



Forwarding and QoS



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.

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

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

- [Cisco Catalyst SD-WAN Forwarding and QoS Overview, on page 1](#)
- [Traffic Behavior With and Without QoS, on page 2](#)
- [How QoS Works, on page 4](#)
- [Workflow to Configure QoS Using Cisco SD-WAN Manager, on page 5](#)
- [Forwarding and QoS Configuration Using the CLI, on page 10](#)
- [Reference: Forwarding and QoS CLI Commands, on page 11](#)

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 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.

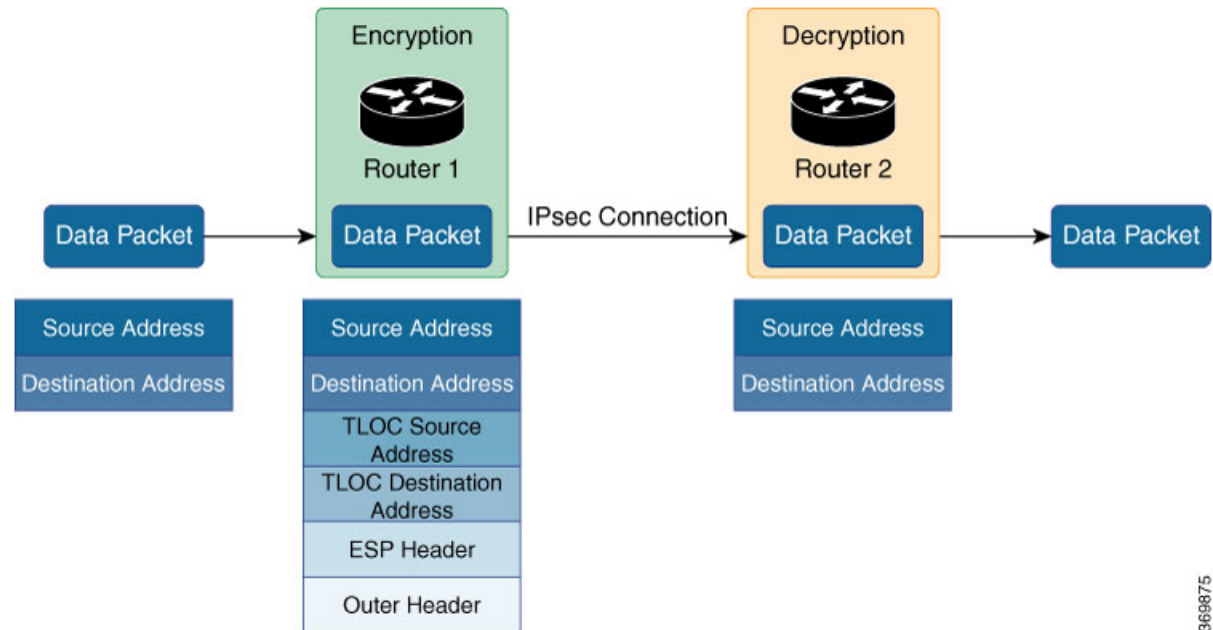


Let's follow the process that occurs when a data packet is transmitted from one site to another when no data policy of any type is configured:

- 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

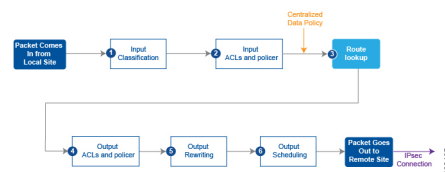


369875

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.	
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.

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**.

- 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

- From the Cisco SD-WAN Manager menu, choose **Configuration > Policies**.
- Click **Localized Policy**.
- 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:
 - Click **Add Policy**.
 - In the Add Policy page, continue to click **Next** till you navigate to Policy Overview page.
 - In the Policy Overview page, enter **Policy Name** and **Description** for your localized policy.
- 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

- Click **Forwarding Class/QoS**. When you navigate to the Forwarding Classes/QoS page, QoS Map is selected by default.
- Click **Add QoS Map**, and then click **Create New**.
- Enter the name and description for the QoS mapping.
- Queue 0 has already been defined by default and cannot be modified. Click the **Add Queue**.
- Select a required queue from the **Queue** drop-down.
- 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

Class	Priority	DSCP	Layer 2 Class of Service
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 you 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 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.

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.

Create Access Lists to Classify Data Packets

Apply Access Lists

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.

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
```

