



## CHAPTER 8

# Provisioning: Working with Policies, Properties, and Traffic Rules

---

A major part of your Quality of Service (QoS) configuration is the definition of policies, QoS properties, and traffic rules. QoS properties define the QoS actions that will be applied to specific data packets. These properties and the associated rules for inbound and outbound traffic are managed within policies, which are applied to a specified set of network elements.

The following topics provide information about creating and managing policies, QoS properties and traffic rules:

- [Working with Policies, page 8-1](#)
- [Working with Traffic Rules, page 8-25](#)
- [More Information on Policy Configuration, page 8-39](#)

### Related Topics

- [Basic Concepts in QPM, page 1-13](#)

## Working with Policies

The following topics describe how to create and work with policies in QPM:

- [Understanding Policies, page 8-2](#)
- [Creating a Policy, page 8-5](#)
- [Defining QoS Properties and Mappings, page 8-9](#)

- [Setting Network Element Assignments, page 8-14](#)
- [Copying Policies, page 8-15](#)
- [Importing Device QoS Configurations to Policies, page 8-17](#)
- [Viewing Policy Information, page 8-19](#)
- [Modifying a Policy, page 8-21](#)
- [Deleting a Policy, page 8-24](#)

**Related Topics**

- [Working with Traffic Rules, page 8-25](#)
- [Working with Policy Templates, page 6-5](#)

## Understanding Policies

Policies are constrained sets of QoS properties, traffic rules, and assigned network elements. A policy consists of:

- **Device constraints**—These are defined by device properties, such as device model, operating system version, network element type, and so on.  
  
These constraints determine the QoS features that can be defined in the policy, and the type of network elements on which the QoS properties and traffic rules can be configured. You can define multiple device constraints in a policy, but they must all be for the same network element type.
- **QoS properties**—These include the policy's scheduling type, and other properties and QoS mappings that are applied to all traffic on the network elements to which they are deployed. The scheduling type can affect the QoS properties that can be defined for the policy group. For example, CRTP, LFI, trust state, and so on.
- **Assigned network elements**—These are the network elements to which the policy's properties and traffic rules are deployed. A network element can be assigned to only one policy in a policy group.

If you need to be able to change traffic rules on a given network element (for example, applying certain traffic rules during the first shift, and different traffic rules during the second shift), you can create two policy groups.

In each group, define the appropriate policies, and assign the network element to each policy. Then, when you deploy a policy group, the network element will take on the rules and properties of its assigned policy within that policy group.

- **Traffic Rules**—Traffic Rules are applied to specific traffic flows entering or leaving the network elements on which they are deployed.

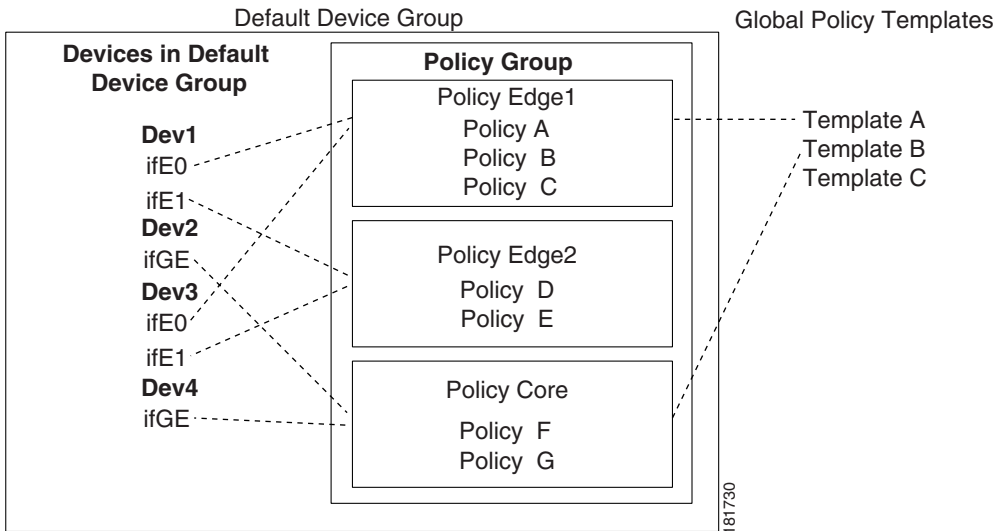
Voice policies contain the QoS properties and traffic rules for each relevant point in the IP telephony network. Each voice policy contains a voice role attribute, which specifies the role of an interface, according to its type, function, and location on the network.

For more information about voice policies, see [Chapter 7, “Provisioning: Configuring QoS for IP Telephony.”](#)

Policies are managed within policy groups. You can define shared policies across policy groups by either copying policy definitions, or by using a global policy template. Policy templates are policy definitions without network element assignments.

[Figure 8-1](#) shows the relationship between a policy group, its policies, policy templates, and assigned network elements.

Figure 8-1 Relationship between Policies, Policy Templates, and Assigned Network Elements



The example policy group has been created in the San Jose device group. The policy group contains three policies—Edge1, Edge2, and Core. Policy Edge1 is linked to Policy Template A.

This means that its traffic rules and properties are inherited from Template A. Policy Core is linked to Template B. Policy Edge2 is not linked to a template.

Interfaces ifE0 on Dev1, and ifE0 on Dev3, are assigned to policy Edge1. This means that the traffic rules and QoS properties in policy Edge1 will be deployed to those interfaces.

Interfaces ifE1 on Dev1, and ifE1 on Dev3, are assigned to policy Edge2. Different interfaces on a single device can be assigned to different policies. Interfaces ifGE on Dev2, and ifGE on Dev4 are assigned to policy Core.

When working with a policy, QPM presents you with only those QoS properties and traffic rule actions, and network elements that are valid for the defined device constraints.

### Related Topics

- [Creating a Policy, page 8-5](#)
- [Defining QoS Properties and Mappings, page 8-9](#)

- [Setting Network Element Assignments, page 8-14](#)
- [Working with Traffic Rules, page 8-25](#)
- [Copying Policies, page 8-15](#)
- [Importing Device QoS Configurations to Policies, page 8-17](#)
- [Working with Policy Templates, page 6-5.](#)
- [Viewing Policy Information, page 8-19](#)
- [More Information on Policy Configuration, page 8-39](#)
- [Basic Concepts in QPM, page 1-13](#)

## Creating a Policy

Create a policy when you want to define a group of QoS properties and traffic rules for a set of device elements with common properties.

This topic describes how to use the Policy Definition wizard to create a new policy in the following ways:

- Define the policy's device constraints using the Policy Definition wizard  
You can define device constraints manually, or from a set of selected network elements. When you use a set of network elements, QPM uses their common device properties to create one or more device constraint definitions.  
After you have defined the device constraints, you can continue to define QoS properties and traffic rules, or assign network elements.
- Link the new policy to a policy template  
The policy you are creating will use the device constraint definitions, the QoS properties, and traffic rules defined for the template. You cannot edit the policy's properties or traffic rules while it is linked to the template. You can disconnect the template, and then edit the policy.
- Copy the device constraints, QoS properties, and traffic rules, from a policy template  
The policy is not linked to the template, and you can edit the policy without affecting the template. Policy templates do not include network element assignments, so you must assign network elements to the policy.

- Copy the device constraints and, optionally, QoS properties and traffic rules, from another policy

The source policy can reside in a different policy group from the policy you are creating. You can also copy the device assignments from the source policy to the new policy, if the policies are in different policy groups in the same device group.

To create a policy:

---

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

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

To create a policy in a different policy group, select the required policy group in the Policy Group list box.

**Step 2** Click **Create**.

The Policy Definition wizard opens.

**Step 3** In the General Definition page:

- a. Enter the name of the new policy.
- b. Enter a description for the policy (optional).
- c. To define device constraints using the wizard, go to step [e](#). To define the policy using advanced options, click on the triangle next to **Advanced**. The **Advanced** field expands.
- d. Select how you want to create the policy, and fill in the appropriate fields.

For more information about the General Definition page fields, see [Policy Definition Wizard: General Definition Page, page B-81](#).

**e. Click **Next**.**

- If you are creating the policy manually, the Device Constraints page appears. Continue with [Step 4](#).
- If you are creating the policy from a template, or other policy, the Capabilities Report page appears. Continue with [Step 5](#).

You can also navigate through the wizard using the wizard navigation TOC in the left pane.

**Step 4** In the Device Constraints page, define the policy's device constraint definitions. This determines the QoS features you can use, and the type of network elements that can be assigned to the policy:

- Click **Define Manually** to define a new constraint 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](#).
- Click **OK**.

The Device Constraints page reappears displaying the new device constraint.

Repeat this step to create additional device constraints.

The network element type is the same for all constraints in the policy group and cannot be changed.

- Click **Define from Inventory** to define a new constraint from network elements.
  - Select the device model, and type of network element you want to use to define the device constraint. Click **OK**.
  - In the page that appears, 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**.
- Click **Next** to move to the next step in the wizard.

The Capabilities Report page appears.

**Step 5** In the Capabilities Report page, you can view a summary of the QoS features that can be configured for the policy group, according to the device constraints.

For more information about this page, see [Policy Definition Wizard: Capabilities Report Page, page B-89](#).

- Click **Finish**.

The QoS Properties page appears. See [Defining QoS Properties and Mappings, page 8-9](#).

---

### More Ways to Create Policies

- Copy an existing policy group in the Policy Table page. See [Copying Policies, page 8-15](#).
- Upload a device's existing QoS configuration into QPM. QPM will convert the device's QoS configuration into traffic rules and properties in new or existing policies. See [Importing Device QoS Configurations to Policies, page 8-17](#).

### Related Topics

- [Understanding Policies, page 8-2](#)
- [Defining QoS Properties and Mappings, page 8-9](#)
- [Setting Network Element Assignments, page 8-14](#)
- [Modifying a Policy, page 8-21](#)
- [Working with Traffic Rules, page 8-25](#)
- [Working with Policy Templates, page 6-5](#)
- [Viewing Policy Information, page 8-19](#)
- [More Information on Policy Configuration, page 8-39](#)

## Defining QoS Properties and Mappings

A policy's QoS properties and mappings apply to all flows passing through the interface. QoS properties include scheduling properties, traffic control features, and other QoS features, depending on the device constraints for the policy group.

Mappings include NBAR port mappings, DSCP to CoS, CoS to DSCP, IP precedence to DSCP, DSCP to markdown, excess markdown, Ingress Queue SRR configuration, and Egress Queue SRR Configuration values.

The following topics describe how to configure QoS properties and mappings for a policy or a policy template:

- [Defining QoS Properties, page 8-9](#)
- [Defining Mappings, page 8-12](#)

### Defining QoS Properties

This topic describes how to define QoS properties using the QoS Properties wizard.

The following QoS properties can be configured for a policy or policy template (depending on the device constraints):

- Congestion Management—The type of scheduling and the scheduling parameters, if required.
- Shaping Settings:
  - Frame Relay Traffic Shaping (FRTS) parameters
  - Modular Shaping parameters
- Traffic Control Settings:
  - IP RTP priority parameters
  - IP RTP header compression (CRTP) parameters
  - Link Fragmentation and Interleaving (LFI) parameters
  - Voice configuration (FRF) parameters
  - Signaling parameters
  - Trust state parameters
  - QoS style—port-based or VLAN-based

- Tx ring
- QoS Pre Classification
- Maximum Reserved Bandwidth
- CoS Override
- Inline power—Implements inline power on power-enabled Ethernet line cards.
- Congestion Avoidance—Weighted Random Early Detect (WRED) parameters

After you create a policy, or policy template, and define its device constraints using the Policy Definition wizard, you can define its QoS properties using the QoS Properties wizard.

The QoS Properties wizard lets you configure only those QoS properties that conform to the device constraints of the policy. Some QoS properties are inter-dependent, therefore the selection of available QoS properties might change as you proceed through the wizard.



#### Note

---

When you create a policy, or policy template, from another policy, or policy template, its QoS properties are defined automatically.

---

The following procedure describes all the pages in the QoS Properties wizard. However, when you define QoS properties, some (or occasionally, all) of the pages or options might not appear, depending on the device constraints for the policy, or policy template.

To define QoS properties and mappings:

---

- Step 1** Open the QoS Properties page in one of the following ways:
- After you finish the Policy Definition wizard, click **Finish**.
  - In the Policy Table page, or in the Policy Templates page, click the number in the QoS Properties column for the required policy.
  - In the Policy Table TOC, or in the Policy Template TOC, select **QoS Properties**.
- Step 2** In the QoS Properties page, click **Edit** in the QoS Properties table. The Scheduling page of the QoS Properties wizard appears.

- Step 3** In the Scheduling page:
- a. Choose the scheduling type from the list box.
  - b. Configure the queuing properties, if required. If you do not fill in the queuing property fields, the defaults on the device will be used. For more information about the fields in this page, see [QoS Properties Wizard: Congestion Management Page, page B-90](#).
  - c. Click **Next** to proceed to the next available page.



---

**Note** You can also navigate through the wizard using the wizard navigation TOC in the left pane.

---

- Step 4** In the Shaping Settings page:
- a. Configure the FRTS properties, or modular shaping properties. For more information about the fields in this page, see [QoS Properties Wizard: Shaping Settings Page, page B-104](#).
  - b. Click **Next** to proceed to the next available page.

- Step 5** In the Traffic Control Settings page:
- a. Configure the Traffic Control properties. For more information about the fields in this page, see [QoS Properties Wizard: Traffic Control Settings Page, page B-104](#).
  - b. Click **Next** to proceed to the next available page.

- Step 6** In the Congestion Avoidance Settings page:
- a. Configure the WRED properties. For more information about the fields in this page, see [QoS Properties Wizard: Congestion Avoidance Page, page B-105](#).
  - b. Click **Next** to proceed to the Summary page.

- Step 7** Review the summary page. For more information about the fields in this page, see [QoS Properties Wizard: Summary Page, page B-108](#).

- Step 8** After you are satisfied with the configuration, click **Finish**.  
The QoS Properties page reappears, displaying the QoS properties you have configured.

You can now do one of the following:

- Define mappings. See [Defining Mappings, page 8-12](#).
  - Define traffic rules. See [Creating a Traffic Rule, page 8-28](#).
  - Assign the policy to network elements. See [Setting Network Element Assignments, page 8-14](#).
- 

### Related Topics

- [Defining Mappings, page 8-12](#)
- [Viewing Policy Information, page 8-19](#)
- [Configuring FRTS Policies, page 8-47](#)

## Defining Mappings

The following mappings can be configured for a policy or policy template (depending on the device constraints):

- NBAR port mappings
- DSCP to markdown and excess markdown tables
- DSCP mapping tables
- SRR Ingress and Egress mapping tables

To define mappings:

---

- Step 1** Open the QoS Properties page in one of the following ways:
- After you finish the Policy Definition wizard, click **Finish**.
  - In the Policy Table page, or in the Policy Templates page, click the number in the QoS Properties column for the required policy.
  - In the Policy Table TOC, or in the Policy Template TOC, select **QoS Properties**.

The available mappings are displayed in the Mappings table.

- Step 2** To configure mappings, or to change the mapping settings, click **Edit** by a mapping. The corresponding Mappings page appears.

If the mapping has been configured, the current mapping settings are displayed.

If the mapping has not been configured, default mapping values are displayed.

See the following topics for more information about these pages:

- [NBAR Port Mappings Page, page B-58](#)
- [DSCP to CoS Mappings Page, page B-60](#)
- [CoS to DSCP Mappings Page, page B-62](#)
- [IP Precedence to DSCP Mappings Page, page B-64](#)
- [DSCP to Markdown Mappings Page, page B-65](#)
- [Excess Markdown Mappings Page, page B-67](#)
- [SRR Queue In Configurations Page, page B-68](#)
- [SRR Queue Out Configurations Page, page B-71](#)
- [Egress Queue Configurations Page, page B-71](#)

**Step 3** To save the displayed default mappings, click **Save Defaults**. If the default mappings are not displayed, click **Reset**, then click **Save Defaults**.

**Step 4** To configure or change a mapping, click **Create** (NBAR Port Mappings only), or select a mapping and click **Edit**. The corresponding Mapping dialog box opens.

**Step 5** Set the mapping as required, and click **OK**.

See the following topics for more information about these dialog boxes:

- [NBAR Port Mapping Dialog Box, page B-59](#)
- [DSCP to CoS Mapping Dialog Box, page B-61](#)
- [CoS to DSCP Mapping Dialog Box, page B-63](#)
- [IP Precedence to DSCP Mapping Dialog Box, page B-65](#)
- [DSCP to Markdown Mapping Dialog Box, page B-66](#)
- [Excess Markdown Mapping Dialog Box, page B-68](#)
- [SRR Queue In Configurations Page, page B-68](#)
- [SRR Queue Out Configurations Page, page B-71](#)
- [Egress Queue Configurations Page, page B-71](#)

The Mappings page reappears displaying the new mapping. Repeat [Step 4](#) and [Step 5](#) to create or edit additional mappings.

- Step 6** To delete an entire mapping configuration, click **Delete** in the Mappings page. The QoS Properties page appears.
- Step 7** After you have finished configuring mappings, click **Done** in the Mappings page. to return to the QoS Properties page.
- 

### Related Topics

- [Defining QoS Properties, page 8-9](#)
- [Viewing Policy Information, page 8-19](#)

## Setting Network Element Assignments

After you create a policy and define its device constraints, you can assign network elements to it. QPM lets you assign only those network elements in the device group that match the policy's device constraint definitions.

You can change network element assignments. When you assign network elements that are already assigned to a different policy, QPM automatically removes the previous assignment and saves the new assignment.

You can also remove network element assignments.



### Tip

---

To delete the current QoS configuration on a network element, create a policy with no configuration, and assign the network element to it.

---

This topic describes how to set network element assignments for the current policy. You can also set network element assignments from the Device Table. See [Setting a Device's Policy Assignment, page 4-14](#), and [Setting Network Element Assignments, page 8-14](#) for more information.

To assign network elements:

---

- Step 1** Open the Assigned Network Elements page in one of the following ways:
- In the Policy Groups page, or the Attached Policy Groups page, click in the Network Elements column for the required policy group.
  - In the Policy Group TOC, select **Assigned Network Elements**.

The Assigned Network Elements page displays the network elements that have been assigned to the policy group.

- Step 2** To assign network elements to the policy group:
- a. Click **Add**. The Assignment window opens displaying the network elements in the current device group that match the policy group's device constraints.
  - b. Select the desired network elements, and click **Assign**. The Assigned Network Elements page reappears, displaying all the network elements assigned to the policy group.
- Step 3** To remove network elements from the policy group assignment, select the assigned network elements in the Assigned Network Elements page, and click **Remove**.

See the following topics for more information about these pages:

- [Assigned Network Elements Page, page B-76](#)
  - [Add Assignment Dialog Box, page B-78](#)
- 

#### Related Topics

- [Creating a Policy, page 8-5](#)
- [Defining QoS Properties and Mappings, page 8-9](#)
- [Working with Traffic Rules, page 8-25](#)
- [Viewing Policy Information, page 8-19](#)

## Copying Policies

You can create new policies by copying existing policies. The new policy contains the source policy's device constraint definitions, and QoS properties, and, optionally, its traffic rules.

If you are copying to a different policy group within the current device group, you can also copy the source policy's network element assignments.

The new policy is given the default name, "Copy <number> of <source policy>." You should rename the policy with a more meaningful name.

To copy policies:

---

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

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

To change policy group, select the required policy group in the Policy Group list box.

**Step 2** Select the check box next to the policy you want to copy, and click **Copy**.

The Copy Policy dialog box opens.

**Step 3** Choose how to copy the policy:

- a. Select the device group and policy group to which you want to copy the selected policy group.
- b. To copy the QoS properties and traffic rules to the new policy, click the Copy with traffic rules and properties check box.
- c. To copy the network element assignments to the new policy, select the Copy with assignments check box. This check box is not available if you are copying within a policy group, or to another device group.
- d. Click **OK**.

The Policy Table page reappears.

See [Copy Policy Dialog Box, page B-53](#) for more information about the fields in this dialog box.

**Step 4** If you copied to a different policy group, select the required policy group in the Policy Group list box, to view the new policies.

---

### Related Topics

- [Setting Network Element Assignments, page 8-14](#)
- [Viewing Policy Information, page 8-19](#)
- [Modifying a Policy, page 8-21](#)

## Importing Device QoS Configurations to Policies

You can import the existing QoS configurations on devices into QPM policies. This is useful if you install QPM in a network where you already have QoS-configured devices.

The import process incorporates the following steps for each device:

1. The configuration that is running on the device is translated to QoS properties and traffic rules.

If the configuration contains commands that QPM does not support, those commands are not imported. Supported commands that were not successfully imported are identified in the import report.

2. For each interface, QPM creates a new policy containing the traffic rules and properties configured on the interface, and assigns the interface to it.

If the interface is already assigned to a policy in the same policy group, the assignment is deleted before the assignment to the new policy is set.

3. After all device configurations have been imported, QPM minimizes the number of policies by aggregating network elements that have similar constraints and are assigned to policies with identical properties and traffic rules. Each set of network elements is then assigned to a single policy.
4. After the import operation is complete, an HTML report is generated, which you can view in your browser. This report provides:
  - A summary of the new policies, and details of the network element assignments to those policies.
  - Details of the QoS configurations that were not successfully imported. Import failure may be caused by incomplete configurations that exist on the router, or unsupported options.

On deployment, some imported QoS configurations might use a different CLI from the original, however the QoS capabilities remain unchanged.

If QPM uses different naming conventions, the old configuration might be deleted and recreated using QPM's conventions, even if there are no configuration changes.

To import QoS configurations to policies:

---

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

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

To upload a device's configuration into a different policy group, select the required policy group in the Policy Group list box.

**Step 2** Select **Select Devices for QoS import** in the TOC.

The Select Devices for QoS Import page appears displaying the list of devices in the current device group.

**Step 3** Select the check boxes next to the devices whose policies you want to import, and click **Import**.

A dialog box appears informing you that the import process has started.

**Step 4** In the Import dialog box, do one of the following:

- View a report showing the status and other details of the upload process:

**a.** Click **View**.

The Import Reports page appears.

**b.** Select the report you want to view, and click **View**.

The selected report is displayed in a separate window.

- Click **Continue** to continue editing traffic rules.

The Policy Table page appears. If the import is still in progress, not all imported policy groups will be listed. Refresh the browser window to see additional policies as they are imported.

---

### Related Topics

- [Modifying a Policy, page 8-21](#)
- [Working with Traffic Rules, page 8-25](#)

## Viewing Policy Information

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

To view policy information:

---

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

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

To modify a policy in a different policy group, select the required policy group in the Policy Group list box.

**Step 2** To open policy information pages from the Policy Table page, do any of the following:

- Click the required policy name.

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

- Select a policy, and click **Edit**.

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

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

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

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

The In Traffic Rules page appears, displaying the inbound traffic rules for the selected policy.

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

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

- Click the network elements link for the required policy.

The Assigned Network Elements page appears, displaying the network elements that are assigned to the selected policy.

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

- Step 3** Open any policy information page from the Policy 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.

You can modify policy details from these information pages.

See the following topics for more information about these pages:

- [General Page \(Policy and Template\), page B-54](#)
  - [Device Constraints Page, page B-56](#)
  - [QoS Properties Page, page B-57](#)
  - [In Traffic Rules/Out Traffic Rules Page, page B-73](#)
  - [Assigned Network Elements Page, page B-76](#)
- 

### Related Topics

- [Modifying a Policy, page 8-21](#)
- [Defining QoS Properties and Mappings, page 8-9](#)
- [Setting Network Element Assignments, page 8-14](#)
- [Working with Traffic Rules, page 8-25](#)

## Modifying a Policy

Modify a policy when you want to modify:

- General definitions
- Device constraint definitions:
  - After you define the first device constraint in a policy, you cannot change the network element type definition. All constraints in a policy 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 must contain at least one constraint definition. You cannot delete a constraint definition if it is the only constraint definition for the policy.
- QoS properties and mappings—See [Defining QoS Properties and Mappings](#), page 8-9.
- In Traffic Rules/Out Traffic Rules—You can add, remove, and edit traffic rules. See [Working with Traffic Rules](#), page 8-25.
- Network element assignments—You can add and remove network element assignments. See [Setting Network Element Assignments](#), page 8-14.



---

**Note**

You cannot modify a policy that is linked to a policy template. You must disconnect the policy from the template, or modify the template. See [Disconnecting Policies from Policy Templates](#), page 6-11.

---

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

To modify a policy:

---

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

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

To modify a policy in a different policy group, select the required policy group in the Policy Group list box.

The Policy Table page displays for each policy, the number of QoS properties, and the number of In/Out Traffic Rules it contains, and the number of assigned network elements.

For policies that are linked to templates, the linked template name is displayed, and the properties and policies are shown as “inherited.” For more information about the Policy Table page, see [Policy Table Page, page B-51](#).

- Step 2** To edit the general definitions for the policy group:
- a. Click the required 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.
  - b. Click **Edit** in the General page.  
The Policy Definition wizard opens, displaying the General Definition page.
  - c. Edit the name and description in the General Definition page, as required.

- Step 3** 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 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:
  - a. Select the constraint definition, and click **Edit**.

The Device Definitions page appears.

- b. Edit the device constraints.

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




---

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

---

- c. 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:
    - a. Click **Define Manually**. The Device Definitions page appears.
    - b. Define the device constraints. For more information about the fields in this page, see [Policy Definition Wizard: Constraints Definition Page, page B-83](#).

**Note**

---

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

---

- c. Click **OK**. The Device Constraints page reappears displaying the new device constraint.
  - To define a new constraint from network elements:
    - a. Click **Define from Inventory**.
    - b. Select the type and model of network element to use to define the device constraint. Click **OK**.

**Note**

---

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

---

- c. 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](#).
- d. Click **Define Constraint**. The Device Constraints page reappears displaying the new device constraint.

**Step 4** After you have completed your policy definitions, click **Finish** to exit the Policy Definition wizard.

---

**Related Topics**

- [Creating a Policy, page 8-5](#)
- [Viewing Policy Information, page 8-19](#)
- [Defining QoS Properties and Mappings, page 8-9](#)
- [Setting Network Element Assignments, page 8-14](#)
- [Working with Traffic Rules, page 8-25](#)
- [Working with Policy Templates, page 6-5](#)

## Deleting a Policy

Delete a policy when you no longer want to apply its QoS properties and traffic rules to any of the assigned devices.

**Note**

---

When you delete a policy, all its contents are deleted.

---

To delete a policy:

---

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

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

To delete a policy in a different policy group, select the required policy group in the Policy Group list box.

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

A warning message appears.

**Step 3** Click **OK** to confirm the deletion.

The policy and its contents are deleted.

---

**Related Topics**

- [Viewing Policy Information, page 8-19](#)
- [Modifying a Policy, page 8-21](#)

# Working with Traffic Rules

Your traffic rules define the QoS actions that are to be applied to specific traffic flows.

The following topics describe how to create and manage policies:

- [Understanding Traffic Rules, page 8-25](#)
- [Displaying the Traffic Rules Pages, page 8-26](#)
- [Creating a Traffic Rule, page 8-28](#)
- [Modifying a Traffic Rule, page 8-35](#)
- [Deleting Traffic Rules, page 8-36](#)
- [Changing the Priority of Traffic Rules, page 8-38](#)

## Understanding Traffic Rules

After you have defined a policy or policy template with device constraints and QoS property definitions, you can add traffic rules to it.

Using QPM, you can create the following types of traffic rules:

- QoS traffic rules—A *QoS traffic rule* is a conditional statement that applies one or more specified QoS actions to a packet if the packet satisfies the conditions (filters) defined in the policy.
- Access control traffic rules—An *access control traffic rule* permits or denies the flow of data if the data packet satisfies the conditions (filters) defined in the traffic rule. An access control traffic rule does not have an associated QoS action.

**Note**

---

You cannot create access control traffic rule on all Cisco devices.

---

The filter you create for a traffic rule can be broad, in which case the traffic rule is applied to a high percentage of the traffic that travels through the device or interface, or it can be very narrow and selective.

When the device determines that a packet satisfies the conditions of the traffic rule, it applies the traffic rule's action to it.

In general, if there is more than one traffic rule defined on the interface or device, the device looks at the traffic rules in order, top to bottom, until the first match is found, at which point it applies the traffic rule and ignores remaining traffic rules.

If you are creating an advanced policing traffic rule, however, you can specify that additional traffic rules be considered after the device applies a matching traffic rule.

When you define traffic rules, QPM presents you with only actions and settings that are valid for the device constraints and QoS properties defined for the policy.

You can enable and disable traffic rules without deleting them, and you can change the order in which traffic rules are checked on the interface.

### Related Topics

- [What Types of Quality of Service Does QPM Handle?](#), page 2-3
- [Creating a Traffic Rule](#), page 8-28
- [Modifying a Traffic Rule](#), page 8-35
- [Enabling and Disabling Traffic Rules](#), page 8-37
- [Changing the Priority of Traffic Rules](#), page 8-38

## Displaying the Traffic Rules Pages

Your starting point for working with traffic rules is the lists of traffic rules in the policy or policy template. Inbound traffic rules and outbound traffic rules are displayed in separate pages.

The following topics describe how to display traffic rules:

- [Displaying Traffic Rules in a Policy](#), page 8-27
- [Displaying Traffic Rules in a Policy Template](#), page 8-27

## Displaying Traffic Rules in a Policy

You access the traffic rules for a policy from the Policy Table page. To do this:

---

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

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

**Step 2** To view policies in a different policy group, select the required policy group in the Policy Group list box.

**Step 3** In the Policy Table page, click the number of In or Out traffic rules for the required policy.

The In Traffic Rules or Out Traffic Rules page appears, displaying the inbound or outbound traffic rules in the current policy.

If the Policy TOC is displayed, you can select **In Traffic Rules**, or **Out Traffic Rules**, as required.

---

## Displaying Traffic Rules in a Policy Template

You access the traffic rules for a policy from the Policy Templates page.

### Procedure

---

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

The Templates page appears displaying the policy templates.

**Step 2** In the Templates page, click the number of In or Out traffic rules for the required template.

The In Traffic Rules or Out Traffic Rules page appears, displaying the inbound or outbound traffic rules in the template.

If the Templates TOC is displayed, you can select **In Traffic Rules**, or **Out Traffic Rules**, as required.

---

**Related Topics**

- [Creating a Traffic Rule, page 8-28](#)
- [Modifying a Traffic Rule, page 8-35](#)
- [Enabling and Disabling Traffic Rules, page 8-37](#)
- [Changing the Priority of Traffic Rules, page 8-38](#)

## Creating a Traffic Rule

Create a QoS Traffic Rule to apply specific QoS actions to selected traffic flows. Create an Access Control Traffic Rule to permit or deny specific classes of traffic. Access Control Traffic Rules do not contain any associated actions.

You can create traffic rules in a policy, or in a policy template.

The QPM Traffic Rule wizard guides you through the following steps required to define traffic rules in the inbound or outbound direction:

- [General Traffic Rule Definition, page 8-28](#)
- [Defining a Traffic Rule Filter, page 8-29](#)
- [Defining QoS Traffic Rule Actions, page 8-33](#)
- [Viewing the Traffic Rule Summary, page 8-35](#)

## General Traffic Rule Definition

The general traffic rule definition for inbound or outbound traffic rules includes the following:

- Traffic Rule name
- Traffic Rule description
- Type of Traffic Rule—QoS Traffic Rule or Access Control Traffic Rule (if relevant)

To define a traffic rule:

- 
- Step 1** Open the In Traffic Rules or Out Traffic Rules page for the policy or policy template in which you want to create a new traffic rule. See [Displaying the Traffic Rules Pages, page 8-26](#).
- Step 2** In the Traffic Rules page, click **Create**.  
The In/Out Traffic Rule wizard opens, displaying the In/Out Traffic Rule Wizard - General page.
- Step 3** In the Traffic Rule Wizard - General page:
- Enter the traffic rule name.
  - Enter a description for the traffic rule, if desired.
  - Select the type of traffic rule you want to create—QoS traffic rule, or access control traffic rule.
- Step 4** Click **Next** to proceed to the Filter step in the wizard. See [Defining a Traffic Rule Filter, page 8-29](#).
- 

#### Related Topics

- [Defining QoS Traffic Rule Actions, page 8-33](#)
- [Viewing the Traffic Rule Summary, page 8-35](#)

## Defining a Traffic Rule Filter

Define a filter to specify the traffic to which the traffic rule 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 traffic rule.
- 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 traffic rule, do not define more than 12 match statements in the traffic rule filter.

The In/Out Traffic Rule wizard guides you through the process of defining filter conditions and rules for your traffic rule.

To define a traffic rule filter:

- 
- Step 1** Open the In/Out Traffic Rule Wizard - Filter page:
- If the Traffic Rule wizard is not open, open the relevant Traffic Rules page. See [Displaying the Traffic Rules Pages, page 8-26](#). Select the traffic rule whose filter you want to edit, and click **Edit**. The Traffic Rule wizard opens, displaying the In/Out Traffic Rule Wizard - General page.
  - If the wizard is open, click **Next** in the Traffic Rule Wizard - Filter 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 traffic rule:
- **Create New Filter**—The traffic rule is applied to traffic that matches any of the filter conditions. If you do not define filter rules, the traffic rule 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 traffic rule. Go to [Step 8](#).
- Step 4** Define a filter rule:
- a. Click **Create** in the Filters 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. Edit the rule conditions as required, and click **Done** to return to the Filter page.

**Step 7** To delete a filter rule, select the filter rule in the Filter page, and click **Delete**.

**Step 8** After you have completed your filter definitions, click **Next**.

- If you are defining a QoS traffic rule, the Traffic Rule Wizard - Actions page appears. See [Defining QoS Traffic Rule Actions](#), page 8-33.
- If you are defining an access control traffic rule, the Summary page appears. See [Viewing the Traffic Rule Summary](#), page 8-35.

---

### Related Topics

- [General Traffic Rule Definition](#), page 8-28
- [Working with Aliases](#), page 6-1

## Defining QoS Traffic Rule Actions

The Traffic Rule Actions step of the Traffic Rule 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 traffic rule

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 Policy Wizard - Actions step. However, when you define actions for a policy, some of the options might not appear, depending on the device constraints and QoS properties of the policy group.

To define QoS Traffic Rule Actions:

- 
- Step 1** Open the Traffic Rule Wizard - Actions page:
- If the Traffic Rule wizard is not open, open the relevant Traffic Rules page. See [Displaying the Traffic Rules Pages, page 8-26](#). Select the traffic rule whose action you want to edit, and click **Edit**. The Traffic Rule wizard opens, displaying the Traffic Rule Wizard - General page. Click **Actions** from the TOC
  - If the Traffic Rule wizard is open, click **Next** in the Traffic Rule Wizard - Filter page. The Policy 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:
- [In/Out Traffic Rule Wizard: Marking Actions Page, page B-123](#)
  - [In/Out Traffic Rule Wizard: Microflow Policing Actions Page, page B-125](#)
  - [In/Out Traffic Rule Wizard: Policing Actions Page, page B-127](#)
  - [In/Out Traffic Rule Wizard: Shaping Actions Page, page B-131](#)
  - [In/Out Traffic Rule Wizard: Queuing Actions Page, page B-132](#)
  - [In/Out Traffic Rule Wizard: Traffic Control Page, page B-135](#)
  - [In/Out Traffic Rule Wizard: Congestion Avoidance Actions Page, page B-136](#)
  - [In/Out Traffic Rule Wizard: Service Policy Actions Page, page B-137](#)
- Step 3** After you have completed defining the policy actions, click **Next** to proceed to the Summary step in the wizard. See [Viewing the Traffic Rule Summary, page 8-35](#).
- 

#### Related Topics

- [General Traffic Rule Definition, page 8-28](#)
- [Defining a Traffic Rule Filter, page 8-29](#)

## Viewing the Traffic Rule Summary

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

To view the Traffic Rule Summary:

- 
- Step 1** If the Policy Wizard - Summary page is not displayed, select **Summary** in the wizard navigation TOC.
  - Step 2** Review the traffic rule 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 traffic rule summary, click **Finish** to complete the traffic rule and exit the wizard.
- 

### Related Topics

- [General Traffic Rule Definition, page 8-28](#)
- [Defining a Traffic Rule Filter, page 8-29](#)
- [Defining QoS Traffic Rule Actions, page 8-33](#)

## Modifying a Traffic Rule

You can modify a traffic rule by changing its properties, filter, or actions. When you redeploy the traffic rules, the modified traffic rule replaces the old traffic rule on the policy's assigned network elements.

You cannot modify traffic rules within a policy that is linked to a policy template. You must either disconnect the policy template first, or modify the policy template.

To modify a traffic rule:

- 
- Step 1** Open the In Traffic Rules or Out Traffic Rules page for the policy or policy template in which you want to modify a traffic rule. See [Displaying the Traffic Rules Pages, page 8-26](#).

- Step 2** In the Traffic Rules page, select the check box next to the traffic rule you want to edit, and click **Edit**. The Traffic Rule wizard opens, displaying the Traffic Rule Wizard - General page. Change the name or description of the traffic rule if required.
- Step 3** 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 traffic rule filter, see [Defining a Traffic Rule Filter, page 8-29](#).
  - To modify the traffic rule actions, see [Defining QoS Traffic Rule Actions, page 8-33](#).
- Step 4** After you have finished editing the traffic rule click **Finish**. The Traffic Rule Wizard - Summary page appears. See [Viewing the Traffic Rule Summary, page 8-35](#).
- 

#### Related Topics

- [Working with Aliases, page 6-1](#)
- [Working with Policy Templates, page 6-5](#)

## Deleting Traffic Rules

When you no longer want to use a traffic rule, you can delete it from the policy or policy template. When you redeploy the traffic rules, the deleted traffic rule is removed from the policy's assigned network elements.

You cannot delete a traffic rule in a policy that is linked to a policy template. You must either first disconnect the policy template, or delete the traffic rule in the linked policy template.

#### Before You Begin

If you are not sure whether you will need a traffic rule, consider disabling it instead of deleting it. See [Enabling and Disabling Traffic Rules, page 8-37](#) for information on disabling a traffic rule.

To delete Traffic Rules:

- 
- Step 1** Open the In Traffic Rule or Out Traffic Rule page for the policy or policy template in which you want to delete a traffic rule. See [Displaying the Traffic Rules Pages, page 8-26](#).
  - Step 2** In the Traffic Rule page, select the check box(es) next to the traffic rule or policies you want to delete.
  - Step 3** Click **Delete**.
- 

#### Related Topics

- [Enabling and Disabling Traffic Rules, page 8-37](#)

## Enabling and Disabling Traffic Rules

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

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

To enable or disable traffic rules:

- 
- Step 1** Open the In Traffic Rules or Out Traffic Rules page for the policy or policy template in which you want to work. See [Displaying the Traffic Rules Pages, page 8-26](#).
  - Step 2** In the Traffic Rules page, select the check box(es) next to the traffic rule or traffic rule you want to enable or disable.
  - Step 3** Click **Enable** or **Disable** as required.
-

## Changing the Priority of Traffic Rules

The device examines QoS traffic rules in the order until a match is found for the packet. Even if a packet satisfies more than one traffic rule, it will be treated as satisfying only the first traffic rule that the device encounters.

However, you can define your traffic rule to include the Continue setting, in which case a subsequent match will be sought.

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

If you are creating complex traffic rule 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 traffic rule statement you want applied.

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

To change the priority of Traffic Rules:

- 
- Step 1** Open the In Traffic Rules or Out Traffic Rules page for the policy or policy template in which you want to reorder policies. See [Displaying the Traffic Rules Pages, page 8-26](#).
  - Step 2** In the Traffic Rules page, click **Reorder**.  
The Reorder dialog box opens.
  - Step 3** Select the traffic rule that you want to reorder.
  - Step 4** Click the Up or Down button to reorder the traffic rule as required.
-

# More Information on Policy Configuration

This section provides additional information about configuring QoS on different types of interfaces and devices:

- [QoS Configuration on Network Element Types, page 8-39](#)
- [Configuring FRTS Policies, page 8-47](#)
- [Configuring VLAN Policies, page 8-49](#)
- [Configuring VC Bundle Policies, page 8-49](#)

## Related Topics

- [Advanced IP Telephony Network Configuration, page 7-27](#)

## QoS Configuration on Network Element Types

Policies can be assigned to only one type of network element. For some devices, you will need to define several policies to consolidate the QoS configuration on the device.

To create a complete QoS configuration for a single type of network element, you might need to define more than one policy. For example, when configuring FRTS policies, and when configuring VLAN policies.

There are other cases, where you might need two policies. For example, you configure markdown in policing traffic rules on Catalyst ports at the port level, but to change the default markdown mapping values, you must define an additional policy at the device level.

This section provides tables listing the types of QoS configurations that can be configured for each network element type, for different device models:

- [Types of QoS Configurations on IOS Devices](#)
- [Types of QoS Configurations on Catalyst Devices](#)
- [Types of QoS Configurations on Layer 2 Switches Running IOS](#)
- [Types of QoS Configurations on Layer 3 Devices](#)

**Table 8-1** *Types of QoS Configurations on IOS Devices*

Device Model	Network Element Type				
	Device	Interface	ATM PVC	FR DLCI	VLAN
1600	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
1700	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
1720	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
1750	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
1760	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
2500	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
2600	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
3200	NBAR Port Mapping	Scheduling Properties Actions	Not Available	Scheduling Properties Actions	Actions (VLAN scheduling is inherited from its ports.)

**Table 8-1** *Types of QoS Configurations on IOS Devices (continued)*

Device Model	Network Element Type				
	Device	Interface	ATM PVC	FR DLCI	VLAN
3600	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties: Actions	Scheduling Properties Actions	Not available
3700	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
3800	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
4000	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
4500	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
4700	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
7100	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
7200	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available

**Table 8-1** *Types of QoS Configurations on IOS Devices (continued)*

Device Model	Network Element Type				
	Device	Interface	ATM PVC	FR DLCI	VLAN
7300	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
7400	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
7500	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
7600	DSCP Mappings NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Actions (VLAN scheduling is inherited from its ports.)
7700	No QoS configuration at device level.	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
AS5300	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
AS5800	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
C4GWY	No QoS configuration at device level.	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available

**Table 8-1** *Types of QoS Configurations on IOS Devices (continued)*

Device Model	Network Element Type				
	Device	Interface	ATM PVC	FR DLCI	VLAN
Cat3550	DSCP Mappings	Scheduling Properties Actions	Not available	Not available	DSCP Mappings Actions (VLAN scheduling is inherited from its ports.)
Cat3750	DSCP Mappings	Properties Actions	Not available	Not available	Not available
Cat4000(IOS)	DSCP Mappings	Scheduling Properties Actions	Not available	Not available	Actions (VLAN scheduling is inherited from its ports.)
Cat4200	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
Cat4500(IOS)	DSCP Mappings	Scheduling Properties Actions	Not available	Not available	Actions (VLAN scheduling is inherited from its ports.)
Cat6000_PFC1 (IOS)	DSCP Mappings NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Actions (VLAN scheduling is inherited from its ports.)

Table 8-1 Types of QoS Configurations on IOS Devices (continued)

Device Model	Network Element Type				
	Device	Interface	ATM PVC	FR DLCI	VLAN
Cat6000_PFC2 (IOS)	DSCP Mappings NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Actions (VLAN scheduling is inherited from its ports.)
Cat6000_PFC3 (IOS)	DSCP Mappings NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Actions (VLAN scheduling is inherited from its ports.)
MSFC (QoS is supported on the FlexWan module only)	NBAR Port Mapping	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available
RSM	No QoS configuration at device level.	Scheduling Properties Actions	Not available	Scheduling Properties Actions	Not available
VG200	No QoS configuration at device level.	Scheduling Properties Actions	Scheduling Properties Actions	Scheduling Properties Actions	Not available

**Table 8-2** *Types of QoS Configurations on Catalyst Devices*

Device Model	Network Element Type		
	Device	Interface	VLAN
Cat2948	Scheduling Actions	Properties	Not available
Cat2980	Scheduling Actions	Properties	Not available
Cat4000	Scheduling Actions	Properties	Not available
Cat4500	Scheduling Actions	Properties	Not available
Cat5000	Actions	Not available	Not available
Cat6000_NO_PFC	Scheduling	Properties	Not available
Cat6000_PFC1	Scheduling DSCP Mappings Actions	Properties Actions	Actions (VLAN scheduling is inherited from its ports.)
Cat6000_PFC2	Scheduling DSCP Mappings Actions	Properties Actions	Actions (VLAN scheduling is inherited from its ports.)
Cat6000_PFC3	Scheduling DSCP Mappings Actions	Properties Actions	Actions (VLAN scheduling is inherited from its ports.)

**Table 8-3** *Types of QoS Configurations on Layer 2 Switches Running IOS*

<b>Devices / NEs</b>	<b>Device</b>	<b>Interface</b>
Cat2900	Not available	Actions
Cat2950	Scheduling	Properties Actions
Cat2950_SI	Scheduling	Properties Actions
Cat3500	Not available	Properties Actions

**Table 8-4** *Types of QoS Configurations on Layer 3 Devices*

<b>Devices / NEs</b>	<b>Device</b>	<b>Interface</b>	<b>POI</b>
Cat2948_L3	Scheduling	Scheduling Actions	Not available
Cat4232_L3	Scheduling	Scheduling Actions	Not available
Cat4908_L3	Scheduling	Scheduling Actions	Not available
Cat8500	Not available	Not available	Scheduling

## Configuring FRTS Policies

This section describes how to configure Frame Relay Traffic Shaping (FRTS) on a frame relay main interface, and how to configure FRTS for frame relay subinterfaces and DLCIs.

### Configuring FRTS for Frame Relay Main Interfaces

To configure FRTS for frame relay main interfaces:

1. Use the Policy Definition wizard to create a new policy with the following constraint definition:
  - Select the device's Model and OS version.
  - Network Element—Select **Interface**.
  - Interface Type—Select **Frame Relay**.
  - Interface Card—Select **NA**.
2. In the QoS Properties wizard, define the following:
  - In the Congestion Management page, select a scheduling method.
  - In the Shaping Settings page, enable FRTS, and configure FRTS parameters.
  - Define any other desired property.
3. Use the Traffic Rule wizard to configure traffic rules if required.
4. Assign frame relay main interfaces to the policy group.

### Configuring FRTS for Frame Relay Subinterfaces or DLCIs

To configure FRTS for frame relay subinterfaces or DLCIs, you must create two policies:

- A policy to enable FRTS on the frame relay main interface to which the subinterfaces or DLCIs belong.
- A policy to configure FRTS for the subinterfaces or DLCIs.

To configure FRTS for frame relay subinterfaces or DLCIs:

- 
- Step 1** Create a policy for the frame relay main interface:
- Use the Policy Definition wizard to create a new policy as described in Step 1 in [Configuring FRTS for Frame Relay Main Interfaces](#).
  - In the QoS Properties wizard, select the Enable FRTS in the Shaping Settings page. Do not set FRTS parameters.
  - Assign the main interface of the frame relay subinterfaces or DLCIs to this policy group.
- Step 2** Create a policy for the frame relay subinterfaces or DLCIs:
- Use the Policy Definition wizard to create a new policy as described in Step 1 in [Configuring FRTS for Frame Relay Main Interfaces](#). For DLCIs, select FR DLCI as the network element in the Constraints Definition page.
  - Define FRTS properties and other policies as described in steps 2 and 3 in [Configuring FRTS for Frame Relay Main Interfaces](#).
  - Assign frame relay subinterfaces or DLCIs to the policy.
- 

- Frame relay main interfaces and subinterfaces can have different QoS capabilities, therefore do not assign main interfaces and subinterfaces to the same policy. Create one policy for the main interfaces and another policy for the subinterfaces, as described above.
- If FRTS is configured for frame relay subinterfaces or DLCIs, but their parent interfaces are not defined with FRTS, the subinterface configuration will not be deployed. You can generate a FRTS Conflicts report to display these frame relay subinterfaces or DLCIs.

#### Related Topics

- [Creating a Policy, page 8-5](#)
- [Defining QoS Properties and Mappings, page 8-9](#)
- [Setting Network Element Assignments, page 8-14](#)

## Configuring VLAN Policies

To configure policies on a VLAN, you must create two policies:

- A policy for the VLAN:
  - Define the type of network element in the Device Constraints Definition page of the Policy Definition wizard as VLAN.
  - Assign the VLAN to the policy.
  - Define traffic rules for the VLAN.
- A policy for the VLAN interfaces on which you want to configure the VLAN traffic rules:
  - In the QoS Properties wizard, define the QoS style in the Traffic Control Settings page as VLAN-based.
  - Assign the required VLAN interfaces to the policy.
  - Do not define any traffic rules in this policy.



### Note

When configuring VLAN-based policies for devices with Native IOS, the **switch port** CLI command must be configured on the device.

### Related Topics

- [Creating a Policy, page 8-5](#)
- [Defining QoS Properties and Mappings, page 8-9](#)
- [Setting Network Element Assignments, page 8-14](#)

## Configuring VC Bundle Policies

To configure policies on a VC Bundle, you must create two policies:

- A policy for the VC Bundle:
  - Define the type of network element in the Device Constraints Definition page of the Policy Definition wizard as FrameRelay or ATM.
  - Assign the FrameRelay or ATM to the policy.
  - Define traffic rules for the VC Bundle.

- A policy for the VC Bundle interfaces on which you want to configure the VC Bundle traffic rules:
  - In the QoS Properties wizard, define the QoS style in the Traffic Control Settings page as VC Bundle-based.
  - Assign the required VC Bundle interfaces to the policy.
  - Do not define any traffic rules in this policy.

**Note**

---

When configuring VC Bundle-based policies for devices with Native IOS, the **switch port** CLI command must be configured on the device.

---

**Related Topics**

- [Creating a Policy, page 8-5](#)
- [Defining QoS Properties and Mappings, page 8-9](#)
- [Setting Network Element Assignments, page 8-14](#)