Default AAR and QoS Policies

Table 1: Feature History

Feature Name	Release Information	Description
Configure Default AAR and QoS Policies	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature enables you to efficiently configure default application-aware routing (AAR), data, and quality of service (QoS) policies for Cisco IOS XE Catalyst SD-WAN devices. The feature provides a step-by-step workflow for categorizing the business relevance, path preference, and other parameters for network applications, and applying those preferences as traffic policy.

Information About Default AAR and QoS Policies

It is often helpful to create an AAR policy, a data policy, and a QoS policy for devices in a network. These policies route and prioritize traffic for best performance. When creating these policies, it is helpful to distinguish among the applications producing network traffic, based on the likely business relevance of the applications, and to give higher priority to business-relevant applications.

Cisco SD-WAN Manager provides an efficient workflow to help you create a default set of AAR, data, and QoS policies to apply to devices in the network. The workflow presents a set of more than 1000 applications that can be identified by network-based application recognition (NBAR), an application recognition technology built into Cisco IOS XE Catalyst SD-WAN devices. The workflow groups the applications into one of three business-relevance categories:

- Business-relevant: Likely to be important for business operations, for example, Webex software.
- Business-irrelevant: Unlikely to be important for business operations, for example, gaming software.

- Default: No determination of relevance to business operations.

Within each of the business-relevance categories, the workflow groups the applications into application lists, such as broadcast video, multimedia conferencing, VoIP telephony, and so on.

Using the workflow, you can accept the predefined categorization of each application's business relevance or you can customize the categorization of specific applications by moving them from one of the business-relevance categories to another. For example, if, by default, the workflow predefines a specific application as business-irrelevant, but that application is important for your business operations, then you can recategorize the application as Business-relevant.

The workflow provides a step-by-step procedure for configuring the business relevance, path preference, and service level agreement (SLA) category.

After you complete the workflow, Cisco SD-WAN Manager produces a default set of the following:

- AAR policy
- QoS policy
- Data policy

After you attach these policies to a centralized policy, you can apply these default policies to Cisco IOS XE Catalyst SD-WAN devices in the network.

Background Information About NBAR

NBAR is an application recognition technology included in Cisco IOS XE Catalyst SD-WAN devices. NBAR uses a set of application definitions called protocols to identify and categorize traffic. One method that NBAR uses to recognize traffic is DNS Snooping. For NBAR to correctly categorize certain types of traffic, the unencrypted DNS traffic must pass through the router. One of the categories that it assigns to traffic is the business-relevance attribute. The values of this attribute are Business-relevant, Business-irrelevant, and Default. In developing protocols to identify applications, Cisco estimates whether an application is likely to be important for typical business operations, and assigns a business-relevance value to the application. The default AAR and QoS policy feature uses the business-relevance categorization provided by NBAR.

Benefits of Default AAR and QoS Policies

- Manage and customize bandwidth allocations.
- Prioritize applications based on their relevance to your business.

Prerequisites for Default AAR and QoS Policies

- Knowledge about the relevant applications.
- Familiarity with the SLAs and QoS markings to prioritize traffic.

Restrictions for Default AAR and QoS Policies

- When you customize a business-relevant application group, you cannot move all the applications from that group to another section. Application groups of business-relevant section need to have at least one application in them.
- Default AAR and QoS policies do not support IPv6 addressing.

Supported Devices for Default AAR and QoS Policies

- Cisco 1000 Series Integrated Services Routers (ISR1100-4G and ISR1100-6G)
- Cisco 4000 Series Integrated Services Routers (ISR44xx)
- Cisco Catalyst 8000V Edge Software
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8500 Series Edge Platforms
- Cisco C1100 Series Integrated Services Router

Use Cases for Default AAR and QoS Policies

If you are setting up a Cisco Catalyst SD-WAN network and want to apply an AAR and a QoS policy to all the devices in a network, use this feature to create and deploy these policies quickly.

Configure Default AAR and QoS Policies Using Cisco SD-WAN Manager

Follow these steps to configure default AAR, data, and QoS policies using Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Add Default AAR & QoS**.

   The **Process Overview** page is displayed.
3. Click **Next**.

   The **Recommended Settings based on your selection** page is displayed.
4. Based on the requirements of your network, move the applications between the **Business Relevant**, **Default**, and **Business Irrelevant** groups.

Note When customizing the categorization of applications as Business-relevant, Business-irrelevant, or Default, you can only move individual applications from one category to another. You cannot move an entire group from one category to another.

5. Click **Next**.

   On the **Path Preferences (optional)** page, choose the **Preferred** and **Preferred Backup** transports for each traffic class.

6. Click **Next**.

   The **App Route Policy Service Level Agreement (SLA) Class** page is displayed.

   This page shows the default settings for **Loss**, **Latency**, and **Jitter** values for each traffic class. If necessary, customize **Loss**, **Latency**, and **Jitter** values for each traffic class.

7. Click **Next**.

   The **Enterprise to Service Provider Class Mapping** page is displayed.

   a. Select a service provider class option, based on how you want to customize bandwidth for different queues. For further detials on QoS queues, refer to the section **Mapping of Application Lists to Queues**

   b. If necessary, customize the bandwidth percentage values for each queues.

8. Click **Next**.

   The **Define prefixes for the default policies and applications lists** page is displayed.

   For each policy, enter a prefix name and description.

9. Click **Next**.

   The **Summary** page is displayed. On this page, you can view the details for each configuration.

   You can click **Edit** to edit the options that appeared earlier in the workflow. Clicking edit returns you to the relevant page.

10. Click **Configure**.

    Cisco SD-WAN Manager creates the AAR, data, and QoS policies and indicates when the process is complete.

    The following table describes the workflow steps or actions and their respective effects:

Table 2: Workflow Steps and Effects

Workflow Step	Affects the Following
Recommended Settings based on your selection	AAR and data policies
Path Preferences (optional)	AAR policies

Workflow Step	Affects the Following
App Route Policy Service Level Agreement (SLA) Class: • Loss • Latency • Jitter	AAR policies
Enterprise to Service Provider Class Mapping	Data and QoS policies
Define prefixes for the default policies and applications	AAR, data, QoS policies, forwarding classes, application lists, SLA class lists

11. To view the policy, click **View Your Created Policy**.

Note To apply the default AAR and QoS policies to the devices in the network, create a centralized policy that attaches the AAR and data policies to the required site lists. To apply the QoS policy to the Cisco IOS XE Catalyst SD-WAN devices, attach it to a localized policy through device templates.

Mapping of Application Lists to Queues

The following lists show each service provider class option, the queues in each option, and the application lists included in each queue. The application lists are named here as they appear on the Path Preferences page in this workflow.

4 QoS class

- Voice
  - Internetwork control
  - VoIP telephony
- Mission critical
  - Broadcast video
  - Multimedia conferencing
  - Real-Time interactive
  - Multimedia streaming
- Business data
  - Signaling
  - Transactional data
  - Network management
  - Bulk data

- Default
  - Best effort
  - Scavenger

5 QoS class

- Voice
  - Internetwork control
  - VoIP telephony
- Mission critical
  - Broadcast video
  - Multimedia conferencing
  - Real-Time interactive
  - Multimedia streaming
- Business data
  - Signaling
  - Transactional data
  - Network management
  - Bulk data
- General data
  - Scavenger
- Default
  - Best effort

6 QoS class

- Voice
  - Internetwork control
  - VoIP telephony
- Video
  - Broadcast video
  - Multimedia conferencing
  - Real-Time interactive
- Mission Critical

- Multimedia streaming

- Business data
  - Signaling
  - Transactional data
  - Network management
  - Bulk data

- General data
  - Scavenger

- Default
  - Best effort

8 QoS class

- Voice
  - VoIP telephony

- Net-ctrl-mgmt
  - Internetwork control

- Interactive video
  - Multimedia conferencing
  - Real-Time interactive

- Streaming video
  - Broadcast video
  - Multimedia streaming

- Call signaling
  - Signaling

- Critical data
  - Transactional data
  - Network management
  - Bulk data

- Scavengers
  - Scavenger

- Default
  - Best effort

Monitor Default AAR and QoS Policies

Monitor Default AAR Policies

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Custom Options**.
3. Choose **Traffic Policy** from **Centralized Policy**.
4. Click **Application Aware Routing**.

   A list of AAR policies is displayed.
5. Click **Traffic Data**.

   A list of traffic data policies is displayed.

Monitor QoS Policies

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Custom Options**.
3. Choose **Forwarding Class/QoS** from **Localized Policy**.
4. Click **QoS Map**.

   A list of QoS policies is displayed.

Note To verify QoS polices, refer to Verify QoS Policy.