Cisco Catalyst SD-WAN Forwarding and QoS Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x

First Published: 2020-04-30

Last Modified: 2023-12-18

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

CHAPTER 2

What's New in Cisco IOS XE (SD-WAN)

CHAPTER 3

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

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.

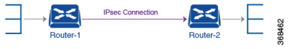
While the routing protocols running in the control plane provide a router the best route to reach the network that is on the service side of a remote router, there will be situations where it is beneficial to select more specific routes. Using forwarding, there are ways you can affect the flow of data 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).

Traffic Behavior With and Without QoS

Default Behavior without Data Policy

When no centralized data policy is configured on the Cisco SD-WAN Controller, all data traffic is transmitted from the local service-side network to the local router, and then to the remote router and the remote service-side network, with no alterations in its path. When no access lists are configured on the local router to implement QoS or mirroring, the data traffic is transmitted to its destination with no alterations to its flow properties.

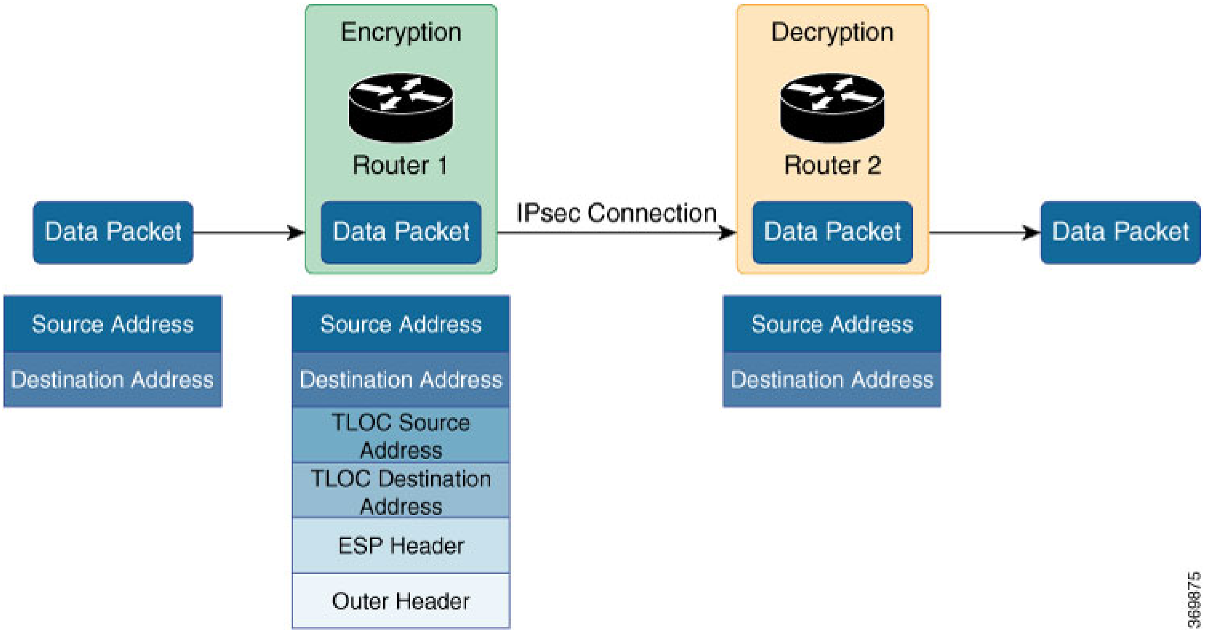


Let's follow the process that occurs when a data packet is transmitted from one site to another when no data policy of any type is configured:

- A data packet arriving from the local service-side network and destined for the remote service-side network comes to the router-1. The packet has a source IP address and a destination IP address.
- The router looks up the outbound SA in its VPN route table, and the packet is encrypted with SA and gets the local TLOC. (The router previously received its SA from the Cisco SD-WAN Controller. There is one SA per TLOC. More specifically, each TLOC has two SAs, an outbound SA for encryption and an inbound SA for decryption.)
- ESP adds an IPsec tunnel header to the packet.
- An outer header is added to the packet. At this point, the packet header has these contents: TLOC source address, TLOC destination address, ESP header, destination IP address, and source IP address.
- The router checks the local route table to determine which interface the packet should use to reach its destination.
- The data packet is sent out on the specified interface, onto the network, to its destination. At this point, the packet is being transported within an IPsec connection.
- When the packet is received by the router on the remote service-side network, the TLOC source address and TLOC destination address header fields are removed, and the inbound SA is used to decrypt the packet.
- The remote router looks up the destination IP address in its VPN route table to determine the interface to use to reach to the service-side destination.

The figure below details this process.

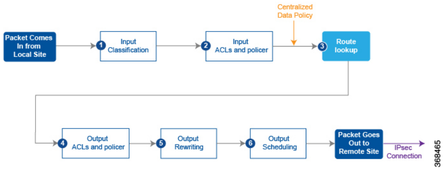
Figure 1: Data Packet Transmission without Policy



Behavior Changes with QoS Data Policy

When you want to modify the default packet forwarding flow, you design and provision QoS policy. To activate the policy, you apply it to specific interfaces in the overlay network in either the inbound or the outbound direction. The direction is with respect to the routers in the network. You can have policies for packets coming in on an interface or for packets going out of an interface.

The figure below illustrates the QoS policies that you can apply to a data packet as it is transmitted from one branch to another. The policies marked Input are applied on the inbound interface of the router, and the policies marked Output are applied on the outbound interface of the router, before the packets are transmitted out the IPSec tunnel.



The table below describes each of the above steps.

Step	Description	Command
1	Define class map to classify packets, by importance, into appropriate forwarding classes. Reference the class map in an access list.	**class-map**
2	Define policer to specify the rate at which traffic is sent on the interface. Reference the policer in an access list. Apply the access list on an inbound interface.	**policer**
3	The router checks the local route table to determine which interface the packet should use to reach its destination.	N/A

Step	Description	Command
4	Define policer and reference the policer in an access list. Apply the access list on an outbound interface.	**policer**
5	Define QoS map to define the priority of data packets. Apply the QoS map on the outbound interface.	**policy-map**
6	Define rewrite-rule to overwrite the DSCP field of the outer IP header. Apply the rewrite-rule on the outbound interface.	**rewrite-rule**

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

You can configure shaping to control the maximum rate of traffic sent. You can configure the aggregate traffic rate on an interface to be less than the line rate so that the interface transmits less traffic than it is capable of transmitting. You can apply shaping to outbound interface traffic.

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 31,250,000 bytes of burst value.

If you set the burst value to 15,000 bytes, the system automatically adjusts to the higher burst tolerance of 31,250,000 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.

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
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)
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
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
!
!
```

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
```

CHAPTER 4

Per-Tunnel QoS

Table 4: Feature History

Feature Name	Release Information	Description
Per-Tunnel QoS	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature lets you apply a Quality of Service (QoS) policy on individual tunnels, ensuring that branch offices with smaller throughput are not overwhelmed by larger aggregation sites. This feature is only supported for hub-to-spoke network topologies.
Increase Per Tunnel QoS Session Scale	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Cisco Catalyst SD-WAN Manager can manage 10,000 sessions of per-tunnel QoS.

Information about Per-Tunnel QoS

Overview of Per-Tunnel QoS

Use the Per-tunnel QoS feature to apply a quality of service (QoS) policy on a Cisco IOS XE Catalyst SD-WAN device hub on a per-tunnel or per-spoke instance in the egress direction.

Per-tunnel QoS can only be applied on hub-to-spoke network topologies. Per-tunnel QoS on a hub lets you shape tunnel traffic to individual spokes. It also differentiates individual data flows going through the tunnel or the spoke for policing.

Benefits of Per-Tunnel QoS

Before the introduction of Per-tunnel QoS feature on Cisco Catalyst SD-WAN, QoS on a hub could be configured to measure only the aggregate outbound traffic for all spokes. Per-tunnel QoS for Cisco Catalyst SD-WAN provides the following benefits.

- A QoS policy is configurable on the basis of session groups, thus providing the capability of regulating traffic from hub to spokes at a per-spoke level.
- The hub cannot send excessive traffic to a small spoke and overrun it.
- The maximum outbound bandwidth and QoS queue are set up automatically when each spoke registers with an Overlay Management Protocol (OMP) message.
- The amount of outbound hub bandwidth that a "greedy" spoke can consume can be limited; therefore, the traffic can't monopolize a hub's resources and starve other spokes.
- Multiple policies (MPoL) are supported. This enables underlay and TLOC extension traffic to coexist with the overlay tunnel traffic.

Supported Platforms

Per-Tunnel QoS for Hub

The following series of platforms can be configured as hubs for the per-tunnel QoS in Cisco Catalyst SD-WAN.

- Cisco 1000 Series Aggregation Services Routers
- Cisco 1000 Series Integrated Services Routers
- Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Cloud Services Router 1000V Series
- Cisco Catalyst 8000 Edge Platforms Family

Per-Tunnel QoS for Spokes

The following series of Cisco IOS XE Catalyst SD-WAN devices can be configured as spokes for per-tunnel QoS in Cisco Catalyst SD-WAN.

- Cisco 1000 Series Aggregation Services Routers
- Cisco 1000 Series Integrated Services Routers
- Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Cloud Services Router 1000V Series
- Cisco Catalyst 8000 Edge Platforms Family
- Cisco 1000 Series Integrated Services Routers (ISRs)

- ISR1100-4G
- ISR1100-6G
- ISR1100-4GLTENA and ISR1100-4GLTEGB

Restrictions for Per-Tunnel QoS

- Only hub-to-spoke network topology is supported for configuring per-tunnel QoS. Spoke-to-spoke network topology isn't supported.
- Only Cisco IOS XE Catalyst SD-WAN devices are supported as hubs for per-tunnel QoS. However, both Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices are supported as spokes in the hub-to-spoke topology supported for per-tunnel QoS.
- In Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, per-tunnel QoS can only be configured using the Cisco VPN Interface Ethernet template in Cisco vManage 20.1.1.
- Per-tunnel QoS with loopback WAN for non-binding mode isn’t supported on the hub.
- For per-tunnel QoS to work with 3-level hierarchical policies, you must use the reserved class-map name, "SDWAN_underlay" for middle level policy.
- Maximum number of sessions:
  - (Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.11.1a)

    You can configure a maximum number of sessions to which the QoS policy is applied. When the number of Cisco Catalyst SD-WAN user sessions with QoS policy reaches its limit, the QoS policy is not applied for any other sessions. The number of sessions that you can configure is from 100 to 6,000. The default QoS maximum session for all platforms is 4,000.
  - (Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a)

    The number of sessions that you can configure is from 100 to 10,000.

How Per-Tunnel QoS Works in Hub-to-Spoke Topologies

In Cisco IOS XE Release 17.2 , the Per-Tunnel QoS feature is supported on hub-to-spoke network topologies only. Per-tunnel QoS is not supported for spoke-to-spoke topology.

- Per-tunnel QoS is applied to routers with the hub role on a per-session basis.
- Routers that are assigned the spoke role publish the downstream-bandwidth information per TLOC route through OMP.
- Overlay and underlay tunnels share the same QoS policy and the bandwidth remaining is configurable for both underlay and overlay tunnels.
- The bandwidth remaining ratio is automatically calculated on each session based on the remote downstream bandwidth.

Configure Per Tunnel QoS Using Cisco SD-WAN Manager

To configure per-tunnel QoS, perform the following tasks in the order specified.

Step 1: Configure QoS Map

A QoS map can be added to a localized data policy. For more details on the various QoS parameters, see QoS parameters section in the Policies Guide. To configure QoS map:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy** and then click **Add Policy**.
3. From the list type shown in the left pane, choose **Class Map**. The list displays existing class maps. Choose a class map from the list and click **Next**.

   OR

   Create a new class map:

   a. Click **Add New Class Map**.

   b. Enter a name for the class map.

   c. From the **Queue** drop-down list, choose a number (from 0-7).

   d. Click **Save** and then click **Next**.

4. Click the **Add QoS Map** and choose **Create New**.
5. Enter a name and description for the map.
6. Click **Add Queue**, enter the requested details, and click **Save Queue**.
7. Click **Save Policy**.

Step 2: Choose the QoS Map to be Added to the Feature Template

Per-tunnel QoS can only be configured through the Cisco VPN Interface Ethernet template. To enable per-tunnel QoS on other WAN interface types, use the global CLI add-on template.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

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

3. Choose a device from the list on the left. Feature templates applicable to the device are shown in the right pane.
4. Choose the **Cisco VPN Interface Ethernet** template.
5. Enter a name and description for the feature template.
6. Choose the **ACL/QoS** option.

7. Enter the requested details.
   - **Shaping Rate:** Choose Global from the drop-down list and enter a shaping rate in kbps.
   - **QoS Map:** Choose Global from the drop-down list and enter the name of the QoS map that you want to include in the feature template.

8. Click **Save**.

Step 3: Attach the Localized QoS Policy and the Feature Template to the Device Template

1. Attach the localized policy created in Step 1 to the device template.
2. Attach the feature template created in Step 2 to the device template. See Create Device Templates from Feature Templates for more details.

Note Ensure that you attach the localized policy and the feature template to the same device template.

Step 4 Configure Hub Role for Per-Tunnel QoS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**. All the features templates are listed.

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

3. For the Cisco VPN Interface template that you want to add per-tunnel QoS policy to, click **...** and choose **Edit**.

   Alternatively, you can create a new **Cisco VPN Interface Ethernet** template following the instructions in the previous sections and then proceed with the steps below.

4. When the template opens, click the **Tunnel** option at the top of the page.
5. From the **Tunnel Interface** drop-down list, choose **Global** and choose **On**.

   A new set of fields display below the **Tunnel Interface** option. These new fields are specific to per-tunnel QoS and display only when you choose the **On** option.

6. From the **Per-tunnel Qos** drop-down list, choose **Global** and then choose **On**.

   The **Per-tunnel QoS Aggregator** field appears after you set **Per-tunnel Qos** to **On**. If this field is set to **Off**, which is the default behavior, it means that the device selected in the template is assigned the spoke role. If the field is set to **On**, it means that the device is assigned the hub role.

7. Choose **Global** from the **Per-tunnel QoS Aggregator** drop-down menu, and choose **On**. The device has now been assigned the role of a hub.

   When you choose the On option, the **Tunnel Bandwidth Percent** field displays.

8. You can either leave the Tunnel Bandwidth Percent value at default (50) or choose **Global** from the drop-down menu to enter a value based on your network requirement.

The remaining fields under the Tunnel section are not specific to per-tunnel QoS. You can either leave the values at default or enter values specific to your network.

9. Click **Update**. The feature template updates with per-tunnel QoS configuration.

Step 5: Configure Spoke Role for Per-Tunnel QoS

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**. All the features templates are listed.

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

3. For the Cisco VPN Interface Template that you want to add the per-tunnel QoS policy to, click **...** and choose **Edit**.

   OR

   Create a new **Cisco VPN Interface Ethernet** template following the instructions in the previous sections and then proceed with the steps below.

4. When the template opens, click **Tunnel**.
5. From the **Tunnel Interface** drop-down list, choose **Global** and choose the **On** option.

   A new set of fields display below the Tunnel Interface option. These new fields are specific to per-tunnel QoS and display only when you choose the **On** option.

6. From the **Per-tunnel Qos** drop-down menu, choose **Global** and choose the **On** option.

   The **Per-tunnel QoS Aggregator** field displays after you set **Per-tunnel Qos** to **On**. This field is set to off by default. If this field is set to **Off**, it means that the device selected in the template is assigned the spoke role.

7. The downstream bandwidth needs to be configured for the device to effectively take the spoke role. To configure the downstream bandwidth, click **Basic Configuration** at the top of the page.
8. Scroll down to the **Bandwidth Downstream** Field and choose **Global** from the drop-down menu.
9. Enter a value for the downstream bandwidth and click **Update** at the bottom of the page.

Configure Per Tunnel QoS Using a CLI Template

This topic shows the task flow for configuring per-tunnel QoS using CLI templates with the help of examples.

Example: Create QoS MaP

```
class-map match-any SDWAN_underlay
 match any
!
class-map match-all Queue0
 match qos-group 0
!
class-map match-all Queue1
```

```
 match qos-group 1
!
class-map match-all Queue3
 match qos-group 3
 !
policy-map qos_policy_4class_cedge
class Queue0
  priority level 1
  police rate percent 25
class Queue1
  bandwidth remaining ratio 20
class Queue3
  bandwidth remaining ratio 15
class class-default
 bandwidth remaining ratio 40
!
```

Example: Apply a QoS Map to an Ethernet Interface

```
policy-map per_tunnel_qos_policy_GigabitEthernet0/0/1
 class SDWAN_underlay
  bandwidth remaining percent 50
  service-policy qos_policy_4class_cedge
!
policy-map shape_GigabitEthernet0/0/1
 class class-default
  shape average 10000000
  service-policy qos_policy_4class_cedge_GigabitEthernet0/0/1
!
interface GigabitEthernet0/0/1
  service-policy output shape_ GigabitEthernet0/0/1
!
```

Example: Configure a Device as a Hub

```
sdwan
 interface GigabitEthernet0/0/1
  tunnel-interface
   encapsulation ipsec
   color public-internet restrict
   tunnel-qos hub
  exit
```

Example: Configure a Device as a Spoke

```
sdwan
 interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec
   color public-internet restrict
   tunnel-qos spoke
  exit
  bandwidth-downstream 50000
 exit
```

Example: Configure Number of Sessions

```
platform qos sdwan max-session 5000
sdwan
interface GigabitEthernet0/0/2
tunnel-interface
 encapsulation ipsec
 color public-internet restrict
 tunnel-qos spoke
exit
bandwidth-downstream 50000
top
interface Tunnel0
ip unnumbered GigabitEthernet0/0/2
tunnel source GigabitEthernet0/0/2
tunnel mode sdwan
```

Verify Per-Tunnel QoS Configuration

Run the **show sdwan running-config** command to verify the per-tunnel QoS configuration on a Cisco IOS XE Catalyst SD-WAN device configured as a hub.

```
Device# show sdwan running-config
class-map match-any Queue0
 match qos-group 0
!
class-map match-any Queue1
 match qos-group 1
!
class-map match-any Queue3
 match qos-group 3
!
class-map match-any SDWAN_underlay
 match any
!
policy-map per_tunnel_qos_policy_GigabitEthernet0/0/1
 class SDWAN_underlay
  bandwidth remaining percent 50
  service-policy qos_policy_4class_cedge
 !
!
policy-map qos_policy_4class_cedge
 class Queue0
  priority level 1
  police rate percent 25
   !
 !
 class Queue1
  bandwidth remaining ratio 20
!
 class class-default
  bandwidth remaining ratio 40
!
 class Queue3
  bandwidth remaining ratio 15
 !
!
policy-map shape_GigabitEthernet0/0/1
 class class-default
  service-policy per_tunnel_qos_policy_GigabitEthernet0/0/1
  shape average 100000000
 !
!
interface GigabitEthernet0/0/1
 description INET Transports
 service-policy output shape_GigabitEthernet0/0/1
!
sdwan
 interface GigabitEthernet0/0/1
```

```
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color public-internet restrict
   tunnel-qos hub
  exit
 exit
!
```

Run the **show sdwan running-config sdwan** command to verify the per-tunnel QoS configuration on a Cisco IOS XE Catalyst SD-WAN device configured as a spoke.

```
Device# show sdwan running-config sdwan
sdwan
 interface GigabitEthernet0/0/1
  tunnel-interface
   encapsulation ipsec weight 1
   color public-internet restrict
   tunnel-qos spoke
  exit
  bandwidth-downstream 50000
exit
```

Run the **show running-config** command to verify the per-tunnel QoS configuration on a Cisco vEdge device configured as a spoke.

```
Device# show running-config
vpn 0
interface ge0/0
  tunnel-interface
   tunnel-qos spoke
!
bandwidth-downstream 50000
!
```

Monitor Per-Tunnel QoS

Use the following monitoring commands to monitor the performance of per-tunnel QoS.

- **show platform software sdwan qos template** : Displays the child templates used for per-tunnel QoS.
- **show platform software sdwan qos policy** : Displays per-tunnel QoS policy instance parameters like policy template, bandwidth, and bandwidth remaining-ratio.
- **show platform software sdwan qos target** : Displays per-tunnel QoS policy target database per sd-wan session and tunnel interface.
- **show policy-map interface GigabitEthernet** *0/0/1*: Displays the statistics status and the configured policy maps on the specified interface.
- **show policy-map multipoint Tunnel** *10 10.10.10.20*: Displays the per-tunnel QoS statistics on the tunnel ID specified.
- **show platform software sdwan qos summary** : Confirms the count of sessions, policies, WAN interfaces, and adaptive QoS sessions.

CHAPTER 5

QoS on Subinterface

Table 5: Feature History

Feature Name	Release Information	
QoS on Subinterface	This feature enables Quality of Service (QoS) policies to be applied to individual subinterfaces.	

A physical interface may be treated as multiple interfaces by configuring one or more logical interfaces called subinterfaces. One use case is separating the traffic of different VLANs by using a separate subinterface for each VLAN.

Quality of Service (QoS) policies may be applied to individual subinterfaces. Configure QoS as usual, specifying the interface and subinterface using the *interface*:*subinterface* notation. For example, for GigabitEthernet interface 4, subinterface 100: GigabitEthernet4.100

Limitations

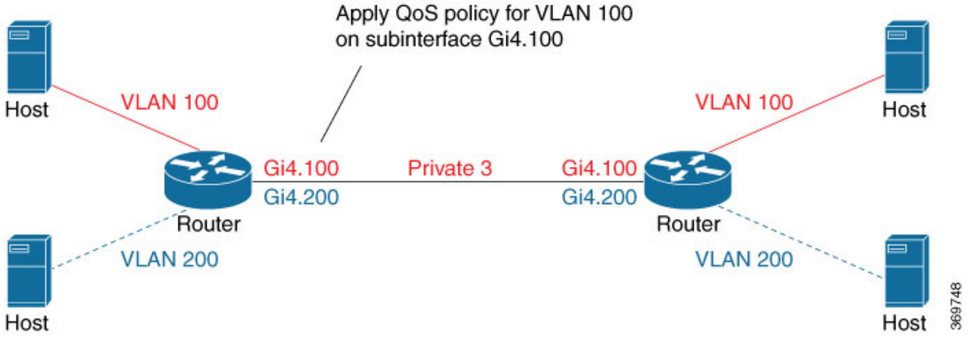
- Do not configure a QoS policy on both a main interface and one of its subinterfaces. The exception is a class-default shape policy on the main interface.

- A QoS policy that is applied to a subinterface must have shaping defined. This configured with the shape command. Example:

```
policy-map shape_GigabitEthernet4.100
    class class-default
        service-policy xyz_QoS-model
        shape average 100000000
```

Configuration Example: QoS on Subinterface

This example applies a QoS policy to subinterface GigabitEthernet4.100 (shown in red in the figure below). This subinterface handles traffic for VLAN 100. The QoS policy affects only subinterface GigabitEthernet4.100, and not subinterface GigabitEthernet4.200, which is on the same physical interface.



Configure QoS on Subinterface Using Cisco SD-WAN Manager

To apply a QoS policy to a subinterface using Cisco SD-WAN Manager, the procedure is similar to that used for configuring policies on a main interface. Add a subinterface feature template to the device template for the target device. This enables loading the QoS policy onto the subinterface.

Before you Begin

- Configure a QoS Policy from **Configuration** > **Policies** > **Localized Policy** > **Custom Options** > **Forwarding Class/QoS**.
- Apply a QoS Policy to a subinterface and define shaping.

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

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

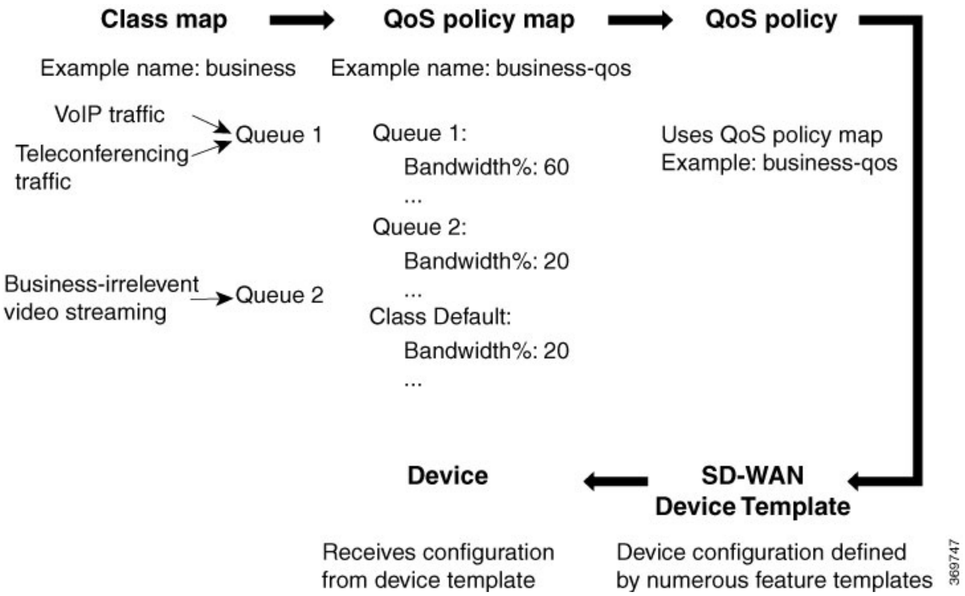
  3. Choose an applicable feature template, such as Cisco VPN Interface Ethernet, and go to the **ACL/QoS** area of the template.
  4. Configure the following fields:
     - Shaping Rate (Kbps)
     - QoS Map

Procedure

This procedure applies a QoS policy to a subinterface.

Prerequisite: One or more class maps have been defined. These assign classes of traffic (for example, VoIP traffic) to specific queues.

Figure 2: Overview of Workflow for Applying a QoS Policy



1. Create a QoS policy map.
   a. From Cisco SD-WAN Manager, choose **Configuration** > **Policies**.
   b. Click **Localized Policy**.
   c. Click **Add Policy** to create a new policy map.
   d. Click **Next**.
   e. Click **Add QoS Map** and choose **Create New** from the drop-down menu.
   f. (This step relies on class maps that have been defined. The class maps assign classes of traffic to specific queues. The queues then represent those classes of traffic. This step uses the queues to control how the traffic will be handled.)

      In the **Add Queue** dialog box, choose queues that represent the types of traffic relevant to the QoS objectives. Configure parameters such as Bandwidth% and Buffer% for the queues. For example, to configure bandwidth for audio traffic, choose a queue that represents audio traffic and configure the bandwidth parameter. Click **Save Queue**.
   g. Click **Save Policy**.

2. Create a QoS policy that uses the QoS policy map defined above.

   See the documentation for creating a QoS policy.

3. Use a device template to push the QoS policy to the target device.

Note The device policy defines other parts of the device configuration also. This procedure only affects the QoS policy portion.

a. From Cisco SD-WAN Manager, choose **Configuration** > **Templates**.

b. From the list of templates, locate the device template for the target device.

c. For the desired template row, click **...** and choose Edit.

d. In the **Additional Templates** area, in the **Policy** field, click the drop-down menu and choose the policy name.

e. Click **Update**.

f. Click **Next**.

g. In the left pane, choose the target device. The configuration appears in the right pane.

h. Click **Configure Devices** to push the policy to the device. Cisco SD-WAN Manager displays the Task View, showing the status of the update tasks.

4. Load the QoS policy onto the subinterface.

   Prerequisite: The subinterface feature template must already have been added to the device template.

a. From Cisco SD-WAN Manager, choose **Configuration** > **Templates**.

b. Click **Feature Templates**.

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

c. In the list of templates, locate the feature template for the subinterface. This is the subinterface to which you are assigning the QoS policy.

d. In the **Device Templates** column, confirm that the feature template is assigned to a device template.

e. In the **Devices Attached** column, confirm that the feature template is assigned to a device.

f. For the desired template row, click **...** and choose Edit.

g. Click **ACL/QoS** to jump to the ACL/QoS section.

h. In the Shaping Rate field, use the drop-down menu to choose **Global** or **Device Specific**, and enter a shaping rate value.

i. In the **QoS Map** field, use the drop-down menu to choose **Global** and enter the QoS policy map name.

j. Click **Update**.

k. In the left pane, choose the device to view the configuration in the right pane.

l. Click **Configure Devices** to push the policy map to the subinterface. Cisco SD-WAN Manager displays the Task View, showing the status of the update tasks.

Configure QoS on a Subinterface Using the CLI

```
class-map match-any DATA
     match qos-group 1
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 Queue7
     match qos-group 7
class-map match-any WEB
     match qos-group 7

policy-map xyz_QoS-model
     class Queue0
          priority percent 37
     class Queue1
          bandwidth percent 33
      class Queue7
            random-detect
           bandwidth percent 10
      class class-default
            random-detect
           bandwidth percent 20
policy-map shape_GigabitEthernet4.100
     class class-default
           service-policy xyz_QoS-model
           shape average 100000000
 !

interface GigabitEthernet4.100
 no shutdown
 encapsulation dot1Q 100
 ip address 173.10.0.2 255.255.255.0
 ip mtu 1496
 service-policy output shape_GigabitEthernet4.100
exit

exit
interface Tunnel3
 no shutdown
 ip unnumbered GigabitEthernet4.100
 tunnel source GigabitEthernet4.100
 tunnel mode sdwan
exit

sdwan
 interface GigabitEthernet4.100
  tunnel-interface
   encapsulation ipsec
   color private3 restrict
   max-control-connections 0

policy
 class-map
  class Queue0 queue 0
  class VOICE queue 0
  class DATA queue 1
  class Queue1 queue 1
  class Queue2 queue 2
  class Queue7 queue 7
  class WEB queue 7
 !
```

CHAPTER 6

Adaptive QoS

Table 6: Feature History

Feature Name	Release Information	Description
Adaptive QoS	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables WAN interface shapers and per-tunnel shapers at the enterprise edge to adapt to the available WAN bandwidth. The capability to adapt to the bandwidth controls differentiated packet drops at the enterprise edge and reduces or prevents packet drops in the network core.

Limitations and Restrictions

- Adaptive QoS is only supported on Cisco IOS XE Catalyst SD-WAN devices. Only Cisco IOS XE Catalyst SD-WAN devices can be configured as hub devices. This means that for adaptive QoS to work, the spokes should also be Cisco IOS XE Catalyst SD-WAN devices.

- Adaptive QoS is only supported on to hub-to-spoke network topology.

- Adaptive QoS support on DIA/DCA interfaces is dependent upon the throughput of the overlay session.

- If an edge device is configured as hub, the WAN interface on the edge device cannot be configured with adaptive QoS.

- Adaptive QoS is supported for loopback interfaces only when a single loopback interface is bound to a single physical interface.

Information About Adaptive QoS

Overview of Adaptive QoS

Enterprise networks are increasingly using the Internet as a form of WAN transport. Therefore, QoS models need to adapt accordingly. QoS works effectively when deployed in a service-level agreement (SLA) environment, like Multiprotocol Label Switching (MPLS) networks. The available bandwidth on the Internet at a given time can vary. It can often be much lesser than the actual bandwidth that is offered by the service provider. In a non-SLA environment, QoS has limitations because it can't predict the changing bandwidth on the link.

With adaptive QoS, the shapers at the edge of the enterprise (WAN interface shaper and per-tunnel shaper) can adapt to the available WAN bandwidth, both Internet and Long-term Evolution (LTE). Thus, adaptive QoS can control differentiated drops at the enterprise edge and reduce the packet drops in the Internet core. When the adaptive QoS capability is not available, shapers that are applied as part of the egress QoS policy are static in value. They are configured based on the service provider bandwidth offering and don't change with time, thus they don’t reflect the actual available Internet bandwidth.

Benefits of Adaptive QoS

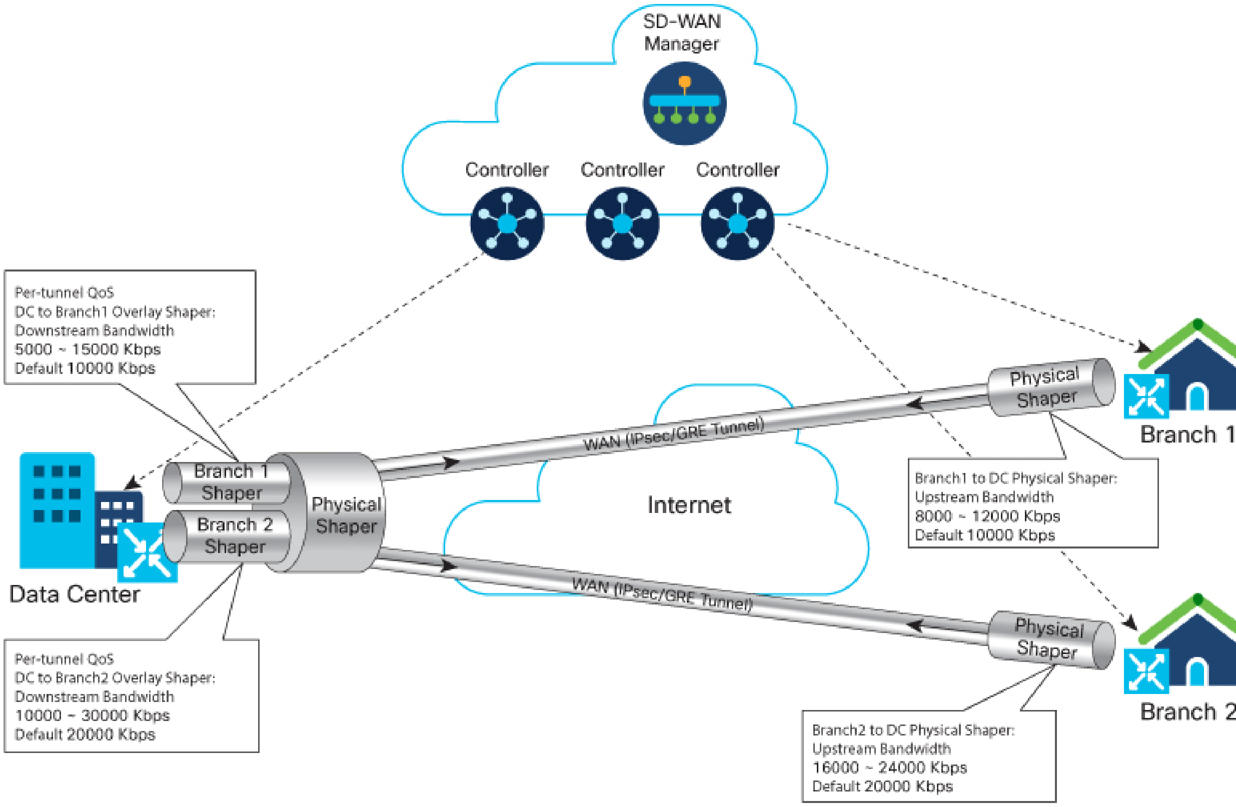
- Adjusts the shaper parameters based on the actual available Internet bandwidth in both directions, which is periodically computed
- Allows configuring a QoS policy on the spoke towards the hub
- Ensures better control of application performance at the enterprise edge even when the bandwidth fluctuates
- Allows aggregate tunnel shape adaptation to provide effective bandwidth between spoke and hub

How Adaptive QoS Works in Cisco Catalyst SD-WAN

LTE and Internet bandwidth changes dynamically based on weather conditions and external parameters. In addition, Internet bandwidth can also fluctuate with the network conditions of the service provider, their congestion, and configurations.

Application traffic is prone to packet drops at the Internet core when the bandwidth is less, and the traffic can't be differentiated by user-defined priority. In such scenarios, Cisco Catalyst SD-WAN adaptive QoS automatically updates the shaper rate in real time based on the Internet and LTE link bandwidth.

Adaptive QoS can be enabled through Cisco SD-WAN Manager on a specific interface of an edge device that is configured with the spoke role in a hub-to-spoke network topology. You can specify minimum, maximum, and default values. You can also configure a timer interval at a global level on a WAN interface to measure the drop rates.



In the image, adaptive per-tunnel QoS is configured on the WAN interfaces of the spoke devices (Branch 1 and Branch 2) through Cisco SD-WAN Manager with the following configurations:

Table 7: Branch 1 Configuration

Parameter	Values
Upstream Bandwidth (Edge/spoke device in branch 2 to edge device/hub in the data center)	• **Range:** 8000 Kbps—12000 Kbps • **Default:** 10000 Kbps
Downstream Bandwidth (Edge device/hub of data center to the edge/spoke device in branch 2)	• **Range:** 5000 Kbps—15000 Kbps • **Default:** 10000 Kbps
Adapt Period	30 Minutes

Table 8: Branch 2 Configuration

Parameter	Values
Upstream Bandwidth (Edge/spoke device in branch 2 to edge device/hub in the data center)	• **Range:** :16000 Kbps—20000 Kbps • **Default:** 10000 Kbps
Downstream Bandwidth (Edge device/hub of data center to the edge/spoke device in branch 2)	• **Range:** 10000 Kbps—30000 Kbps • **Default:** 20000 Kbps
Adapt Period	60 Minutes

Data Center

In the image, the per-tunnel QoS on the hub device in the data center reflects the downstream bandwidth configured on the spoke devices in Branch 1 and Branch 2.

Adaptive QoS in Cisco Catalyst SD-WAN is based on an algorithm based on packet drop or loss that works as follows:

Traffic Behavior	Analysis and Corresponding Adaptive QoS Behavior
No drops on the WAN or shapers	Shaper rate is not adjusted because the user traffic rate is low
Packet Drops in WAN	WAN bandwidth is oversubscribed. The shaper rate is thus adjusted to go DOWN to avoid packet drops.
Packet Drops in Shapers	A drop in shapers without packet drops in WAN indicates that the available WAN bandwidth is not being utilized; and therefore, the shaper rate is adjusted to go UP.

Workflow of Adaptive QoS

When the adapt period is configured, adaptive QoS follows these stages.

- **Adapt:** This is the initial stage where the shaping rate is based on the default value or is recalculated based on the last cycle.
- **Measure:** In this stage, shaper or WAN loss metrics are calculated. A single adapt cycle can have multiple loss measurement cycles.
- **Verify or Recalculate:** This stage verifies whether the shaper rate works as expected. Based on both the shaper rate and WAN loss rate, the drop-based algorithm is used to calculate the appropriate shaping rate for the next cycle.

Configure Adaptive QoS

To configure adaptive QoS use the Cisco VPN template for one of the following interfaces: Ethernet, Cellular, or DSL.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

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

3. Choose a device from the list on the left. Feature templates that are applicable to the device are shown in the right pane.
4. Choose one of the available Cisco VPN Interface templates. In this example, we've chosen the **Cisco VPN Interface Ethernet** template.
5. Enter a name and description for the feature template.
6. Click **ACL/QoS**.
7. Notice that Adaptive QoS is disabled by default. To enable it, from the Adaptive QoS drop-down list, choose **Global**, and choose **On**.
8. (Optional) Enter adaptive QoS parameters. You can leave the additional details at as default or specify your values.
    - **Adapt Period:** Choose **Global** from the drop-down list, click **On**, and enter the period in minutes.
    - **Shaping Rate Upstream:** Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, and default upstream bandwidth in Kbps.
    - **Shaping Rate Downstream:** Choose **Global** from the drop-down list, click **On**, and enter the minimum, maximum, downstream, and upstream bandwidth in Kbps.
9. Click **Save**.
10. Attach the feature template to a device template.

Configure Adaptive QoS Using the CLI

The following example shows the adaptive QoS configuration on the Ethernet interface of a Cisco IOS XE Catalyst SD-WAN device.

```
sdwan
 interface GigabitEthernet1
 qos-adaptive
  period 90
  downstream 8000
  downstream range 6000 10000
  upstream 8000
  upstream range 4000 16000
 exit
 tunnel-interface
  encapsulation ipsec weight 1
  color biz-internet
  no last-resort-circuit
  vmanage-connection-preference 5
  allow-service all
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
 exit
exit
```

Customize Adaptive QoS Configuration

How the Adaptive QoS Algorithm Works

With adaptive QoS, the QoS shaper rate is adjusted based on WAN loss and local network loss. WAN and local network loss are measured based on the IPSec or GRE sequence number in the overlay session. The adaptive QoS algorithm brings the QoS shaper rate DOWN when WAN loss crosses the configured threshold. The algorithm brings the QoS shaper rate UP when the local network loss is detected to be over the threshold.

The adaptive QoS algorithm consists of the following parameters.

Table 9:

Parameter	Default Value	Customizable	Adaptive QoS Behavior
WAN loss threshold	0.2%	Yes	If the WAN loss detected is above the threshold, the shaper rate adapts DOWN.
Spoke overlay traffic threshold	40%	Yes	The QoS shaper rate for a spoke adapts UP or DOWN only when the overlay user traffic out of the overall traffic is above the threshold.
Local loss threshold	0.1%	No	If only local loss detected is above the threshold (WAN loss is still within the threshold), and the traffic throughput crosses a certain usage threshold, the shaper rate adapts UP.
Pre-adapting UP overlay user traffic threshold	90%	No	When both WAN and local loss are below the threshold, and the overlay user traffic usage of the QoS shaper is above the threshold, the QoS shaper rate adapts UP.
Hub adapting UP overlay user traffic usage threshold	90%	No	When only local loss is above the threshold, and the QoS shaper rate for and the overlay user traffic is above the threshold, the QoS shaper rate adapts UP. This behavior prevents adapting if there is congestion on the parent schedulers.

Parameter	Default Value	Customizable	Adaptive QoS Behavior
Adapting Stride	Minimum: 1% Maximum: current QoS shaper rate	No	The QoS shaper rate adapts UP if the normal stride is 1/10 of the QoS shaper rate range. The QoS shaper rate adapts DOWN based on the normal stride in the shaper rate and WAN loss rate.

Customize Adaptive QoS Thresholds

The following parameters in the adaptive QoS algorithm can be customized.

- **WAN loss threshold:**

  Use the **platform qos sdwan adapt wan-loss-permillage** *<1~999 permillage>* through the configuration mode of the device CLI or using the CLI add-on feature template in Cisco SD-WAN Manager.

- **Spoke overlay traffic percentage:**

  Use the **platform qos sdwan adapt spoke-overlay-usage** *<1~100 percent>* through the configuration mode of the device CLI or using the CLI add-on feature template in Cisco SD-WAN Manager.

Monitor Adaptive QoS

Verify Upstream Configuration

The following sample output shows the adaptive QoS statistics collected for upstream traffic.

```
Device# show platform software sdwan qos adapt stats
INTERFACE             DEFAULT  MIN     MAX     PERD   SHAPE-RATE
                      (kbps)  (kbps)  (kbps)  (min)  (kbps)
GigabitEthernet0/0/4  20000   10000   40000   1      40000
```

This sample output shows upstream adaptive QoS statistics.

```
Device# show platform software sdwan qos adapt history all

SDWAN upstream adaptive QoS
Interface: GigabitEthernet3
Adaptive QoS History:
TIME                LOCAL-LOSS WAN-LOSS TOTAL-OFFER THROUGHPUT ADAPT SHAPE-RATE
                                         (pps)       (kbps)          (kbps)
2020-06-08T07:49:46 0.0%       0.0%     9600        13827      NOPE  50000
2020-06-08T07:48:46 0.0%       0.0%     9600        13826      NOPE  50000
2020-06-08T07:47:46 0.0%       0.0%     9600        13825      NOPE  50000
2020-06-08T07:46:46 0.0%       0.0%     9600        13827      NOPE  50000
2020-06-08T07:45:46 0.0%       0.0%     9600        13828      NOPE  50000
2020-06-08T07:44:46 0.0%       0.0%     9600        13828      NOPE  50000
2020-06-08T07:43:46 0.0%       0.0%     9600        13827      NOPE  50000
2020-06-08T07:42:46 0.0%       0.0%     9600        13832      NOPE  50000

SDWAN upstream adaptive QoS
Interface: Loopback0
Adaptive QoS History:
TIME                LOCAL-LOSS WAN-LOSS TOTAL-OFFER THROUGHPUT ADAPT SHAPE-RATE
                                         (pps)       (kbps)          (kbps)
2020-06-08T07:49:46 50.8%      0.0%     16282       7980       UP    8099
```

```
2020-06-08T07:48:46 50.2%      0.8%     16282       8073        DOWN  8019
2020-06-08T07:47:46 50.8%      0.0%     16287       8005        UP    8099
2020-06-08T07:46:46 50.4%      0.7%     16282       8056        DOWN  8019
2020-06-08T07:45:46 50.9%      0.0%     16282       7976        UP    8099
2020-06-08T07:44:46 50.2%      0.9%     16282       8084        DOWN  8019
2020-06-08T07:43:46 50.7%      0.1%     16282       8002        UP    8099
2020-06-08T07:42:46 50.2%      0.9%     16282       8083        DOWN  8019
```

This sample output shows the history of the upstream adaptive QoS for the specified interface.

```
Device# show platform software sdwan qos adapt history GigabitEthernet0/0/4
SDWAN upstream adaptive QoS
Interface: GigabitEthernet0/0/4
Adaptive QoS History:
TIME                LOCAL-LOSS WAN-LOSS TOTAL-OFFER THROUGHPUT ADAPT SHAPE-RATE
                                         (pps)       (kbps)          (kbps)
2020-05-21T02:43:44 56.0%      0.0%     34952       22087       UP    25100
2020-05-21T02:42:44 62.0%      0.0%     34952       19089       UP    22100
2020-05-21T02:41:44 67.9%      0.0%     34952       16091       UP    19100
2020-05-21T02:40:44 73.9%      0.0%     34952       13091       UP    16100
2020-05-21T02:39:44 79.9%      0.0%     34952       10091       UP    13100
2020-05-21T02:38:44 80.1%      0.0%     34952       9990        UP    10100
2020-05-21T02:37:44 80.1%      29.4%    34952       9990        DOWN  10000
2020-05-21T02:36:44 80.1%      29.4%    34952       9990        DOWN  10000
```

The following sample output shows the verification of the adaptive QoS configuration in the policy map applied to the GigabitEthernet3 interface.

```
Device# show policy-map interface GigabitEthernet3


  Service-policy output: shape_GigabitEthernet3

    Class-map: class-default (match-any)
      89140978 packets, 16580958431 bytes
      30 second offered rate 23246000 bps, drop rate 5255000 bps
      Match: any
      Queueing
      queue limit 83 packets
      (queue depth/total drops/no-buffer drops) 0/25186569/0
      (pkts output/bytes output) 73636046/13696793305
      shape (average) cir 20143000, bc 80572, be 80572
      target shape rate 20143000

      Service-policy : qos_policy_4class_cedge

        queue stats for all priority classes:
          Queueing
          priority level 1
          queue limit 512 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 2004810/373383409

        Class-map: Critical (match-any)
          6566981 packets, 1222194617 bytes
          30 second offered rate 13000 bps, drop rate 0000 bps
          Match: qos-group 0
          Priority: Strict, b/w exceed drops: 0

          Priority Level: 1
```

Verify Downstream Configuration

The following sample output shows the downstream adaptive QoS configuration.

```
Device# show sdwan omp tlocs

---------------------------------------------------
tloc entries for 10.6.0.3
                 lte
                 ipsec
---------------------------------------------------
            RECEIVED FROM:
peer            10.8.3.3
status          C,I,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     attribute-type    installed
     encap-key         not set
     encap-proto       0
     encap-spi         261
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         176.16.6.2
     public-port       12346
     private-ip        176.16.6.2
     private-port      12346
     public-ip         176:16:6::2
     public-port       12346
     private-ip        176:16:6::2
     private-port      12346
     bfd-status        up
     domain-id         not set
     site-id           601
     overlay-id        not set
     preference        1000
     tag               not set
     stale             not set
     weight            1
     version           3
    gen-id             0x8000012c
     carrier           carrier6
     restrict          0
     on-demand          0
     groups            [ 0 ]
     bandwidth         80000
     bandwidth-dmin    50000
     bandwidth-down    100000
     bandwidth-dmax    100000
     adapt-qos-period  15
     adapt-qos-up      1
     qos-group         default-group
     border             not set
     unknown-attr-len  not set
```

The following sample output shows downstream adaptive QoS statistics.

```
Device# show platform software sdwan qos adapt stats
================= Adaptive QoS Stats =================
COLOR           DEST-TLOC       DEST-IP         DEST-PORT ENCAP DEFAULT   MIN       MAX
    PERD SHAPE-RATE
                                                                (kbps)    (kbps)    (kbps)
    (min)(kbps)
```

```
lte             172.16.255.11   10.0.5.11       12347     IPSEC 100000    50000      100000
    1    100000
lte             172.16.255.14   10.1.14.14      12346     IPSEC 100000    50000      100000
    1    100000
```

The following sample output shows the adaptive QoS history of the eight most recent sessions on the tunnel.

```
Device# show platform software sdwan qos adapt history Tunnel1 10.1.14.14
SDWAN OMP Session
Color: lte
Dest Tloc: 172.16.255.14
Dest IP: 10.1.14.14
Dest Port: 12346
Encap: IPSEC
Adaptive QoS History:
TIME                LOCAL-LOSS WAN-LOSS TOTAL-OFFER THROUGHPUT ADAPT SHAPE-RATE
                                        (pps)       (kbps)           (kbps)
2020-05-21T04:51:28 30.0%      0.4%     87380       87852      DOWN  86973
2020-05-21T04:50:28 28.0%      2.9%     87380       90481      DOWN  87851
2020-05-21T04:49:28 31.9%      0.0%     87380       85553      UP    90474
2020-05-21T04:48:28 35.9%      0.0%     87380       80477      UP    85474
2020-05-21T04:47:28 39.9%      0.0%     87380       75475      UP    80474
2020-05-21T04:46:28 40.5%      0.0%     87380       74727      UP    75474
2020-05-21T04:45:28 39.9%      0.6%     87380       75480      DOWN  74727
2020-05-21T04:44:28 40.5%      0.0%     87380       74737      UP    75481
```

The following sample output shows the average shaper rate, target shaper rate, and the bandwidth remaining.

```
Device# show policy-map multipoint Tunnel1 10.1.14.14

Interface Tunnel1 <--> 10.1.14.14

  Service-policy output: SDWANPolicy4325397

    Class-map: class-default (match-any)
      343994858 packets, 59167000300 bytes
      5 minute offered rate 114034000 bps, drop rate 37596000 bps
      Match: any
      Queueing
      queue limit 362 packets
      (queue depth/total drops/no-buffer drops) 0/76866318/0
      (pkts output/bytes output) 246459053/45841211875
      shape (average) cir 87966000, bc 351864, be 351864
      target shape rate 87966000
      bandwidth remaining ratio 8

      Service-policy : qos_policy_4class_cedge

        queue stats for all priority classes:
          Queueing
          priority level 1
          queue limit 512 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 40145494/7466889901

        Class-map: Critical (match-any)
          68807464 packets, 11834768360 bytes
          5 minute offered rate 22815000 bps, drop rate 10139000 bps
          Match: qos-group 0
          Priority: Strict, b/w exceed drops: 0

          Priority Level: 1
          police:
              rate 15 %
```

```
                  rate 13065500 bps, burst 408296 bytes
                conformed 40141805 packets, 6904295187 bytes; actions: transmit
```

CHAPTER 7

Per-VPN QoS

Table 10: Feature History

Feature Name	Release Information	Description
Per-VPN QoS	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	When a Cisco IOS XE Catalyst SD-WAN device receives traffic belonging to different VPNs from the branch network, you can configure a QoS policy to limit the bandwidth that can be used by the traffic belonging to each VPN or each group of VPNs.

Restriction for Per-VPN QoS

- Before you apply Per-VPN QoS, you must upgrade Cisco SD-WAN Controller software to Cisco SD-WAN Release 20.6.1 or a later release, and Cisco SD-WAN Manager to Cisco vManage Release 20.6.1 or a later release.

- VPN-QoS policy must be applied to a WAN interface and affects outbound traffic on the specific WAN interface to which it is applied.

- While applying a VPN-QoS policy to a WAN interface, you must configure a shaping rate for the interface.

- For each VPN or group of VPNs that you wish to include in a VPN-QoS policy, you must define a QoS map to allocate resources to the various queues.

- The sum of the minimum bandwidths allocated to each VPN or each group of VPNs must be less than shaping rate configured for the WAN interface.

After you apply a VPN-QoS policy, during congestion, IPSec-encapsulated packets may be forwarded out of sequence. To prevent valid out-of-sequence packets being dropped on the remote side, you must enable IPSec extended anti-replay window on both the source and remote Cisco IOS XE Catalyst SD-WAN devices.

- You can include a maximum of 100 VPN lists in a VPN-QoS policy map.
- Cisco SD-WAN Manager QoS monitoring does not support the monitoring of the VPN-QoS policy.
- You cannot configure Per-VPN QoS together with Per-Tunnel QoS.

Information About Per-VPN QoS

A Cisco IOS XE Catalyst SD-WAN device receives traffic from a branch network and routes the traffic to a remote branch through the SD-WAN overlay network. The link from the WAN interface of the Cisco IOS XE Catalyst SD-WAN device has limited bandwidth. To achieve a desired QoS for traffic belonging to different applications, you must control how the limited bandwidth is used. When the traffic from the branch network belongs to different VPNs, you may need to restrict the bandwidth that can be used by traffic belonging to different VPNs and categorize the traffic belonging to each VPN into various priority classes through a QoS policy.

You can configure the following aspects to achieve a specific QoS for each VPN or each group of VPNs:

- Classes: Create forwarding classes and associate them with specific interface queues (queue 0 to queue 7). To differentiate traffic from different applications, you can assign traffic from each application or application group to a specific forwarding class.
- VPN Lists: Define a VPN list consisting of a VPN or two or more VPNs that must be treated alike
- QoS Maps: Define parameters such as the bandwidth and buffer percentage, and the scheduling and packet-drop schemes for each queue.
- VPN QoS Map: Associate a QoS map with each VPN list and define the minimum and maximum bandwidth that must be used by traffic belonging to the VPNs in the VPN list.
- WAN Interface: Associate the VPN QoS Map with the Cisco VPN Interface Ethernet template for the WAN interface. Use the same template to specify a shaping rate for the interface.

When you complete these configurations, a three-level hierarchical QoS model is applied to the branch traffic comprising the following scheduling and shaping considerations:

- packet scheduling based on forwarding classes and bandwidth distribution among interface queues
- packet scheduling and bandwidth distribution among VPNs or VPN groups
- shaping of the WAN interface bandwidth

Extended Anti-Replay Window

The IPSec session between two WAN edge devices is common for all VPNs. The packets from each of the eight interface queues are encapsulated using a different sequence name space (SNS). When you apply QoS policy per VPN, packets are prioritized based on their forwarding class and associated interface queue, and the bandwidth available for the VPN to which the packets belong. As a result, during a congestion, the IPSec encapsulated packets may be forwarded out of sequence and be dropped by the remote WAN edge device.

To avoid valid out of sequence packets being dropped, you can configure an extended anti-replay window on both the source and remote Cisco IOS XE Catalyst SD-WAN device.

When you enable extended anti-replay and configure an extended anti-replay window, the source WAN edge router adds a time stamp to each packet in the IPSec ESP HDR 99. On receiving a packet, if the packet sequence number is lower than the lowest sequence number in the sequence window, the remote router examines the time stamp.

- If the time stamp is within the configured window or exceeds the highest time stamp in the window, the packet is accepted.
- If the time stamp is lower than the lowest time stamp in the configured window, the packet is dropped.

Note Duplicate packets with sequence numbers beyond the IPSec anti-replay sequence window but within extended anti-replay window cannot be detected and may be forwarded towards the branch.

Benefits of Per-VPN QoS

- Bandwidth consumption and traffic throughput can be controlled based on the VPN to which the traffic belongs.
- A greedy VPN cannot use outbound bandwidth beyond the allocated limit and does not starve other VPNs.
- Different classes of service can be configured for each VPN on a single WAN interface.

Configure Per-VPN QoS

Create Forwarding Classes

When you create a forwarding class, you map it to a queue. By associating traffic from different applications with different classes, you can ensure that the packets enter different queues. Using the QoS map, you can configure the outbound bandwidth, buffer and other properties for each queue to prioritize among the traffic streams served by these queues and achieve the desired QoS.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. From the list types on the left, click **Class Map**.
5. Click **New Class List**.
    a. Enter a unique name for the forwarding class.
    b. Choose a queue to which to map the forwarding class.
    c. Click **Save**.

6. Repeat Step 5 and the substeps to create more forwarding classes.

Create VPN Lists

A VPN list consists of one or more VPNs that need to be treated alike. To apply a specific QoS policy to traffic from a VPN or a group of similar VPNs, the QoS policy is linked to the corresponding VPN list.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. From the list types on the left, click **VPN**.
5. Click **New VPN List**.
    a. Enter a unique name for the VPN list.
    b. Enter the IDs of the VPNs to be included in the list.
    c. Click **Add**.
6. Repeat Step 5 and the substeps to create more VPN lists.

Create QoS Maps

Use QoS maps to distribute resources such as bandwidth and buffer among forwarding classes. Create as many QoS maps as required to apply different QoS policies to the different VPN lists.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. Click **Next**.
5. Click **Add QoS Map** and click **Create New**.
6. Enter a unique name for the QoS map.
7. Enter a description for the QoS map.
8. Click **Add Queue**.
    a. Choose a queue to add to the map.
    b. Choose the bandwidth percentage to allocate to the queue.
    c. Choose the buffer percentage to allocate to the queue.
    d. Packets exceeding the bandwidth or buffer percentage are dropped. Choose whether the packets are dropped randomly (**Random Early**) or from the end of the queue (**Tail**).
    e. Click **Save Queue**.

9. Repeat Step 8 and the substeps to add as more queues.
10. Click **Save Policy**.

Create VPN QoS Map

Use a VPN QoS Map to associate QoS policies with target VPN lists.

Note Before you proceed with the following steps, configure the required QoS Maps and VPN lists.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy** and click **Next**.
4. Create or import QoS maps and click **Next**.
5. Click **VPN QoS Map**.
6. Click **Add VPN Policy** and click **Create New**.
7. Enter a unique name and a description for the VPN QoS map.
8. For the default VPN, click the Edit icon.
    a. (Optional) Enter the maximum bandwidth for traffic belonging to the default VPN.
    b. Choose a QoS Map to apply a QoS policy to the default VPN.
    c. Click **Save VPN**.
9. Click **Add VPN**.
    a. Choose a VPN list.
    b. Enter the minimum bandwidth for traffic belonging to the VPNs.
    c. (Optional) Enter the maximum bandwidth for traffic belonging to the VPNs.
    d. Choose a QoS Map to apply a QoS policy to the VPNs.
    e. Click **Save VPN**.
10. Repeat Step 9 and the substeps to add more VPN lists.
11. Click **Save Policy**.
12. Apply the localized policy to the relevant device template.

Configure Extended Anti-Replay Window

Configure extended anti-replay window on both the source and remote Cisco IOS XE Catalyst SD-WAN devices.

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

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

3. In the list of templates, locate the Cisco Security template for the Cisco IOS XE Catalyst SD-WAN device.
4. Click **...** for the template and choose **Edit**.
5. Choose **Basic Configuration**.
6. To enable **Extended Anti Replay**, click **On**.
7. (Optional) Enter **Extended Anti-Replay Window** duration.

   Default duration: 256 ms

   Range: 10 ms to 2048 ms

   Note Choose an appropriate duration based on the configured queue limits and the traffic profile.

8. Click **Update**.

Attach VPN QoS Map to WAN Interface

To apply the QoS policy per VPN, attach the VPN QoS map to the Cisco VPN Interface Ethernet template for the WAN interface.

Note Before you proceed with the following steps, apply the localized policy in which the VPN-QoS Map is defined to the relevant device template.

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

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

3. In the list of templates, locate the Cisco VPN Interface Ethernet template for the WAN interface.
4. Click **...** adjacent to the template and choose **Edit**.
5. Choose **ACL/QoS**.
6. For **Shaping Rate (kbps)**, choose the configuration type as **Global** and enter a shaping rate value.
7. For **VPN QoS Map**, choose the configuration type as **Global** and enter the name of the VPN QoS map.

8. Click **Update**.

Configure Per-VPN QoS Using CLI

Example: Configure Per-VPN QoS

This section provides example command sequences to configure QoS for a VPN or a group of VPNs using a CLI template.

1. Configure class maps for VPN groups.

```
class-map match-any VPN_GROUP_100
 match packet-tag 1 100 65535
class-map match-any VPN_GROUP_101
 match packet-tag 1 101 65535
 match packet-tag 1 102 65535
class-map match-any VPN_GROUP_103
 match packet-tag 1 103 65535
 match packet-tag 1 104 65534
class-map match-any VPN_GROUP_106
 match packet-tag 1 106 65534
 match packet-tag 1 108 65534
```

2. Configure QoS policy map.

```
policy-map qos_policy_4class_10Mbps
 class Queue0
  priority level 1 2000
 class Queue1
  bandwidth remaining ratio 30
  random-detect precedence-based
 class class-default
  bandwidth remaining ratio 25
 class Queue3
  bandwidth remaining ratio 25
```

3. Configure VPN QoS policy map.

```
policy-map VPN-QoS1_200Mbps
 class VPN_GROUP_100
  bandwidth remaining ratio 50
  service-policy qos_policy_4class_10Mbps
  shape average 20000000
 class VPN_GROUP_101
  bandwidth remaining ratio 100
  service-policy qos_policy_8class_20Mbps
 class VPN_GROUP_103
  bandwidth remaining ratio 150
  service-policy qos_policy_4class_30Mbps
  shape average 50000000
 class VPN_GROUP_106
  bandwidth remaining ratio 200
  service-policy qos_policy_8class_40Mbps
  shape average 100000000
 class class-default
  bandwidth remaining ratio 500
  service-policy qos_policy_8class_100Mbps
```

4. Configure extended anti-replay window.

```
security
 ipsec
  extended-ar-window 256
```

5. Attach VPN QoS policy map to WAN Ethernet interface.

```
policy-map shape_GigabitEthernet0/0/1
 class class-default
  service-policy VPN-QoS1_200Mbps
  shape average 200000000
!
interface GigabitEthernet0/0/1
 service-policy output shape_GigabitEthernet0/0/1
```

6. Configure VPN packet tag.

```
sdwan
 vpn packet-tag 1
!
```

Note Per-VPN QoS uses the **vpn packet-tag** command to classify the VPN ID. Use this command only while configuring per-VPN QoS using the CLI. The command is automatically pushed when you configure per-VPN QoS through Cisco SD-WAN Manager.

Here's the complete configuration example:

```
class-map match-any VPN_GROUP_100
 match packet-tag 1 100 65535
class-map match-any VPN_GROUP_101
 match packet-tag 1 101 65535
 match packet-tag 1 102 65535
class-map match-any VPN_GROUP_103
 match packet-tag 1 103 65535
 match packet-tag 1 104 65534
class-map match-any VPN_GROUP_106
 match packet-tag 1 106 65534
 match packet-tag 1 108 65534
!
policy-map qos_policy_4class
 class Queue0
  police rate percent 20
  priority level 1
 class Queue1
  bandwidth remaining ratio 30
  random-detect precedence-based
 class class-default
  bandwidth remaining ratio 25
 class Queue3
  bandwidth remaining ratio 25
!
policy-map qos_policy_4class_10Mbps
 class Queue0
  priority level 1 2000
 class Queue1
  bandwidth remaining ratio 30
  random-detect precedence-based
 class class-default
  bandwidth remaining ratio 25
 class Queue3
  bandwidth remaining ratio 25
!
```

```
policy-map qos_policy_4class_30Mbps
 class Queue0
  priority level 1 6000
 class Queue1
  bandwidth remaining ratio 30
  random-detect precedence-based
 class class-default
  bandwidth remaining ratio 25
 class Queue3
  bandwidth remaining ratio 25
!
policy-map qos_policy_8class
 class Queue0
  police rate percent 20
  priority level 1
 class Queue1
  bandwidth remaining ratio 10
  random-detect precedence-based
 class class-default
  bandwidth remaining ratio 15
 class Queue3
  bandwidth remaining ratio 10
  random-detect precedence-based
 class Queue4
  bandwidth remaining ratio 15
 class Queue5
  bandwidth remaining ratio 10
 class Queue6
  bandwidth remaining ratio 15
  random-detect precedence-based
 class Queue7
  bandwidth remaining ratio 5
!
policy-map qos_policy_8class_100Mbps
 class Queue0
  priority level 1 20000
 class Queue1
  bandwidth remaining ratio 10
  random-detect precedence-based
 class class-default
  bandwidth remaining ratio 15
 class Queue3
  bandwidth remaining ratio 10
  random-detect precedence-based
 class Queue4
  bandwidth remaining ratio 15
 class Queue5
  bandwidth remaining ratio 10
 class Queue6
  bandwidth remaining ratio 15
  random-detect precedence-based
 class Queue7
  bandwidth remaining ratio 5
!
policy-map qos_policy_8class_20Mbps
 class Queue0
  priority level 1 4000
 class Queue1
  bandwidth remaining ratio 10
  random-detect precedence-based
 class class-default
  bandwidth remaining ratio 15
 class Queue3
  bandwidth remaining ratio 10
  random-detect precedence-based
 class Queue4
  bandwidth remaining ratio 15
 class Queue5
  bandwidth remaining ratio 10
 class Queue6
  bandwidth remaining ratio 15
  random-detect precedence-based
 class Queue7
  bandwidth remaining ratio 5
!
policy-map qos_policy_8class_40Mbps
 class Queue0
  priority level 1 8000
 class Queue1
  bandwidth remaining ratio 10
  random-detect precedence-based
 class class-default
  bandwidth remaining ratio 15
 class Queue3
  bandwidth remaining ratio 10
  random-detect precedence-based
 class Queue4
  bandwidth remaining ratio 15
 class Queue5
  bandwidth remaining ratio 10
 class Queue6
  bandwidth remaining ratio 15
  random-detect precedence-based
 class Queue7
  bandwidth remaining ratio 5
!
policy-map VPN-QoS1_200Mbps
 class VPN_GROUP_100
  bandwidth remaining ratio 50
  service-policy qos_policy_4class_10Mbps
  shape average 20000000
 class VPN_GROUP_101
  bandwidth remaining ratio 100
  service-policy qos_policy_8class_20Mbps
 class VPN_GROUP_103
  bandwidth remaining ratio 150
  service-policy qos_policy_4class_30Mbps
  shape average 50000000
 class VPN_GROUP_106
  bandwidth remaining ratio 200
  service-policy qos_policy_8class_40Mbps
  shape average 100000000
 class class-default
  bandwidth remaining ratio 500
  service-policy qos_policy_8class_100Mbps
!
sdwan
 vpn packet-tag 1
!
policy-map shape_GigabitEthernet0/0/1
 class class-default
  service-policy VPN-QoS1_200Mbps
  shape average 200000000
!
interface GigabitEthernet0/0/1
 service-policy output shape_GigabitEthernet0/0/1
!
security
```

```
 ipsec
  rekey              86400
  replay-window      512
  integrity-type     esp ip-udp-esp
  extended-ar-window 256
 !
!
```

Verify Per-VPN QoS Configuration

Verify VPN Group Configuration

The following is a sample output from the execution of the **show sdwan running-config** command with the keyword **class-map** on a Cisco IOS XE Catalyst SD-WAN device:

```
Device#show sdwan running-config class-map
.
.
.
class-map match-any VPN_GROUP_100
 match packet-tag 1 100 65535
!
class-map match-any VPN_GROUP_101
 match packet-tag 1 101 65535
 match packet-tag 1 102 65535
!
class-map match-any VPN_GROUP_103
 match packet-tag 1 103 65535
 match packet-tag 1 104 65534
!
class-map match-any VPN_GROUP_106
 match packet-tag 1 106 65534
 match packet-tag 1 108 65534
!
.
.
.
```

Verify QoS Policy, VPN QoS Policy, and WAN Ethernet Interface Shaping Configuration

The following is a sample output from the execution of the **show sdwan running-config** command with the keyword **policy-map** on a Cisco IOS XE Catalyst SD-WAN device:

```
Device#show sdwan running-config policy-map
policy-map VPN-QoS1_200Mbps
 class VPN_GROUP_100
  bandwidth remaining ratio 50
  service-policy qos_policy_4class_10Mbps
  shape average 20000000
 !
 class VPN_GROUP_101
  bandwidth remaining ratio 100
  service-policy qos_policy_8class_20Mbps
 !
 class VPN_GROUP_103
  bandwidth remaining ratio 150
  service-policy qos_policy_4class_30Mbps
  shape average 50000000
 !
 class VPN_GROUP_106
  bandwidth remaining ratio 200
  service-policy qos_policy_8class_40Mbps
  shape average 100000000
 !
 class class-default
  bandwidth remaining ratio 500
  service-policy qos_policy_8class_100Mbps
 !
!
.
.
.
policy-map qos_policy_4class_10Mbps
 class Queue0
  priority level 1 2000
 !
 class Queue1
  bandwidth remaining ratio 30
  random-detect precedence-based
 !
 class class-default
  bandwidth remaining ratio 25
 !
 class Queue3
  bandwidth remaining ratio 25
 !
!
.
.
.
policy-map shape_GigabitEthernet0/0/1
 class class-default
  service-policy VPN-QoS1_200Mbps
  shape average 200000000
 !
!
```

Verify Extended Anti-Replay Window Configuration

The following is a sample output from the execution of the **show sdwan running-config** command with the keyword **security** on a Cisco IOS XE Catalyst SD-WAN device:

```
Device#show sdwan running-config security
security
 ipsec
  rekey              86400
  replay-window      512
  integrity-type     esp ip-udp-esp
  extended-ar-window 256
 !
!
```

Verify VPN Packet Tag Configuration

The following is a sample output from the execution of the **show sdwan running-config** command with the keyword **sdwan** on a Cisco IOS XE SD-WAN device:

```
Device#show sdwan running-config sdwan
sdwan
 .
 .
 .
 vpn packet-tag 1
 .
 .
 .
 !
!
```

Monitor Per-VPN QoS Using CLI

Monitor Per-VPN QoS on WAN Ethernet Interface

The following is a sample output from the execution of the **show policy-map interface GigabitEthernet** command on a Cisco IOS XE Catalyst SD-WAN device:

```
Device# show policy-map interface GigabitEthernet0/0/1
 GigabitEthernet0/0/1

  Service-policy output: shape_GigabitEthernet0/0/1

    Class-map: class-default (match-any)
      211055879 packets, 148615306000 bytes
      30 second offered rate 509063000 bps, drop rate 309050000 bps
      Match: any
      Queueing
      queue limit 833 packets
      (queue depth/total drops/no-buffer drops) 0/132320694/0
      (pkts output/bytes output) 78735064/58389530406
      shape (average) cir 200000000, bc 800000, be 800000
      target shape rate 200000000

      Service-policy : VPN-QoS1_200Mbps

        Class-map: VPN_GROUP_100 (match-any)
          11408118 packets, 6454975577 bytes
          30 second offered rate 22112000 bps, drop rate 12108000 bps
          Match: packet-tag  1 100 65535
          Queueing
          queue limit 83 packets
          (queue depth/total drops/no-buffer drops) 0/6246212/0
          (pkts output/bytes output) 5161897/2919614491
          bandwidth remaining ratio 50
          shape (average) cir 20000000, bc 80000, be 80000
          target shape rate 20000000

          Service-policy : qos_policy_4class_10Mbps

            queue stats for all priority classes:
              Queueing
              priority level 1
              queue limit 512 packets
              (queue depth/total drops/no-buffer drops) 0/0/0
              (pkts output/bytes output) 5056/842485

            Class-map: Queue0 (match-any)
              5056 packets, 842485 bytes
              30 second offered rate 2000 bps, drop rate 0000 bps
              Match: qos-group 0
              Priority: 2000 kbps, burst bytes 50000, b/w exceed drops: 0

              Priority Level: 1

            Class-map: Queue1 (match-any)
              0 packets, 0 bytes
              30 second 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 remaining ratio 30
                Exp-weight-constant: 4 (1/16)
                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
              30 second offered rate 0000 bps, drop rate 0000 bps
              Match: qos-group 3
              Queueing
              queue limit 83 packets
              (queue depth/total drops/no-buffer drops) 0/0/0
              (pkts output/bytes output) 0/0
              bandwidth remaining ratio 25

            Class-map: class-default (match-any)
              11403053 packets, 6454127998 bytes
              30 second offered rate 22108000 bps, drop rate 12113000 bps
              Match: any
              Queueing
              queue limit 83 packets
              (queue depth/total drops/no-buffer drops) 83/6246212/0
              (pkts output/bytes output) 5156841/2918772006
              bandwidth remaining ratio 25

        Class-map: VPN_GROUP_101 (match-any)
          28507656 packets, 16135333296 bytes
          30 second offered rate 55272000 bps, drop rate 35296000 bps
          Match: packet-tag  1 101 65535
          Match: packet-tag  1 102 65535
          Queueing
          queue limit 833 packets
          (queue depth/total drops/no-buffer drops) 0/18192317/0
          (pkts output/bytes output) 10315322/5838472252
          bandwidth remaining ratio 100

          Service-policy : qos_policy_8class_20Mbps

            queue stats for all priority classes:
              Queueing
              priority level 1
              queue limit 512 packets
              (queue depth/total drops/no-buffer drops) 0/0/0
              (pkts output/bytes output) 0/0

            Class-map: Queue0 (match-any)
              0 packets, 0 bytes
              30 second offered rate 0000 bps, drop rate 0000 bps
              Match: qos-group 0
              Priority: 4000 kbps, burst bytes 100000, b/w exceed drops: 0

              Priority Level: 1

            Class-map: Queue1 (match-any)
              0 packets, 0 bytes
              30 second offered rate 0000 bps, drop rate 0000 bps
              Match: qos-group 1
              Queueing
              queue limit 833 packets
              (queue depth/total drops/no-buffer drops) 0/0/0
              (pkts output/bytes output) 0/0
              bandwidth remaining ratio 10
                Exp-weight-constant: 4 (1/16)
                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                208
          416  1/10
                1               0/0               0/0              0/0                234
          416  1/10
                2               0/0               0/0              0/0                260
          416  1/10
                3               0/0               0/0              0/0                286
          416  1/10
                4               0/0               0/0              0/0                312
          416  1/10
                5               0/0               0/0              0/0                338
          416  1/10
                6               0/0               0/0              0/0                364
          416  1/10
                7               0/0               0/0              0/0                390
          416  1/10

            Class-map: Queue3 (match-any)
              0 packets, 0 bytes
              30 second offered rate 0000 bps, drop rate 0000 bps
              Match: qos-group 3
              Queueing
              queue limit 833 packets
              (queue depth/total drops/no-buffer drops) 0/0/0
              (pkts output/bytes output) 0/0
              bandwidth remaining ratio 10
                Exp-weight-constant: 4 (1/16)
                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                208
          416  1/10
                1               0/0               0/0              0/0                234
          416  1/10
                2               0/0               0/0              0/0                260
          416  1/10
                3               0/0               0/0              0/0                286
          416  1/10
                4               0/0               0/0              0/0                312
          416  1/10
                5               0/0               0/0              0/0                338
          416  1/10
                6               0/0               0/0              0/0                364
          416  1/10
                7               0/0               0/0              0/0                390
          416  1/10

            Class-map: Queue4 (match-any)
              0 packets, 0 bytes
              30 second offered rate 0000 bps, drop rate 0000 bps
              Match: qos-group 4
              Queueing
              queue limit 833 packets
              (queue depth/total drops/no-buffer drops) 0/0/0
              (pkts output/bytes output) 0/0
              bandwidth remaining ratio 15

            Class-map: Queue5 (match-any)
              0 packets, 0 bytes
              30 second offered rate 0000 bps, drop rate 0000 bps
              Match: qos-group 5
              Queueing
              queue limit 833 packets
              (queue depth/total drops/no-buffer drops) 0/0/0
              (pkts output/bytes output) 0/0
              bandwidth remaining ratio 10

            Class-map: Queue6 (match-any)
              0 packets, 0 bytes
              30 second offered rate 0000 bps, drop rate 0000 bps
              Match: qos-group 6
              Queueing
              queue limit 833 packets
              (queue depth/total drops/no-buffer drops) 0/0/0
              (pkts output/bytes output) 0/0
              bandwidth remaining ratio 15
                Exp-weight-constant: 4 (1/16)
                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                208
          416  1/10
```

```
        1               0/0               0/0              0/0                234
  416  1/10
        2               0/0               0/0              0/0                260
  416  1/10
        3               0/0               0/0              0/0                286
  416  1/10
        4               0/0               0/0              0/0                312
  416  1/10
        5               0/0               0/0              0/0                338
  416  1/10
        6               0/0               0/0              0/0                364
  416  1/10
        7               0/0               0/0              0/0                390
  416  1/10

    Class-map: Queue7 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 7
      Queueing
      queue limit 833 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 5

    Class-map: class-default (match-any)
      28507639 packets, 16135323674 bytes
      30 second offered rate 55272000 bps, drop rate 35266000 bps
      Match: any
      Queueing
      queue limit 833 packets
      (queue depth/total drops/no-buffer drops) 832/18192317/0
      (pkts output/bytes output) 10315322/5838472252
      bandwidth remaining ratio 15

Class-map: VPN_GROUP_103 (match-any)
  57015313 packets, 32270667158 bytes
  30 second offered rate 110545000 bps, drop rate 80571000 bps
  Match: packet-tag  1 103 65535
  Match: packet-tag  1 104 65534
  Queueing
  queue limit 208 packets
  (queue depth/total drops/no-buffer drops) 0/41550294/0
  (pkts output/bytes output) 15464994/8753186604
  bandwidth remaining ratio 150
  shape (average) cir 50000000, bc 200000, be 200000
  target shape rate 50000000

  Service-policy : qos_policy_4class_30Mbps

    queue stats for all priority classes:
      Queueing
      priority level 1
      queue limit 512 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0

    Class-map: Queue0 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 0
      Priority: 6000 kbps, burst bytes 150000, b/w exceed drops: 0

      Priority Level: 1
    Class-map: Queue1 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 1
      Queueing
      queue limit 208 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 30
        Exp-weight-constant: 4 (1/16)
        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                 52
  104  1/10
        1               0/0               0/0               0/0                 58
  104  1/10
        2               0/0               0/0               0/0                 65
  104  1/10
        3               0/0               0/0               0/0                 71
  104  1/10
        4               0/0               0/0               0/0                 78
  104  1/10
        5               0/0               0/0               0/0                 84
  104  1/10
        6               0/0               0/0               0/0                 91
  104  1/10
        7               0/0               0/0               0/0                 97
  104  1/10

    Class-map: Queue3 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 3
      Queueing
      queue limit 208 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 25

    Class-map: class-default (match-any)
      57015288 packets, 32270653008 bytes
      30 second offered rate 110544000 bps, drop rate 80551000 bps
      Match: any
      Queueing
      queue limit 208 packets
      (queue depth/total drops/no-buffer drops) 207/41550294/0
      (pkts output/bytes output) 15464994/8753186604
      bandwidth remaining ratio 25

Class-map: VPN_GROUP_106 (match-any)
  57015315 packets, 32270668290 bytes
  30 second offered rate 110545000 bps, drop rate 70593000 bps
  Match: packet-tag  1 106 65534
  Match: packet-tag  1 108 65534
  Queueing
  queue limit 416 packets
  (queue depth/total drops/no-buffer drops) 0/36386201/0
  (pkts output/bytes output) 20629094/11676067204
  bandwidth remaining ratio 200
  shape (average) cir 100000000, bc 400000, be 400000
  target shape rate 100000000

  Service-policy : qos_policy_8class_40Mbps

    queue stats for all priority classes:
      Queueing
      priority level 1
      queue limit 512 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0

    Class-map: Queue0 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 0
      Priority: 8000 kbps, burst bytes 200000, b/w exceed drops: 0

      Priority Level: 1

    Class-map: Queue1 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 1
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 10
        Exp-weight-constant: 4 (1/16)
        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                104
  208  1/10
        1               0/0               0/0              0/0                117
  208  1/10
        2               0/0               0/0              0/0                130
  208  1/10
        3               0/0               0/0              0/0                143
  208  1/10
        4               0/0               0/0              0/0                156
  208  1/10
        5               0/0               0/0              0/0                169
  208  1/10
        6               0/0               0/0              0/0                182
  208  1/10
        7               0/0               0/0              0/0                195
  208  1/10

    Class-map: Queue3 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 3
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 10
        Exp-weight-constant: 4 (1/16)
        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                104
  208  1/10
        1               0/0                0/0              0/0                117
  208  1/10
        2               0/0                0/0              0/0                130
  208  1/10
        3               0/0                0/0              0/0                143
  208  1/10
        4               0/0                0/0              0/0                156
  208  1/10
        5               0/0                0/0              0/0                169
  208  1/10
        6               0/0                0/0              0/0                182
  208  1/10
        7               0/0                0/0              0/0                195
  208  1/10

    Class-map: Queue4 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 4
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 15

    Class-map: Queue5 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 5
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 10

    Class-map: Queue6 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 6
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 15
        Exp-weight-constant: 4 (1/16)
        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                104
  208  1/10
        1               0/0                0/0              0/0                117
  208  1/10
        2               0/0                0/0              0/0                130
  208  1/10
```

```
        3               0/0               0/0               0/0                143
  208  1/10
        4               0/0               0/0               0/0                156
  208  1/10
        5               0/0               0/0               0/0                169
  208  1/10
        6               0/0               0/0               0/0                182
  208  1/10
        7               0/0               0/0               0/0                195
  208  1/10

    Class-map: Queue7 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 7
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 5

    Class-map: class-default (match-any)
      57015295 packets, 32270656970 bytes
      30 second offered rate 110544000 bps, drop rate 70575000 bps
      Match: any
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 415/36386201/0
      (pkts output/bytes output) 20629094/11676067204
      bandwidth remaining ratio 15

Class-map: class-default (match-any)
  57109439 packets, 61483635051 bytes
  30 second offered rate 210589000 bps, drop rate 110479000 bps
  Match: any
  Queueing
  queue limit 833 packets
  (queue depth/total drops/no-buffer drops) 0/29945670/0
  (pkts output/bytes output) 27163757/29202189855
  bandwidth remaining ratio 500

  Service-policy : qos_policy_8class_100Mbps

    queue stats for all priority classes:
      Queueing
      priority level 1
      queue limit 512 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 94100/21122793

    Class-map: Queue0 (match-any)
      94100 packets, 21122793 bytes
      30 second offered rate 46000 bps, drop rate 0000 bps
      Match: qos-group 0
      Priority: 20000 kbps, burst bytes 500000, b/w exceed drops: 0

      Priority Level: 1

    Class-map: Queue1 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 1
      Queueing
      queue limit 833 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 10
        Exp-weight-constant: 4 (1/16)
        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                 208
  416  1/10
        1               0/0               0/0              0/0                 234
  416  1/10
        2               0/0               0/0              0/0                 260
  416  1/10
        3               0/0               0/0              0/0                 286
  416  1/10
        4               0/0               0/0              0/0                 312
  416  1/10
        5               0/0               0/0              0/0                 338
  416  1/10
        6               0/0               0/0              0/0                 364
  416  1/10
        7               0/0               0/0              0/0                 390
  416  1/10

    Class-map: Queue3 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 3
      Queueing
      queue limit 833 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 10
        Exp-weight-constant: 4 (1/16)
        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                 208
  416  1/10
        1               0/0               0/0              0/0                 234
  416  1/10
        2               0/0               0/0              0/0                 260
  416  1/10
        3               0/0               0/0              0/0                 286
  416  1/10
        4               0/0               0/0              0/0                 312
  416  1/10
        5               0/0               0/0              0/0                 338
  416  1/10
        6               0/0               0/0              0/0                 364
  416  1/10
        7               0/0               0/0              0/0                 390
  416  1/10

    Class-map: Queue4 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 4
      Queueing
      queue limit 833 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 15

    Class-map: Queue5 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 5
      Queueing
      queue limit 833 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 10

    Class-map: Queue6 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 6
      Queueing
      queue limit 833 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 15
        Exp-weight-constant: 4 (1/16)
        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                 208
  416  1/10
        1               0/0               0/0              0/0                 234
  416  1/10
        2               0/0               0/0              0/0                 260
  416  1/10
        3               0/0               0/0              0/0                 286
  416  1/10
        4               0/0               0/0              0/0                 312
  416  1/10
        5               0/0               0/0              0/0                 338
  416  1/10
        6               0/0               0/0              0/0                 364
  416  1/10
        7               0/0               0/0              0/0                 390
  416  1/10

    Class-map: Queue7 (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: qos-group 7
      Queueing
      queue limit 833 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 5

    Class-map: class-default (match-any)
      57015327 packets, 61462499322 bytes
      30 second offered rate 210542000 bps, drop rate 110548000 bps
      Match: any
      Queueing
```

```
              queue limit 833 packets
              (queue depth/total drops/no-buffer drops) 832/29945670/0
              (pkts output/bytes output) 27069657/29181067062
              bandwidth remaining ratio 15
Device#
```

Monitor Extended Anti-Replay Feature for Local and Remote TLOCs

The following is a sample output from the execution of the **show sdwan omp tlocs** command on a Cisco IOS XE Catalyst SD-WAN device:

```
Device#show sdwan omp tlocs
.
.
.
---------------------------------------------------
tloc entries for 10.6.0.1
                 mpls
                 ipsec
---------------------------------------------------
            RECEIVED FROM:
peer            10.8.3.3
status          C,I,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     attribute-type    installed
     encap-key         not set
     encap-proto       0
     encap-spi         258
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         176.16.60.2
     public-port       12346
     private-ip        176.16.60.2
     private-port      12346
     public-ip         176:16:60:0:250:56ff:fea5:580a
     public-port       12346
     private-ip        176:16:60:0:250:56ff:fea5:580a
     private-port      12346
     bfd-status        up
     domain-id         not set
     site-id           600
     overlay-id        not set
     preference        1000
     tag               not set
     stale             not set
     weight            1
     version           3
    gen-id             0x8000022f
     carrier           default
     restrict          1
     on-demand          1
     groups            [ 0 ]
     bandwidth         0
     bandwidth-dmin    0
     bandwidth-down    0
     bandwidth-dmax    0
     adapt-qos-period  0
     adapt-qos-up      0
     qos-group         default-group
     border             not set
     extended-ipsec-anti-replay  1
     unknown-attr-len  not set
            RECEIVED FROM:
peer            10.8.4.4
status          C,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     attribute-type    installed
     encap-key         not set
     encap-proto       0
     encap-spi         258
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         176.16.60.2
     public-port       12346
     private-ip        176.16.60.2
     private-port      12346
     public-ip         176:16:60:0:250:56ff:fea5:580a
     public-port       12346
     private-ip        176:16:60:0:250:56ff:fea5:580a
     private-port      12346
     bfd-status        up
     domain-id         not set
     site-id           600
     overlay-id        not set
     preference        1000
     tag               not set
     stale             not set
     weight            1
     version           3
    gen-id             0x8000022f
     carrier           default
     restrict          1
     on-demand          1
     groups            [ 0 ]
     bandwidth         0
     bandwidth-dmin    0
     bandwidth-down    0
     bandwidth-dmax    0
     adapt-qos-period  0
     adapt-qos-up      0
     qos-group         default-group
     border             not set
     extended-ipsec-anti-replay  1
     unknown-attr-len  not set
.
.
.
Device#
```

CHAPTER 8

Troubleshooting Cisco Catalyst SD-WAN Forwarding and QoS Configuration

Support Articles

The documents in this section were created using specific software and hardware listed in the Components Used section of each article. However, this does not mean that they are limited to what is listed in Components Used, and generally remain relevant for later versions of software and hardware. Note that there could be some changes in the software or hardware that can cause commands to stop working, the syntax to change, or GUIs and CLIs to look different from one release to another.

The following are the support articles associated with this technology:

Document	Description
Configure and Verify QoS in SD-WAN Routers	This document describes a step-by-step guide on how to configure and verify QoS Forwarding on SD-WAN routers using Cisco SD-WAN Manager.
Configuring Per-Tunnel QoS from vManage	This video demonstrates how to configure and verify Per-Tunnel QoS via Templates from the Cisco SD-WAN Manager.
QoS Configuration Using vManage GU	This is video provides the steps how to configure QoS using Cisco SD-WAN Manager.