Default AAR and QoS policies

This reference provides information about the default application-aware routing (AAR) and quality of service (QoS) policies, including their development milestones, release information, and feature description.

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 the edge 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. You can configure Default AAR and QoS policies.

Default AAR and QoS policies

A default AAR and QoS policy is a network traffic management policy that

- uses Network-Based Application Recognition (NBAR) to identify and categorize more than 1,000 applications
- groups applications into three business-relevance categories (business-relevant, business-irrelevant, and default), and
- prioritizes traffic based on the business relevance of applications.

Business-relevance categories for applications

The workflow presents a set of more than 1,000 applications that can be identified by NBAR, an application recognition technology built into edge 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 edge devices in the network.

NBAR application recognition example

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.

Default AAR and QoS policies

A default AAR and QoS policy is a network management feature that

- enables management and customization of bandwidth allocations
- allows prioritization of applications based on their relevance to business operations, and
- supports flexible configuration to meet organizational requirements.

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

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

This reference identifies the Cisco hardware and software platforms that support default AAR and QoS policies.

The following Cisco devices are compatible with 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

Default AAR and QoS policy use cases

A default AAR and QoS policy use case is a deployment scenario that

- enables quick creation and deployment of consistent AAR and QoS policies
- applies these policies across all devices in a network, and
- supports efficient setup of a Cisco Catalyst SD-WAN network.

Configure default AAR and QoS policies using Cisco SD-WAN Manager

This task enables you to configure default Application-Aware Routing (AAR) and Quality of Service (QoS) policies using Cisco SD-WAN Manager. It guides you through defining application groups, path preferences, SLA classes, and bandwidth mappings to optimize network performance and traffic management.

Use this task when you need to implement or modify default AAR and QoS policies in your Cisco SD-WAN environment. This workflow is relevant for administrators who want to ensure optimal application performance and bandwidth allocation across the network using Cisco SD-WAN Manager.

Before you begin

Ensure you have access to Cisco SD-WAN Manager and the necessary permissions to configure policies.

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

Procedure

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

The **Process Overview** page is displayed.

Step 2 Click **Next**. Based on the requirements of your network, move the applications between the **Business Relevant**, **Default**, and **Business Irrelevant** groups.

The **Recommended Settings based on your selection** page is displayed.

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.

Step 3 Click **Next**.

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

Step 4 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.

Step 5 Click **Next**.

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

Select a service provider class option, based on how you want to customize bandwidth for different queues. For further details on QoS queues, refer to the section **Mapping of Application Lists to Queues**. If necessary, customize the bandwidth percentage values for each queue.

Step 6 Click **Next**.

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

For each policy, enter a prefix name and description.

Step 7 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.

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
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

Step 8 Click **Configure**.

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

Step 9 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 edge devices, attach it to a localized policy through device templates.

After completing this workflow, default AAR, data, and QoS policies are created and applied as configured. You can view and edit the policies as needed, and the network will use the defined application groups, path preferences, SLA classes, and bandwidth mappings for optimized traffic management.

What to do next

For details on mapping application lists to queues, refer to the following information.

- 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

This task allows you to monitor and verify the status of default Application Aware Routing (AAR) and Quality of Service (QoS) policies in Cisco SD-WAN Manager.

- Ensures visibility into created AAR, traffic data, and QoS policies.
- Supports validation of policy deployment and effectiveness.

Use this task when you need to check the operational status or configuration of default AAR and QoS policies within Cisco SD-WAN Manager.

Monitoring these policies is essential for maintaining optimal network performance and ensuring that traffic management rules are correctly applied.

- Applicable after policy creation or modification.
- Useful for troubleshooting or routine verification of policy status.

Before you begin

Access to Cisco SD-WAN Manager is required.

- Ensure you have appropriate permissions to view configuration and policy menus.

Follow these steps to monitor default AAR and QoS policies:

Procedure

Step 1 Monitor default AAR policies in Cisco SD-WAN Manager.

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

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

  A list of traffic data policies is displayed.

Step 2 Monitor QoS policies in Cisco SD-WAN Manager.

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

  A list of QoS policies is displayed.

After completing these steps, you will be able to view lists of default AAR, traffic data, and QoS policies in Cisco SD-WAN Manager. You can confirm their status and verify that the policies are correctly deployed and operational.

What to do next

For further verification or troubleshooting, consult the referenced documentation or review policy logs as needed.

- Refer to external resources for advanced policy validation.