding and QoS Configuration Using the CLI, on page 9
- Verify Configuration of QoS Policy Map Using the CLI, on page 14
- Reference: Forwarding and QoS CLI Commands, on page 16

Cisco Catalyst SD-WAN Forwarding and QoS Overview

Forwarding takes the data packet and sends it over the transport to the remote side, specifying what to do with the packet. It specifies the interface through which packets are sent to reach the service side of a remote router.

Once the control plane connections of the Cisco Catalyst SD-WAN overlay network are up and running, data traffic flows automatically over the IPsec connections between the routers. Because data traffic never goes to or through the centralized Cisco SD-WAN Controller, forwarding only occurs between the Cisco IOS XE Catalyst SD-WAN devices as they send and receive data traffic.

While the routing protocols running in the control plane provide a router the best route to reach the network that is on the service side of a remote router, there will be situations where it is beneficial to select more specific routes. Using forwarding, there are ways you can affect the flow of data traffic. Forwarding takes the data packet and sends it over the transport to the remote side, specifying what to do with the packet. It specifies the interface through which packets are sent to reach the service side of a remote router.

To modify the default data packet forwarding flow, you create and apply a centralized data policy or a localized data policy. With a centralized data policy, you can manage the paths along which traffic is routed through the network, and you can permit or block traffic based on the address, port, and DSCP fields in the packet's IP header. With a localized data policy, you can control the flow of data traffic into and out of the interfaces of a router, enabling features such as quality of service (QoS).

How QoS Works

The QoS feature on the Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices works by examining packets entering at the edge of the network. With localized data policy, also called access lists, you can provision QoS to classify incoming data packets into multiple forwarding classes based on importance, spread the classes across different interface queues, and schedule the transmission rate level for each queue. Access lists can be applied either in the outbound direction on the interface (as the data packet travels from the local service-side network into the IPsec tunnel toward the remote service-side network) or in the inbound direction (as data packets are exiting from the IPsec tunnel and being received by the local router.

To provision QoS, you must configure each router in the network. Generally, each router on the local service-side network examines the QoS settings of the packets that enter it, determines which class of packets are transmitted first, and processes the transmission based on those settings. As packets leave the network on the remote service-side network, you can rewrite the QoS bits of the packets before transmitting them to meet the policies of the targeted peer router.

Classify Data Packets

You can classify incoming traffic by associating each packet with a forwarding class. Forwarding classes group data packets for transmission to their destination. Based on the forwarding class, you assign packets to output queues. The routers service the output queues according to the associated forwarding, scheduling, and rewriting policies you configure.

Schedule Data Packets

You can configure a QoS map for each output queue to specify the bandwidth. This enables you to determine how to prioritize data packets for transmission to the destination. Depending on the priority of the traffic, you can assign packets higher or lower bandwidth, buffer levels, and drop profiles. Based on the conditions defined in the QoS map, packets are forwarded to the next hop.

On Cisco vEdge devices and Cisco IOS XE Catalyst SD-WAN devices, each interface has eight queues, which are numbered 0 to 7. Queue 0 is reserved, and is used for both control traffic and low-latency queuing (LLQ) traffic. For LLQ, any class that is mapped to queue 0 must also be configured to use LLQ. Queues 1 to 7 are available for data traffic, and the default scheduling for these seven queues is weighted round-robin (WRR). For these queues, you can define the weighting according to the needs of your network. When QoS is not configured for data traffic, queue 2 is the default queue.

Rewrite Data Packets

You can configure and apply rewrite rules on the egress interface to overwrite the Differentiated Services Code Point (DSCP) value for packets entering the network. Rewrite rules allow you to map traffic to code points when the traffic exits the system. Rewrite rules use the forwarding class information and packet loss priority (PLP) used internally by the Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices to establish the DSCP value on outbound packets. You can then configure algorithms such as RED/WRED to set the probability that packets will be dropped based on their DSCP value.

Police Data Packets

You can configure policers to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels.

Shaping Rate

Shaping controls the maximum rate of traffic sent. It enables you to configure the aggregate traffic rate on an interface to be less than the line rate. This allows the interface to transmit less traffic than it is capable of transmitting. You can apply shaping to outbound interface traffic and configure the shaping rate on the egress physical interfaces. Subinterfaces on VLANs do not support shaping.

A token bucket algorithm determines the shaping rate. At a fixed rate, the system places the tokens in an imaginary bucket. Whenever a packet is transmitted, a token is removed from the bucket. When a packet is scheduled to be sent and no token is in the bucket, the packet is held until tokens are available again.



Note

- The cEdge platforms support QoS Shaping on Layer 3 subinterfaces whereas vEdge platforms do not support it.
- The cEdge platform does not support Shaping and QoS policy on bridge interfaces like VLAN and BDI interface.

Policer Burst Tolerance

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

The policer automatically calculates the burst value based on a 250 ms burst tolerance, using the higher user-configured burst value. The burst value adjustment reduces the risk of network congestion. If the user-configured burst value is too low, then the system increases the burst value to match the calculated value, ensuring optimal performance.

For example, if you have a network with a Committed Information Rate (CIR) of 100 Mbps, then the default burst tolerance for this network is set to 250 ms, which equals to 3,125,000 bytes of burst value.

If you set the burst value to 15,000 bytes, the system automatically adjusts to the higher burst tolerance of 3,125,000 bytes. This ensures that the network operates within the appropriate parameters.

Limitations for Forwarding on Cisco IOS XE Catalyst SD-WAN Devices

- Mirroring is not supported.
- Delaying buffer size is not supported.
- Specifying packet loss priority (PLP) is not supported.
- Policers cannot be applied on interfaces. They are applied under local data policy.
- Decreased priority dropping is not supported.
- Access lists applied to the outbound of interface cannot change the QoS classification.

Workflow to Configure QoS Using Cisco SD-WAN Manager

1. Map each forwarding class to an output queue.
2. Create localized policy.
   a. Enable Cloud QoS and Cloud QoS on service side.
   b. Configure QoS scheduler.
   c. (Optional) Create re-write policy.
3. Apply localized policy to device template.
4. Apply QoS map and re-write policy (optional) to WAN interface feature template.
5. Define centralized Traffic Data QoS policy to classify traffic into proper queue.
6. Apply centralized policy.



Note Incorrect QoS configurations may cause crashes on Cisco IOS XE Catalyst SD-WAN devices. Ensure to follow the configuration guidelines carefully.

Map Each Forwarding Class to an Output Queue

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. From the **Custom Options** drop-down, select **Lists** under **Localized Policy**.
3. Select the **Class Map** from the list types.
4. Click the **New Class List**. The Class List pop-up page is displayed.
5. Enter a name for the class. Select a required queue from the **Queue** drop-down list.
6. Click **Save**.
7. Repeat the last three steps to add more class lists as required. The following are example class lists and queue mappings:

Table 1: Class List and Queue Mappings

Class	Queue
VOICE	0
CRTICAL_DATA	1
BULK	2
CLASS_DEFAULT	3

Class	Queue
INTERACTIVE_VIDEO	4
CONTROL SIGNALING	5

Configure Localized Policy

Enable Cloud QoS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. For the desired policy, click **…** and choose **Edit**.

   (Optionally) If the desired policy is not available in the list, you may create a customized localized policy following the steps below:

   a. Click **Add Policy**.

   b. In the Add Policy page, continue to click **Next** till you navigate to Policy Overview page.

   c. In the Policy Overview page, enter **Policy Name** and **Description** for your localized policy.

4. In the Policy Overview page, select the **Cloud QoS** checkbox to enable QoS on the transport side, and select the **Cloud QoS Service side** checkbox to enable QoS on the service side.

Configure QoS Scheduler

1. Click **Forwarding Class/QoS**. When you navigate to the Forwarding Classes/QoS page, QoS Map is selected by default.
2. Click **Add QoS Map**, and then click **Create New**.
3. Enter the name and description for the QoS mapping.
4. Queue 0 has already been defined by default and cannot be modified. Click the **Add Queue**.
5. Select a required queue from the **Queue** drop-down.
6. Slide the **Bandwidth%** and **Buffer%** bar and set the value as required.
7. From the **Drops** drop-down, select the required drop type.
8. Click **Save Queue**.
9. Repeat the last three steps to add more queue as required. The following are the examples for queue and sample Bandwidth/Buffer configurations:

   Table 2: Bandwidth and buffer values and drop algorithm

Queue	Bandwidth/Buffer	Drops
1	30/30	Random Early (RED)

Queue	Bandwidth/Buffer	Drops
2	10/10	Random Early (RED)
3	20/20	Random Early (RED)
4	20/20	Random Early (RED)
5	10/10	Tail Drop

10. QoS queue 0 should now be left at 10% Bandwidth and Buffer.
11. Click **Save Policy**.

Create Re-write Policy

1. (Optional) Click **Policy Rewrite** to add a rewrite policy.
2. From the **Add Rewrite Policy** drop-down, select **Create New**.
3. Enter a name and description for the rewrite rule.
4. Click **Add Rewrite Rule**.
5. In the Add Rule pop-up page:
   a. Select a class from the **Class** drop-down.
   b. Select the priority (**Low** or **High**) from the **Priority** drop-down.

      Low priority is supported only for Cisco IOS XE Catalyst SD-WAN device devices.
   c. Enter the DSCP value (0 through 63) in the **DSCP** field.
   d. Enter the class of service (CoS) value (0 through 7) in the **Layer 2 Class of Service** field.
6. Click **Save Rule**.
7. Repeat the previous 5 and 6 steps to add more QoS Rewrite rules as required. The following are example rewrite rule information:

Table 3: QoS Rewrite Information

Class	Priority	DSCP	Layer 2 Class of Service
BULK	Low	10	1
BULK	High	10	1
DEFAULT	Low	0	0
DEFAULT	High	0	0
CONTROL_SIGNALING	Low	18	2
CONTROL_SIGNALING	High	18	2
CRITICAL_DATA	Low	18	2

Class	Priority	DSCP	Layer 2 Class of Service
CRITICAL_DATA	High	18	2
INTERACTIVE_VIDEO	Low	34	4
INTERACTIVE_VIDEO	High	34	4

8. Click **Save Policy**.
9. Click **Save Policy Changes** to save the changes to the localized master policy.

Apply Localized Policy to the Device Template

Note The first step in utilizing the Localized Policy that is created is to attach it to the device template.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** and select the desired template.

Note In Cisco vManage 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. Click **…**, and click **Edit**.
4. Click **Additional Templates**.
5. From the **Policy** drop-down, choose the Localized Policy that is created in the previous steps.
6. Click **Update**.

Note Once the localized policy has been added to the device template, selecting the **Update** option immediately pushes a configuration change to all of the devices that are attached to this device template. If more than one device is attached to the device template, you will receive a warning that you are changing multiple devices.

7. Click **Next**, and then **Configure Devices**.
8. Wait for the validation process and push configuration from Cisco SD-WAN Manager to the device.

Apply QoS and Re-write Policy to WAN Interface Feature Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Choose a feature template from the list. Click **...**, and click **Edit**.
4. Click **ACL/QoS**.
5. From the **QoS Map** drop-down, select **Global** and enter a name in the field.
6. From the **Rewrite Rule** drop-down, select **Global** and enter a name in the field.
7. To save the feature template changes, click **Update**.

Note The configuration does not take effect till the feature template is attached to the device template.

8. In the left pane, choose the device to view the configuration in the right pane.
9. Click **Configure Devices** to push the policy map. In the pop up page, select the check box and confirm changes on multiple devices. Click **OK**.

Define Centralized Traffic Data QoS Policy to Classify Traffic into Proper Queue

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. For the desired policy in the list, click **...**, and select **Edit**.

   (Optionally) If the desired policy is not available in the list, then you may create the customized centralized policy following the steps below:

   a. Click **Add Policy**.

   b. In the Add Policy page, continue to click **Next** till you navigate to **Configure Traffic Rules** page.
4. Click **Traffic Rules**, then click **Traffic Data**.
5. Click **Add Policy** drop-down.
6. Click **Create New**. The **Add Data Policy** window displays.
7. Enter a **Name** and the **Description**.
8. Click **Sequence Type**. The Add Data Policy popup opens.
9. Select **QoS** type of data policy.
10. Click **Sequence Rule**. The Match/Action page opens, with Match selected by default.
11. From the **Match** box, select the desired policy match type. Then select or enter the value for that match condition. Configure additional match conditions for the sequence rule, as desired.
12. To select actions to take on matching data traffic, click **Actions** box.

13. By default, **Accept** is enabled. Select **Forwarding Class** from actions.
14. In the **Forwarding Class** field, and enter the class value (maximum of 32 characters).
15. Click **Save Match and Actions**.
16. Click **Save Data Policy**.
17. If your are creating a new centralized policy, then click **Next** and navigate to Add policies to Sites and VPNs page.
    a. Enter a **Policy Name** and **Description** for your centralized policy.
    b. Click **Save Data Policy**.

Apply Centralized Policy

1. Click **Policy Application** to apply the centralized policy.
2. Click **Traffic Data**.
3. Click **New Site List and VPN list**.
4. Choose the direction for applying the policy (**From Service**, **From Tunnel**, or **All**), choose one or more site lists, and choose one or more VPN lists.
5. Click **Add**.
6. Click **Save Policy Changes**.
7. A window pops up indicating the policy will be applied to the Cisco SD-WAN Controller.
8. Click **Activate**.
9. Cisco SD-WAN Manager pushes the configuration to the Cisco SD-WAN Controller and indicates success.

Forwarding and QoS Configuration Using the CLI

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).

This example shows how to configure class of service (CoS) to classify data packets and control how traffic flows out of and into the interfaces on Cisco IOS XE Catalyst SD-WAN devices 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. Define an access list to specify match conditions for packet transmission and apply it to a specific interface.
4. Apply the queue map and the rewrite rule to the egress interface.

The sections below show examples of each of these steps.

Map Each Forwarding Class to Output Queue

This example shows a data policy that classifies incoming traffic by mapping each forwarding class to an output queue.

```
policy
class-map
  class Queue0 queue 0
  class ef queue 0
  class Queue1 queue 1
  class Queue2 queue 2
  class be queue 2
  class Queue3 queue 3
  class af1 queue 3
  class Queue4 queue 4
  class af2 queue 4
  class Queue5 queue 5
  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.

```
class-map match-any Queue0
match qos-group 0
!
class-map match-any Queue1
match qos-group 1
!
class-map match-any Queue2
match qos-group 2
!
class-map match-any Queue3
match qos-group 3
!
class-map match-any Queue4
match qos-group 4
!
class-map match-any Queue5
match qos-group 5
!

policy-map test
class Queue0
  priority percent 20
!
class Queue1
  random-detect
  bandwidth percent 20
!
class class-default
  bandwidth percent 20
!
class Queue3
  bandwidth percent 15
!
class Queue4
  random-detect
  bandwidth percent 15
!
```

```
class Queue5
  bandwidth percent 10
!
!
```

Apply a QoS Map to an Ethernet Interface

This example demonstrates how to implement hierarchical traffic shaping on an interface to limit bandwidth while applying further QoS policies within the shaped traffic.

```
policy-map shape_GigabitEthernet0/0/2
 class class-default
  shape average 100000000
  service-policy test
!
interface GigabitEthernet0/0/2
  service-policy output shape_GigabitEthernet0/0/2
!
```

Run the **show running-config interface GigabitEthernet2** command to verify the QoS configuration on a WAN edge device.

```
Device# show running-config interface GigabitEthernet2

interface GigabitEthernet0/0/2
 description INET Transports
 service-policy output shape_GigabitEthernet0/0/2
!
```

Create Access Lists to Classify Data Packets

Define Access Lists

Define an access list to specify match conditions for packet transmission.

```
policy
access-list acl1
  sequence 1
   match
    dscp 46 48
   !
   action accept
    class ef
   !
  !
  sequence 11
   match
    dscp 34
   !
   action accept
    class af3
   !
  !
  sequence 21
   match
    dscp 24
   !
   action accept
    class af2
```

```
   !
  !
  sequence 31
   match
    dscp 18
   !
   action accept
    class af1
   !
  !
  sequence 41
   match
    dscp 0 10
   !
   action accept
    class be
    log
   !
  !
  default-action accept
!
```

Apply Access Lists

Apply Access List to a Specific Interface

This example illustrates how to apply the previously access list defined on the input of a service interface. Here "access-list acl1" is applied on the input of interface Gi0/0/1.

```
sdwan
interface GigabitEthernet0/0/1
  access-list acl1 in
!
 !
!
```

Configure and Apply Rewrite Rule

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.

Apply the Queue Map and Rewrite Rule to the Egress Interface

This example applies the queue map "test" and the rewrite rule "transport" to the egress interface. (Note that you can apply QOS maps to VLAN interfaces, also called subinterfaces, on Cisco IOS XE Catalyst SD-WAN devices (not on Cisco vEdge devices), using Cisco IOS XE SD-WAN Release 16.12.x or later, or Cisco SD-WAN Release 19.1.x or later.)

```
policy
rewrite-rule transport
```

```
  class af1 low layer-2-cos 1
  class af2 low dscp 16 layer-2-cos 2
  class af3 low dscp 24 layer-2-cos 3
  class be low dscp 0
  class ef low dscp 46 layer-2-cos 5
!
sdwan
interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color public-internet restrict
  exit
  rewrite-rule transport
exit
```

Apply a Rewrite Rule for Outgoing Traffic in a Carrier Supporting Carrier Scenario

In carrier supporting carrier (CSC) scenarios, which use MPLS, the **rewrite-rule** command assigns the MPLS EXP value in the MPLS header for outgoing traffic. Use the **rewrite-rule** command using a CLI template or CLI add-on template, and the **mpls-exp-topmost** keyword. If, in a CSC scenario, you use the **dscp** keyword instead, such as with legacy configurations created before support of the **mpls-exp-topmost** keyword, the **rewrite-rule** command converts the DSCP value to an MPLS EXP value in accordance with the standard mapping of DSCP to MPLS EXP values. The benefit of using the **mpls-exp-topmost** keyword is that you can set the MPLS EXP value directly, without depending on the mapping of DSCP to MPLS EXP values.

The following example applies to a CSC scenario. It defines a rewrite rule called rw-exp, which sets the MPLS EXP value for outgoing traffic to 1 and applies the rule to the outbound interface.

Define the rewrite rule using the **mpls-exp-topmost** keyword, as follows:

```
sdwan
  policy
    rewrite-rule rw-exp
      class BULK low mpls-exp-topmost 1
      class BULK high mpls-exp-topmost 1
```

Alternatively, if you define the rewrite rule using the **dscp** keyword, the **rewrite-rule** command converts the value of 10 to an MPLS EXP value of 1, in accordance with the standard mapping of DSCP to MPLS EXP values.

```
sdwan
  policy
    rewrite-rule rw-exp
      class BULK low dscp 10
      class BULK high dscp 10
```

Apply the rule as follows:

```
sdwan
interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color public-internet restrict
  exit
  rewrite-rule rw-exp
exit
```

Verify Configuration of QoS Policy Map Using the CLI

```
Device# show policy-map interface GigabitEthernet0/0/2
 GigabitEthernet0/0/2

  Service-policy output: shape_GigabitEthernet0/0/2

    Class-map: class-default (match-any)
      33823 packets, 6855717 bytes
      5 minute offered rate 31000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 33823/6855717
      shape (average) cir 100000000, bc 400000, be 400000
      target shape rate 100000000

      Service-policy : test

        queue stats for all priority classes:
          Queueing
          queue limit 512 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 33802/6853827

        Class-map: Queue0 (match-any)
          33802 packets, 6853827 bytes
          5 minute offered rate 31000 bps, drop rate 0000 bps
          Match: qos-group 0
          Priority: 20% (20000 kbps), burst bytes 500000, b/w exceed drops: 0


        Class-map: Queue1 (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: qos-group 1
          Queueing
          queue limit 83 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
         (pkts output/bytes output) 0/0
          bandwidth 20% (20000 kbps)
            Exp-weight-constant: 9 (1/512)
            Mean queue depth: 0 packets
            class       Transmitted         Random drop      Tail drop          Minimum
     Maximum     Mark
                    pkts/bytes            pkts/bytes       pkts/bytes          thresh
    thresh     prob

            0               0/0               0/0              0/0                20
       41  1/10
            1               0/0               0/0              0/0                22
       41  1/10
            2               0/0               0/0              0/0                25
       41  1/10
            3               0/0               0/0              0/0                27
       41  1/10
            4               0/0               0/0              0/0                30
       41  1/10
            5               0/0               0/0              0/0                32
       41  1/10
            6               0/0               0/0              0/0                35
```

```
   41  1/10
        7               0/0               0/0               0/0                 37
   41  1/10

    Class-map: Queue3 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 3
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 15% (15000 kbps)

    Class-map: Queue4 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 4
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 15% (15000 kbps)
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0 packets
        class       Transmitted         Random drop      Tail drop          Minimum
 Maximum     Mark
                pkts/bytes            pkts/bytes       pkts/bytes          thresh
thresh     prob

        0               0/0               0/0               0/0                 16
   32  1/10
        1               0/0               0/0               0/0                 18
   32  1/10
        2               0/0               0/0               0/0                 20
   32  1/10
        3               0/0               0/0               0/0                 22
   32  1/10
        4               0/0               0/0               0/0                 24
   32  1/10
        5               0/0               0/0               0/0                 26
   32  1/10
        6               0/0               0/0               0/0                 28
   32  1/10
        7               0/0               0/0               0/0                 30
   32  1/10

    Class-map: Queue5 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 5
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth 10% (10000 kbps)

    Class-map: class-default (match-any)
      21 packets, 1890 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 83 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
```

```
 (pkts output/bytes output) 21/1890
bandwidth 20% (20000 kbps)
```

Reference: Forwarding and QoS CLI Commands

Monitoring Commands

Use the following commands to monitor forwarding and QoS on a Cisco IOS XE Catalyst SD-WAN device:

```
show sdwan policy access-list-associations
show sdwan policy access-list-counters
show sdwan policy access-list-names
show sdwan policy access-list-policers
show sdwan policy data-policy-filter
show sdwan policy rewrite-associations
show policy-map interface GigabitEthernet0/0/2
```