



CHAPTER 6

Provisioning: Working with Macros

QPM provides you with Macros to define certain values and features that will be used while working with policies. The following topics describe the macros used in QPM:

- [Working with Aliases, page 6-1](#)
- [Working with Policy Templates, page 6-5](#)
- [Working with NBAR Custom Mappings, page 6-13](#)
- [Working with Time-Based ACL, page 6-16](#)
- [Working with Policy Maps, page 6-18](#)

Working with Aliases

Definitions of IP aliases, and application aliases, can be stored in QPM libraries, and used in policy definitions across all your policy groups. When you change the alias definition, all policies that reference the definition are affected.

When you deploy historical jobs with referenced alias definitions, QPM performs a validation check on the referenced definitions. See [Chapter 9, “Provisioning: Deploying QoS Policies”](#).

The following topics describe how to work with alias definitions:

- [Defining IP Aliases, page 6-2](#)
- [Defining Application Aliases, page 6-3](#)

- [Modifying Aliases, page 6-3](#)
- [Deleting Aliases, page 6-4](#)

Defining IP Aliases

An IP alias is an alias for a named group of IP addresses (including masks) or host names. It can be used for both source IP and destination IP conditions within a filter. IP aliases are stored in the IP Aliases library.

To define IP alias:

Step 1 Select **Provision > Macros > IP Aliases**.

The IP Aliases page appears, displaying IP alias definitions in the IP Alias library.

Step 2 Click **Create**. The IP Alias dialog box opens.

Step 3 Enter the IP alias name in the Name field.

Step 4 For each IP address you want to add to the alias:

- a. Enter the IP address and mask, or enter host name.
- b. Click **Add** to add the IP address to the alias. The IP address and mask are displayed in the Alias list.

To remove an IP address that you added, select the IP address in the list, and click **Remove**.

For more details, see [IP Alias Editor Dialog Box, page B-2](#).

Step 5 After you have added all the IP addresses to the alias, click **OK**.

The IP Alias page displays the new alias.

Related Topics

- [Modifying Aliases, page 6-3](#)
- [Deleting Aliases, page 6-4](#)

Defining Application Aliases

An application alias is an alias for a defined protocol and port (or group of ports). It can be used in a filter definition for source and destination application conditions. Application aliases are stored in the Application Aliases library.

To define application alias:

Step 1 Select **Provision > Macros > Application Aliases**.

The Application Aliases page appears displaying application alias definitions in the Applications library.

Step 2 Click **Create**.

The Application Alias dialog box opens.

Step 3 Enter the Application alias name in the Name field.

Step 4 Define the protocol, and TCP/UDP port or range, if appropriate.

For more details, see [Application Alias Editor Dialog Box, page B-4](#).

Step 5 Click **OK**.

The Applications page reappears displaying the application alias.

Related Topics

- [Modifying Aliases, page 6-3](#)
- [Deleting Aliases, page 6-4](#)

Modifying Aliases

You can change IP aliases and application aliases. When you modify an alias, all policies that reference it, are modified.

To modify aliases:

Step 1 Select **Provision > Macros**.

Step 2 In the Device Macros TOC, select the library that contains the alias you want to modify.

Step 3 Select the check box next to the alias you want to modify, and click **Edit**.
The Alias dialog box opens, displaying details for the alias.

Step 4 Modify fields as required.

For more details, see:

- [IP Alias Editor Dialog Box, page B-2](#)
- [Application Alias Editor Dialog Box, page B-4](#)

Step 5 Click **OK** in the dialog box. The Alias page displays the modified alias.

Related Topics

- [Defining IP Aliases, page 6-2](#)
- [Defining Application Aliases, page 6-3](#)

Deleting Aliases

You can delete aliases if they are not currently being used in policies.

To delete aliases:

Step 1 Select **Provision > Macros**.

Step 2 In the Device Macros TOC, select the library that contains the aliases you want to delete.

Step 3 Select the check boxes next to the aliases you want to delete.

Step 4 Click **Delete**.

Working with Policy Templates

Policy templates contain QoS properties and traffic rules, but do not contain network element assignments. Policy templates can be used to create policies in any policy group. You can create global policy templates and store them in the Policy Templates library.

The following topics describe how to work with policy group templates:

- [Understanding Policy Templates, page 6-5](#)
- [Creating a Policy Template, page 6-6](#)
- [Viewing Policy Template Information, page 6-7](#)
- [Modifying a Policy Template, page 6-8](#)
- [Disconnecting Policies from Policy Templates, page 6-11](#)
- [Deleting Policy Templates, page 6-13](#)

Understanding Policy Templates

Policy templates can be used to create and share policies across policy groups and device groups. A policy template contains a set of QoS properties and QoS traffic rules for specified device constraints. It does not include any device assignments. Policy templates are stored in the Policy Templates library.

You can create policies by copying policy templates, or by attaching the policy template to the policy.

When a policy template is attached to policies, any change in the policy template will affect the attached policies. You can disconnect policies from their attached policy template at any time.

QPM generates voice policy templates, which are used to create voice policies for IP telephony QoS configuration. You can edit the voice policy templates created by QPM.

Related Topics

- [Creating a Policy Template, page 6-6](#)
- [Modifying a Policy Template, page 6-8](#)
- [Viewing Policy Template Information, page 6-7](#)

- [Disconnecting Policies from Policy Templates, page 6-11](#)
- [Deleting Policy Templates, page 6-13](#)
- [Chapter 7, “Provisioning: Configuring QoS for IP Telephony”](#)

Creating a Policy Template

Create a policy template when you want to share policies across policy groups or device groups.

You create a new policy template in the same way as you create a new policy using the Policy Definition wizard. You can create a new template by copying another template or a policy.

To create a policy template:

-
- Step 1** Create a new policy template and define its device constraints. See [Creating a Policy, page 8-5](#).
 - Step 2** Define the policy template’s QoS properties and mappings. See [Defining QoS Properties and Mappings, page 8-9](#).
 - Step 3** Define traffic rules for the policy template. See [Creating a Traffic Rule, page 8-28](#).
-

Related Topics

- [Viewing Policy Template Information, page 6-7](#)
- [Modifying a Policy Template, page 6-8](#)
- [Deleting Policy Templates, page 6-13](#)

Viewing Policy Template Information

You can view information about the QoS properties and traffic rules for a specific policy template. You can then modify the policy template as required.

You can also view the policies that are attached to a policy template, and you can then disconnect a policy from its template.

To view a policy template information:

Step 1 Select **Provision > Macros > Policy Templates**.

The Templates page appears displaying the global policy templates.

Step 2 To open policy template information pages from the Templates page, do any of the following:

- Click the required template name.

The General page appears, displaying general definitions for the selected policy template.

- Click the number of QoS properties for the required policy template.

The QoS Properties page appears, displaying the QoS properties and mappings for the selected policy template.

- Click the number of In Traffic Rules for the required policy template.

The In Policies page appears, displaying the inbound traffic rules for the selected policy template.

- Click the number of Out Traffic Rules for the required policy template.

The Out Traffic Rules page appears, displaying the outbound traffic rules for the selected policy template.

After you have opened a policy template information page, the TOC changes to the Template TOC.

Step 3 Open any policy template information page from the Template TOC.

In addition to the pages referred to in the previous step, you can also open the Device Constraints page, which displays device constraint definitions for the selected policy template.

You can modify policy template details from these information pages.

Step 4 To view a template's attached policies, click the number of attached policies for the required policy template.

The Attached Policies page appears, displaying the list of attached policies.

You can disconnect a policy from its template in this page.

Related Topics

- [Modifying a Policy Template, page 6-8](#)
- [Deleting Policy Templates, page 6-13](#)
- [Disconnecting Policies from Policy Templates, page 6-11](#)

Modifying a Policy Template

Modify a policy template when you want to modify:

- General definitions
- Device constraint definitions:
 - After you define the first device constraint in a policy template, you cannot change the network element type definition. All constraints in a policy template must be for the same network element type. If you want to change the network element type, you must create a new policy.
 - A policy template must contain at least one constraint definition. You cannot delete a constraint definition if it is the only constraint definition for the policy template.
- QoS properties and mappings—See [Defining QoS Properties and Mappings, page 8-9](#).
- QoS traffic rules—You can add, remove, and edit traffic rules. See [Working with Traffic Rules, page 8-25](#).



Note

If a policy template is attached to policies, any change in the policy template will affect the attached policies. For information on disconnecting a policy from its attached template, see [Disconnecting Policies from Policy Templates, page 6-11](#).

This topic describes how to change a policy template's general definitions, and device constraint definitions.

To modify a policy template:

Step 1 Select **Provision > Macros > Policy Templates**.

The Templates page appears displaying the global policy templates.

Step 2 To edit the general definitions for the policy template:

a. Open the Policy Definition wizard in one of the following ways:

- Select the required policy template, and click **Edit**.
- If you want to view general information first, click the required policy template name. The General page appears for the selected template. The TOC changes to the Template TOC. Click **Edit** in the General page.

The Policy Definition wizard opens, displaying the General Definition page.

b. Edit the name and description in the General Definition page, as required.

To add, edit, or remove device constraint definitions, open the Device Constraints page in the Policy Definition wizard in one of the following ways:

- If the Policy Definition wizard is open, continue to the Device Constraints Definition page.
- Select Device Constraints in the Policy Group TOC.

The Device Constraints page appears. Click **Edit**. The Policy Definition wizard opens, displaying the Device Constraint Definition page.

Modify device constraint definitions as required:

- To edit an existing constraint:
 - Select the constraint definition, and click **Edit**.

The Device Definitions page appears.

- Edit the device constraints. For more information about the fields in this page, see [Policy Definition Wizard: Constraints Definition Page, page B-83](#).

You cannot change the network element type after it has been defined for the first device constraint in the policy.

- Click **OK**.

The Device Constraints page reappears displaying the modified device constraint.

- To delete an existing constraint definition, select the constraint definition, and click **Delete**.

A policy must contain at least one constraint definition. You cannot delete a constraint definition if it is the only constraint definition for the policy.

- To create a new constraint manually:

- Click **Define Manually**.

The Device Definitions page appears.

- Define the device constraints. For more information about the fields in this page, see [Policy Definition Wizard: Constraints Definition Page, page B-83](#).

You cannot change the network element type after it has been defined for the first device constraint in the policy.

- Click **OK**.

The Device Constraints page reappears displaying the new device constraint.

- To define a new constraint from network elements:

- Click **Define from Inventory**.

- Select the type and model of network element to use to define the device constraint. Click **OK**.

You cannot change the network element type after it has been defined for the first device constraint in the policy.

- Select the network elements you want to use to define the device constraints. For more information about the fields in this page, see [Policy Definition Wizard: Constraints Definition Page, page B-83](#).

- Click **Define Constraint**.

The Device Constraints page reappears displaying the new device constraint.

- Step 3** After you have completed modifying your policy template definitions, click **Finish** to exit the Policy Definition wizard.
-

Related Topics

- [Viewing Policy Template Information, page 6-7](#)
- [Deleting Policy Templates, page 6-13](#)
- [Modifying a Policy, page 8-21](#)

Disconnecting Policies from Policy Templates

You can disconnect an individual policy from its template, and you can disconnect several policies from a policy template.

The following topics describe how to disconnect policies from templates:

- [Disconnecting an Individual Policy from its Template, page 6-11](#)
- [Disconnecting Several Policies from a Template, page 6-12](#)

Disconnecting an Individual Policy from its Template

This topic describes how to disconnect an individual policy from its policy template.

To disconnect an individual policy from its template:

- Step 1** Select **Provision > Policy Creation > Policy Table**.

The Policy Table page appears displaying the policies for the current policy group.

- Step 2** Click the policy name, or select the required policy and click **Edit**.
The General page appears for the selected policy. The TOC changes to the Policy TOC.
- Step 3** In the Attached to Template field, click **Disconnect**.
-

Related Topics

- [Disconnecting Several Policies from a Template, page 6-12](#)
- [Modifying a Policy Template, page 6-8](#)
- [Deleting Policy Templates, page 6-13](#)

Disconnecting Several Policies from a Template

This topic describes how to disconnect one or more policies from the Policy Templates page.

To disconnect a number of policies from the template:

- Step 1** Select **Provision > Macros > Policy Templates**.
The Templates page appears displaying the global policy templates.
- Step 2** To view a template's attached policies, click the number of attached policies for the required policy template.
The Attached Policies page appears, displaying the list of attached policies.
- Step 3** Select the policy to disconnect, and click **Disconnect**.
-

Related Topics

- [Disconnecting an Individual Policy from its Template, page 6-11](#)
- [Modifying a Policy Template, page 6-8](#)
- [Deleting Policy Templates, page 6-13](#)

Deleting Policy Templates

You can delete policy templates that are not attached to any policies.

To delete policy templates:

-
- Step 1** Select **Provision > Macros > Policy Templates**.
- The Templates page appears.
- Step 2** Select the check boxes next to the template or templates you want to delete.
- Step 3** Click **Delete**.
-

Related Topics

- [Disconnecting Policies from Policy Templates, page 6-11](#)

Working with NBAR Custom Mappings

Network-Based Application Recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications.

When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate quality of service (QoS) for that application or traffic with that protocol

NBAR supports the use of custom protocols to identify custom applications. Custom protocols support static port-based protocols and applications that NBAR does not currently support. With NBAR supporting the use of custom protocols, NBAR can map static TCP and UDP port numbers to the custom protocols.

The following are the features related to custom protocols with NBAR support:

- Allows you to inspect the payload for certain matching string patterns at a specific offset.
- Allows you to define the names of their custom protocol applications. The user-named protocol can then be used by Protocol Discovery, the Protocol Discovery MIB, the match protocol command, and the ip nbar custom command as an NBAR-supported protocol.

- Allows NBAR to inspect custom protocols specified by traffic direction (that is, traffic heading toward a source or destination rather than traffic in both directions) if desired by the user.
- CLI support that allows a user who is configuring a custom application to specify a range of ports rather than specifying each port individually.

Examples of the QoS features that can be applied to the network traffic (using the MQC) after NBAR has recognized and classified the application or protocol include the following:

- Class-Based Marking
- Class-Based Weighted Fair Queuing (CBWFQ)
- Low Latency Queuing (LLQ)
- Traffic Policing
- Traffic Shaping

NBAR Custom Mappings are used while defining the Filter properties for In/Out Traffic Rules of a policy. They can also be used while defining the Filter properties for Class Maps under a Policy Map.

Related Topics

- [Creating NBAR Custom Mappings, page 6-14](#)
- [Modifying NBAR Custom Mappings, page 6-15](#)
- [Deleting NBAR Custom Mappings, page 6-16](#)

Creating NBAR Custom Mappings

To create an NBAR Custom Mapping in QPM:

Step 1 Choose **Provision > Macros > NBAR Custom Mappings**.

The NBAR Custom Mappings page opens.

Step 2 Click **Create**.

The NBAR Custom Mapping Editor dialog box opens.

- Step 3** Enter values for name, byte location, and ports in the corresponding fields.
- Step 4** Select the format, direction, and protocol from the corresponding drop-down lists.
-

Related Topics

- [NBAR Custom Mapping Editor Dialog Box, page B-11](#)
- [Working with NBAR Custom Mappings, page 6-13](#)
- [Modifying NBAR Custom Mappings, page 6-15](#)

Modifying NBAR Custom Mappings

You can modify the properties of the NBAR Custom Mappings you already created.

To modify NBAR Custom Mappings:

- Step 1** In the NBAR Custom Mappings page, select the NBAR mapping you want to modify, and click **Edit**.
- The NBAR Custom Mapping Editor dialog box opens.
- Step 2** Edit the properties of the mapping as required.
- You cannot modify the name of an NBAR Custom Mapping you already created. Therefore the Name field in the dialog box is not editable.

Related Topics

- [NBAR Custom Mapping Editor Dialog Box, page B-11](#)
- [Working with NBAR Custom Mappings, page 6-13](#)
- [Creating NBAR Custom Mappings, page 6-14](#)

Deleting NBAR Custom Mappings

You can delete the NBAR Custom Mappings that you do not want to use while defining the filter properties for Traffic Rules or Class Maps.

**Note**

Before deleting any NBAR custom mapping, make sure that it is not being used in any In/Out Traffic Rules or Class Maps.

To delete the NBAR Custom Mappings:

-
- Step 1** In the NBAR Custom Mappings page, select the NBAR mappings you want to delete.
- Step 2** Click **Delete**.
- The selected NBAR mappings will be deleted.
-

Related Topics

- [Working with NBAR Custom Mappings, page 6-13](#)

Working with Time-Based ACL

QPM provides you with time based ACL that allows access control based on time, for the configured policies. You create a time range that defines specific times of the day and week in order to implement time-based ACLs.

The time range is identified by a name and then referenced by a function. Therefore, the time restrictions are imposed on the function itself.

Time-based ACLs provide enhanced control over permitting or denying the access to resources for a user. They also enhance policy-based routing (PBR) and queuing functions.

For example, when the provider's access rates vary by time of day, it is possible to automatically and cost effectively reroute traffic. Service providers can dynamically change a committed access rate (CAR) configuration to support the QoS service level agreements (SLAs) that are negotiated for certain times of day.

To configure time-based QoS service policies, QPM uses time-based ACLs as the match-on criteria for a class of traffic. You can create both absolute and periodic time ranges. These time ranges are later referenced by the In/Out Traffic Rules of a policy.

Related Topics

- [Creating Time Ranges for Time-based ACL, page 6-17](#)

Creating Time Ranges for Time-based ACL

To create time ranges for defining time-based ACLs in QPM:

-
- Step 1** Choose **Provision > Macros > Time Based ACL**.
The Time Based ACL page opens.
- Step 2** Click **Create**.
The Time Based ACL dialog box opens.
- Step 3** Enter the time range name, and define the parameters for either one absolute statement or multiple periodic statements, for that time range name.
-

The time range relies on the system's software clock. For the time range feature to work the way you intend, you need a reliable clock source. Cisco Systems recommends that you use Network Time Protocol (NTP) to synchronize the system's software clock.

Related Topics

- [Time Based ACL Dialog Box, page B-14](#)

Working with Policy Maps

QPM provides you with Policy Maps that are based on the hierarchical QoS feature. Policy Maps enable the creation of nested policies, so that you can create multiple levels of policies and attach the same to child policies, which in turn can be attached to the interface.

This feature of QPM helps the users who want to segregate traffic based on flow source or destination, and apply different policing or shaping rules to each class of traffic.

The Policy Map helps you to configure a traffic policy and associate the traffic policy with Class Maps, which contain one or more QoS features. You later attach this Policy Map to an In Traffic Rule or Out Traffic Rule of another policy, using the Service Policy feature.

Related Topics

- [Creating Policy Maps, page 6-18](#)

Creating Policy Maps

To create Policy Maps in QPM:

Step 1 Choose **Provision > Macros > Policy Maps**.

The Policy Maps page opens.

Step 2 Click **Create**.

The Policy Map Definition page opens.

Step 3 Enter the name and description of the new Policy Map in the corresponding fields.

Step 4 Click **Next**.

The Class Definitions for the Policy Map - *new Policy Map* page opens, where *new Policy Map* is the name of the policy map you just created. You can create Class Maps for the Policy map, in this page.

Related Topics:

- [Creating Class Maps, page 6-19](#)
- [Modifying a Policy Map, page 6-29](#)

Creating Class Maps

After you have created a Policy Map by entering the name and description, you should create Class Maps for the Policy Map. The Class Maps contain Filters and Actions, similar to Traffic Rules.

To create Class Maps:

-
- Step 1** In the Class Definitions for the Policy Map - *new Policy Map* page, click **Create**. The Class Map Definition Wizard opens, displaying the first page – General.
- Step 2** In the Class Map Definition Wizard - General page:
- Enter the Class Map name.
 - Enter a description for the Class Map, if desired.
 - Select the type of Class Map you want to create—QoS Class Map, or access control Class Map.
 - Click **Next** to proceed to the Filter step in the wizard. See
-

Related Topics

- [Working with Policy Maps, page 6-18](#)
- [Defining a Class Map Filter, page 6-20](#)
- [Defining QoS Class Map Actions, page 6-23](#)

Defining a Class Map Filter

Define a filter to specify the traffic to which the Class Map should be applied. A filter can contain multiple *filter rules*. Each filter rule is a set of *filter conditions*—to satisfy the filter rule, a packet must satisfy *all* conditions of the filter rule.

To match the filter, a packet must satisfy *any* one of the filter rules.

The available filter elements change according to the policy's device constraints and congestion management properties. Typically, you can identify the traffic by any of the following characteristics:

- Source IP or destination IP. You can use IP aliases from the QPM component libraries.
- Source application or destination application. You can use application aliases from the QPM component libraries.
- Service—IP precedence or DSCP value.

In addition, you might be able to filter using:

- Network Based Application Recognition (NBAR) properties—NBAR is a classification engine that recognizes a wide variety of applications, including web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments.

When an application is recognized and classified by NBAR, a network can invoke services for that specific application.

- IP RTP ports
- CoS value
- MPLS value
- Single ACL Translation—You can define a complex permit or deny filter as a single ACL. This is helpful if you are already using a lot of ACLs on the device, because you are limited in the number of ACLs that you can define on a device.
- Traffic compression properties for the class-based RTP and TCP IP header in the traffic.
- Policy Maps—You can create nested policies (which consists of Class Maps) within a Class Map.

- **Time Range**—You can select a time range name that you already created, for defining time-of-the-day QoS policies. This will help you to control traffic based on different timings for different days of the week.

You can also define a class default filter for unclassified traffic that does not match any other filter condition.

If you want to monitor a Class Map, do not define more than 12 match statements in the Class Map filter.

The Class Map Definition Wizard guides you through the process of defining filter conditions and rules for your Class Map.

To define a Class Map filter:

-
- Step 1** Open the Class Map Definition Wizard - Filter page:
- If the Class Map Definition Wizard is not open, open the relevant Class Maps page. Select the Class Map whose filter you want to edit, and click **Edit**.
The Class Map wizard opens, displaying the Class Map Wizard - General page. Click **Next**.
 - If the wizard is open, click **Next** in the Class Map Definition Wizard - General page, or select **Filter** in the wizard navigation TOC.
- Step 2** Enter a name for the filter, if desired.
- The filter name helps you identify the defined filter in the CLI translation.
- Step 3** Select how to define the filter type of the Class Map:
- **Create New Filter**—The Class Map is applied to traffic that matches any of the filter conditions. If you do not define filter rules, the Class Map is applied to all traffic.
 - **Class Default**—The traffic is applied to all traffic that does not match any of the filters. You do not create any filter conditions for this type of Class Map. Go to [Step 9](#).
- Step 4** Define a filter rule:
- a. Click **Create** in the Filter Rules table.
The Rule Setting page appears, displaying the conditions you can define for each filter rule.
 - b. Click **Edit** next to the condition you want to define.
A dialog box opens.

- c. Define the condition as required.

See the following topics for information about these dialog boxes:

- [Source IP / Destination IP Dialog Box, page B-118](#)
- [Application Dialog Box, page B-114](#)
- [Protocol Dialog Box, page B-116](#)
- [CoS Dialog Box, page B-120](#)
- [MPLS Dialog Box, page B-121](#)
- [Service Dialog Box, page B-120](#)
- [IP-RTP Port Range Dialog Box, page B-121](#)
- [Single ACL Translation Editor Dialog Box; Single ACL Translation Conditions Editor Dialog Box, page B-122](#)
- [Time Based ACL Editing Dialog Box, page B-123](#)



Note For IP and application conditions, you can choose a predefined alias. You can also save a defined condition as an alias in the QPM libraries for future use.

- d. Click **OK** in the Condition dialog box.

The Rule Setting table reappears.

- e. Repeat steps **b** through **d** to create additional conditions for the filter rule.
- f. After you have defined all the rules in the filter condition, click **Done**. The Filter page reappears displaying the filter rule you have defined.

Step 5 Repeat [Step 4](#) to create additional filter rules.

Step 6 To edit a filter rule, select the filter rule in the Filter page, and click **Edit**.

The Rule Setting page appears.

Step 7 Edit the rule conditions as required, and click **Done** to return to the Filter page.

Step 8 To delete a filter rule, select the filter rule in the Filter page, and click **Delete**.

- Step 9** After you have completed your filter definitions, click **Next**.
- If you are defining a QoS Class Map, the Class Map Definition Wizard - Actions page appears. See [Defining QoS Class Map Actions, page 6-23](#).
 - If you are defining an access control Class Map, the Summary page appears. See [Viewing the Class Map Summary, page 6-25](#).
-

Related Topics

- [Defining QoS Class Map Actions, page 6-23](#)
- [Working with Aliases, page 6-1](#)

Defining QoS Class Map Actions

The Class Map Actions step of the Class Map Definition wizard includes several substeps to define the actions to be applied to traffic that matches the filter definition:

- **Marking**—Defines a packet's relative importance. The marking can be used to identify and prioritize packets in subsequent policies.
- **Microflow Policing**—Limits the input transmission rate of traffic, and marks packets.
- **Policing**—Limits the rate of aggregate flows on a single interface or across interfaces.
- **Shaping**—Smooths the flow of outbound traffic.
- **Queuing**—Provides bandwidth guarantees and priority servicing for outbound traffic.
- **Traffic Control**—Sets the traffic compression properties for the class-based RTP and TCP IP header
- **Congestion Avoidance**—Discards packets to avoid congestion.
- **Service Policy**—Assign a policy map (which further consists of class maps) to the Class Map

Cisco Express Forwarding (CEF) must be enabled on a device if you want to deploy NBAR or class-based QoS policies. On VIP platforms, distributed CEF (dCEF) must be enabled.

The global CLI command to enable CEF or dCEF is:

ip cef [distributed] switch

The following procedure describes all the available actions in the Class Map Definition Wizard - Actions step.

To define QoS Class Map Actions:

-
- Step 1** Open the Class Map Definition Wizard - Actions page:
- If the Class Map Definition Wizard is not open, follow these steps to open the Actions page:
 - a. Open the relevant Class Maps page. See [Displaying the Traffic Rules Pages, page 8-26](#).
 - b. Select the Class Map whose action you want to edit, and click **Edit**.
The Class Map Definition Wizard opens, displaying the General page.
 - c. Click **Actions** from the TOC
 - If the Class Map Definition Wizard is open, click **Next** in the Class Map Definition Wizard - Filter page.
The Class Map Definition Wizard - Actions page for Marking appears.
- Step 2** Use the Next button to navigate to the action pages you want to define, or select the actions in the wizard navigation TOC:
- See the following topics for information about these dialog boxes:
- [Class Map Definition Wizard: Marking Actions Page, page B-32](#)
 - [Class Map Definition Wizard: Microflow Policing Actions Page, page B-33](#)
 - [Class Map Definition Wizard: Policing Actions Page, page B-35](#)
 - [Class Map Definition Wizard: Shaping Actions Page, page B-39](#)
 - [Class Map Definition Wizard: Queuing Actions Page, page B-40](#)

- [Class Map Definition Wizard: Traffic Control Actions Page, page B-43](#)
- [Class Map Definition Wizard: Congestion Avoidance Actions Page, page B-44](#)
- [Class Map Definition Wizard: Service Policy Actions Page, page B-45](#)

Step 3 After you have completed defining the policy actions, click **Next** to proceed to the Summary step in the wizard. See [Viewing the Class Map Summary, page 6-25](#).

Related Topics

- [Creating Class Maps, page 6-19](#)
- [Defining a Class Map Filter, page 6-20](#)

Viewing the Class Map Summary

After you have finished defining your Class Map, review the Class Map definitions in the Summary page. You can go back and revise definitions before completing the Class Map Definition wizard.

To view the Class Map Summary:

- Step 1** If the Class Map Definition Wizard - Summary page is not displayed, select **Summary** in the wizard navigation TOC.
- Step 2** Review the Class Map definitions.
- Step 3** To modify any of the settings, choose the relevant step in the wizard navigation TOC, or click the Back button.
- Step 4** After you are satisfied with the Class Map summary, click **Finish** to complete the Class Map and exit the wizard.
-

Related Topics

- [Defining a Class Map Filter, page 6-20](#)
- [Defining QoS Class Map Actions, page 6-23](#)

Modifying a Class Map

You can modify a Class Map (in a Policy Map) by changing its name, filter, or actions. When you redeploy the traffic rules that contains this Policy Map, the modified Class Map replaces the old Class Map on the policy's assigned network elements.

To modify a Class Map:

-
- Step 1** In the Class Definition for the Policy Map - *Policy Map name* page, select the check box next to the Class Map you want to edit, and click **Edit**.
- The Class Map Definition Wizard opens, displaying the General page.
- Step 2** Navigate to pages you want to edit using the wizard Next button, or by choosing a step in the wizard navigation TOC:
- To modify the Class Map filter, see [Defining a Class Map Filter, page 6-20](#).
 - To modify the Class Map actions, see [Defining QoS Class Map Actions, page 6-23](#).
- Step 3** After you have finished editing the Class Map click **Finish**. The Class Map Definition Wizard - Summary page appears. See [Viewing the Class Map Summary, page 6-25](#).
-

Related Topics

- [Creating Class Maps, page 6-19](#)

Deleting Class Maps

When you no longer want to use a Class Map, you can delete it from the Policy Map. When you redeploy the traffic rules (in a policy) that contains this Policy Map, the deleted Class Map is removed from the policy's assigned network elements.

Before You Begin

If you are not sure whether you will need a Class Map, consider disabling it instead of deleting it. See [Enabling and Disabling Class Maps, page 6-27](#) for information on disabling a Class Map.

To delete Class Maps:

-
- Step 1** Open the Class Definitions for the Policy Map - *Policy Map name* page for the Policy Map in which you want to delete a Class Map.
- Step 2** Click the check box(es) next to the Class Maps you want to delete, and click **Delete**.
-

Related Topics

- [Modifying a Class Map, page 6-26](#)
- [Enabling and Disabling Class Maps, page 6-27](#)

Enabling and Disabling Class Maps

When you create a Class Map, it is enabled by default, so that when you deploy to the devices, the Class Map is distributed and takes effect. However, you can disable a Class Map, so that it exists in the policy, but is not deployed to the network.

This allows you to define Class Maps before you want to make them effective, or temporarily remove a Class Map from the network without erasing it completely. You can also enable Class Maps that have been disabled.

To enable or disable Class Maps:

-
- Step 1** Open the Class Definitions for the Policy Map - *Policy Map name* page for the Policy Map in which you want to enable or disable a Class Map.
- Step 2** Click the check box(es) next to the Class Map you want to enable or disable.
- Step 3** Click **Enable** or **Disable** as required.
-

Related Topics

- [Deleting Class Maps, page 6-26](#)
- [Changing the Priority of Class Maps, page 6-28](#)

Changing the Priority of Class Maps

The device examines QoS Class Maps in order until a match is found for the packet. Even if a packet satisfies more than one Class Map, it will be treated as satisfying only the first Class Map that the device encounters, unless you define your Class Map to include the Continue setting, in which case a subsequent match will be sought.

Class Maps on an interface are examined top-down according to the QPM display. Therefore the Class Maps in a policy should appear in order of importance, from top to bottom, to ensure that Class Maps get the priority you require.

If you are creating complex Class Map structures that include Continue settings (so that you can set multiple policies on a given packet), ensure that the statements with the Continue setting come before the subsequent Class Map statement you want applied.

Initially, Class Maps are listed in the order in which they are defined. You can change the order of Class Maps in the list.

To change the priority of Class Maps:

-
- Step 1** Open the Class Definitions for the Policy Map - *Policy Map name* page for the Policy Map in which you want to reorder policies.
 - Step 2** Click **Reorder**.
The Reorder dialog box opens.
 - Step 3** Select the Class Map that you want to reorder. Click the Up or Down button to reorder the Class Map as required.
-

Related Topics

- [Enabling and Disabling Class Maps, page 6-27](#)

Modifying a Policy Map

You can modify a Policy Map by changing its Class Maps and the associated filters and actions.

To modify a Policy Map:

-
- Step 1** In the Policy Map page, select the Policy Map you want to modify, and click **Edit**.
The Policy Map Definition page opens.
You cannot modify the name and description of a Policy Map already created. Therefore the Policy Map Name and Policy Map Description fields are not editable in the Policy Map Definition page.
- Step 2** Click **Next**.
The Class Definitions for the Policy Map - *Policy Map name* page opens.
- Step 3** Add, delete, or modify the Class Maps as required.
-

Related Topics

- [Creating Policy Maps, page 6-18](#)
- [Working with Policy Maps, page 6-18](#)

Deleting Policy Maps

You can delete the Policy Maps that you do not want to use in any nested policies.

If you delete a Policy Map that is already referenced by a policy, a warning message appears. Then you should first delete the Policy Map from the policy and then redeploy the policy on the associated network elements.

To delete Policy Maps:

Step 1 Open the Policy Maps page.

Step 2 Select the Policy Maps you want to delete, and click **Delete**.

The Policy Maps along with the attached Class Maps will be deleted.

Related Topics

- [Creating Policy Maps, page 6-18](#)