Chapter 11

Configuring and Managing Policies with Policy Editor

This chapter describes how to use Policy Editor to configure and manage policies. You can also use the following to configure and manage policies:

- To use the SRC CLI, see ***Chapter 10, Configuring and Managing Policies with the SRC CLI.***
- To use the C-Web interface, see *SRC-PE C-Web Interface Configuration Guide, Chapter 21, Configuring and Managing Policies with the C-Web Interface*.

Topics in this chapter include:

- Before You Configure Policies on page 282
- Configuring Policy Folders on page 284
- Configuring Policy Groups on page 285
- Configuring Policy Lists on page 288
- Configuring Policy Rules on page 291
- Configuring Classify-Traffic Conditions on page 295
- Configuring QoS Conditions on page 316
- Configuring Actions on page 318
- Modifying Policy Objects in the Directory on page 365

Before You Configure Policies

Building policies is a top-down operation. For example, before you can add a subordinate to the policy group, the policy group itself must exist.

Creating a Worksheet

Before you enter policy information into the Policy Editor fields, you must determine what information you want to enter and where it will go. It is best to create a worksheet where you can record such things as names, priorities, addresses, and so on.

To create a worksheet:

1. Determine the policy requirements for your system.
2. Consider information that contains (at a minimum) names and parameters for:
   - Policy group
   - Policy list
   - Policy rules
   - Conditions
   - Actions
3. Record the policy information about the worksheet.

Naming Objects

Object names must be unique and must conform to LDAP distinguished name (DN) constraints. You can provide your own object names, or Policy Editor can assist you by providing a name base for objects when you perform operations such as adding an object or copying and pasting an object into another folder.

You can configure whether or not Policy Editor suggests a name base for newly created objects and, if so, what Policy Editor uses as the name base. You can also specify whether or not object names in the navigation pane are prefixed with their object type. See Table 15 on page 168 in ***Chapter 7, Using Policy Editor***.

If a name conflict occurs, the policy engine changes the object name by suffixing a number to the name separated by an underscore (_). The number is the next integer in sequence that does not cause a name conflict. You will see the new name in the navigation pane. For example, if policy group *internet-slow* exists in the organizational folder *XYZ*, then the policy engine assigns the name *internet-slow_1*. A subsequent policy group creation results in *internet-slow_2*.

Using the apply-groups Statement

When you use the **apply-groups** statement on the JUNOS routing platform to apply a configuration group to a hierarchy level in a configuration, you need to make sure that the SAE configuration group (default name is sdx) is in the first position in the **apply-groups** statement.

Using Expressions

Many of the policy fields can take expressions in addition to literal values. If you can enter an expression for a field, the expression type is noted in the field definition. For information about using and formatting expressions, see *Expressions* on page 404.

Policy Values

As you are planning your policy configuration, you need to understand how invalid values in policies are handled on JUNOS routing platforms and JUNOSe routers.

SAE to JUNOS Routing Platforms

When the SAE sends policies to JUNOS routing platforms, it uses JUNOScript on Blocks Extensible Exchange Protocol (BEEP), which is an XML-based protocol. Many of the configuration values in JUNOScript are strings in which the value is a number. If you enter an integer value that is too large, Policy Editor flags the entry as invalid, but the value is still sent to the router because JUNOScript on BEEP allows for its transmission. The router is the authority that decides whether values are valid for the particular version of the JUNOS software and the routing platform. If the value is too large, the router sends an error message to the SAE.

For example, the valid range for the burst size limit in a policer action is 1,500 to 100,000,000. If a value greater than 100,000,000 is specified in Policy Editor, it is flagged as invalid. However, as usual, the SRC software attempts to activate the service, but the activation will fail because the burst size is an invalid value on the router.

SAE to JUNOSe Routers

When the SAE sends policies to JUNOSe routers, it uses the Common Open Policy Service (COPS) protocol with specific standard Policy Information Bases (PIBs) and private PIBs. Many of the configuration values in the PIBs are not strings in which the value is a number. Sometimes the numeric range in the PIB is larger than the valid range of values on the router. For integer values in policies, the eventual policy on the router has only the portion of a value that can be converted to an integer in the usable range.

The example below for ToS byte is such a case. From the JUNOSe-IP-PIB:

```
...
JunoseIpPolicyClaclRuleEntry ::= SEQUENCE {
...
junoseIpPolicyClaclRuleTosByte Integer32,
junoseIpPolicyClaclRuleTosMask Integer32,
...
```

If a policy has a literal ToS byte value of 300, the high bits are ignored (or a mask of 255 is used) so that the value used for the ToS byte is 44; that is, 300 minus 256.

Configuring Policy Folders

You use policy folders to organize policy groups. To create a policy folder:

1. In the Policy Editor navigation pane, right-click a Policy folder, and select **New > PolicyFolder**.

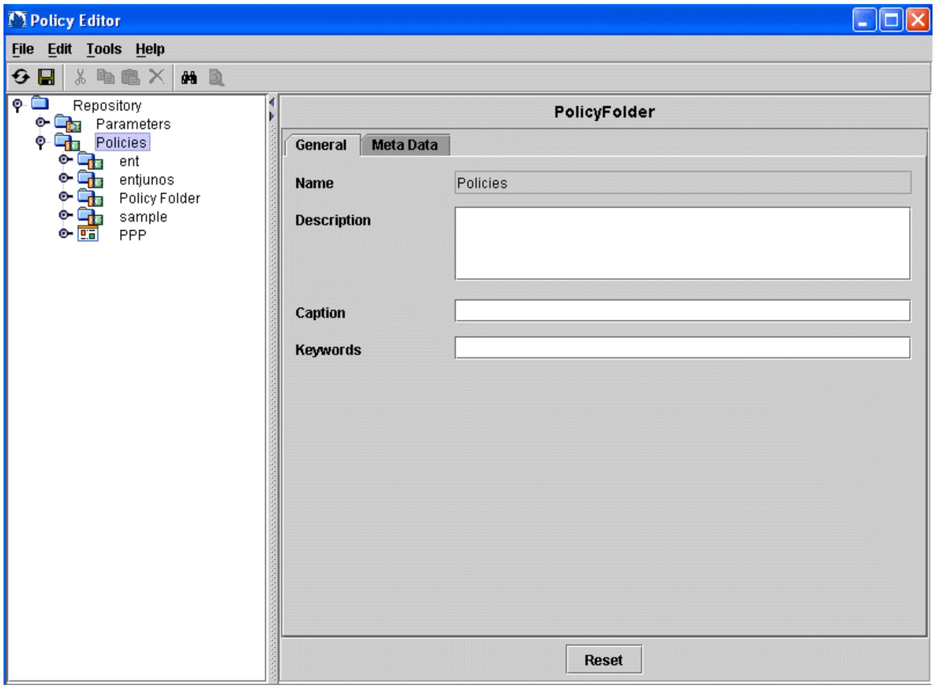
   The PolicyFolder Name dialog box appears.

2. Enter the policy folder name, and click **OK**.

   The new policy folder appears in the navigation pane.

3. Select the new policy folder.

   The PolicyFolder pane appears.



Name: Policies

4. Edit or accept the default values for the fields.

   See *Policy Folder Fields* on page 285.

5. Select **File > Save**.

Policy Folder Fields

In Policy Editor, you can modify the following fields in the PolicyFolder content pane.

Description

- Description of the policy folder.
- Value—Text
- Default—No value

Caption

- Short description of the policy folder.
- Value—Text
- Default—No value

Keywords

- Series of words that Policy Editor uses as a filter for keyword searches.
- Value—Text
- Default—No value

Configuring Policy Groups

You create policy groups within policy folders. To add a policy group:

1. In the Policy Editor navigation pane, right-click the **Policies** folder, and select **New > PolicyGroup**.

   or

   Cut or copy an existing policy group, and paste it to create a new policy group.

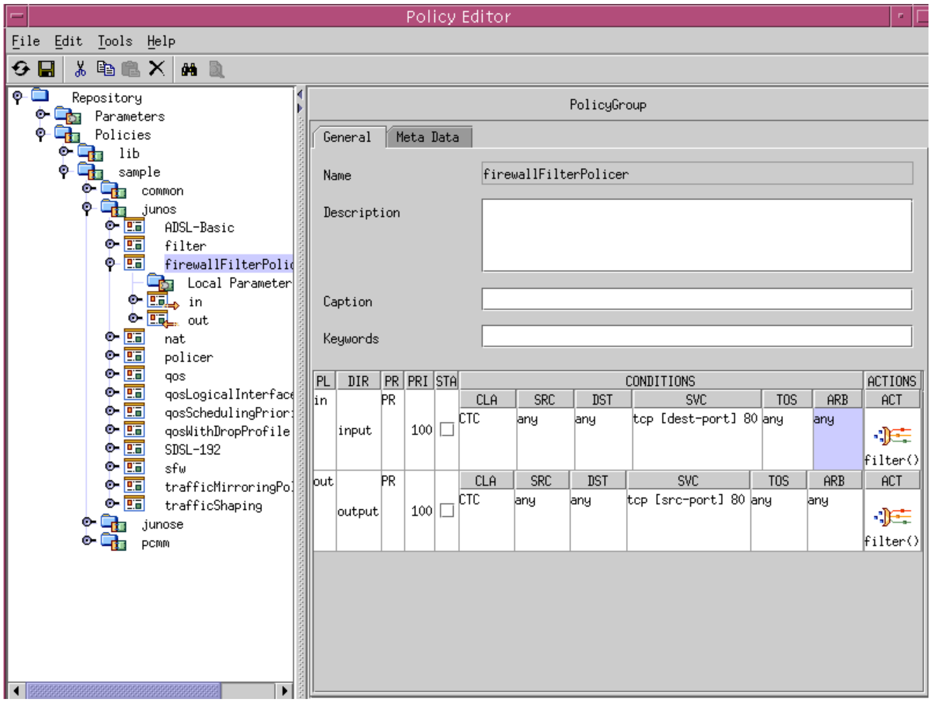
   The PolicyGroup Name dialog box appears.

2. Enter a unique name for the policy group, and click **OK**.

   The new policy group appears in the navigation pane.

3. Select the new policy group.

   The PolicyGroup pane appears.



Name firewallFilterPolicer

Description

Caption

Keywords

PL	DIR	PR	PRI	STA	CONDITIONS						ACTIONS
					CLA	SRC	DST	SVC	TOS	ARB	ACT
in	input	PR	100	☐	CTC	any	any	tcp [dest-port] 80	any	any	filter()
out	output	PR	100	☐	CTC	any	any	tcp [src-port] 80	any	any	filter()

4. Edit or accept the default values for the policy group fields.

   See *Policy Folder Fields* on page 285.

5. Select **File** > **Save**.

The PolicyGroup pane contains a table that summarizes the policy lists and rules that are within the policy group. See. *Using the PolicyGroup Summary Table* on page 287.

Policy Group Fields

In Policy Editor, you can modify the following fields in a PolicyGroup content pane.

Description

- Description of the policy group.
- Value—Text
- Default—No value

Caption

- Short description of the policy group.
- Value—Text
- Default—No value

Keywords

- Series of words that Policy Editor uses as a filter for keyword searches.
- Value—Text
- Default—No value

Using the PolicyGroup Summary Table

The PolicyGroup pane contains a table that summarizes the policy lists and rules that are within the policy group. The fields in the table vary depending on the type of policy lists and rules in the policy group. Table 25 describes the fields in the policy group summary table.

Table 25: Fields in Policy Editor Summary Tables

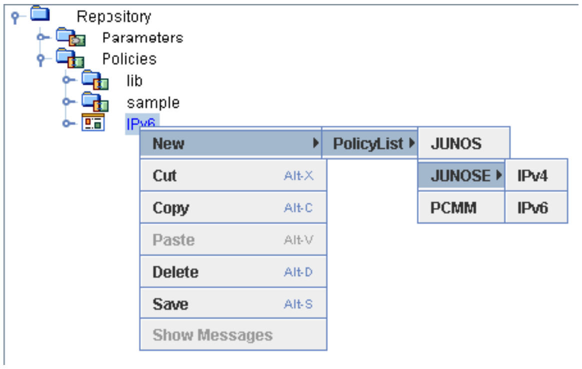
Field	Description	To Change the Field
ACT	Action applied to a policy group.	Double-click on an ACT cell. The corresponding action dialog box appears. or Right-click on an ACT cell. A pop-up menu appears from which you can edit or delete an action.
ARB	JUNOS filter conditions.	Double-click on an ARB cell. The Arbitrary Condition dialog box appears.
CLA	Classifier.	Double-click on a CLA cell. The condition pane appears.
DIR	Indicates the applicability of the policy list—whether the policy list associated with the policy group applies to egress or ingress traffic flow or both egress and ingress traffic flow. For PCMM policies, indicates whether the policy is for an upstream service flow or a downstream service flow.	Click on a DIR cell. A drop-down menu appears from which you can select a direction.
DST	Destination network matching.	Double-click on a DST cell. The Destination Network Condition dialog box appears.
FWC	Forwarding class QoS condition.	Double-click on an FWC cell. The QoS Condition dialog box appears.
PL	Name of the policy list.	Double-click on a PL cell. The PolicyList pane appears.
PR	Name of the policy rule.	Double-click on a PR cell. The PolicyRule pane appears.
PRI	Precedence that is applied to the actions of a policy rule.	Double-click on a PRI cell. A text cursor appears that allows you to type a new precedence.
ROLES	Indicates whether the policy list is a JUNOS policy list or a JUNOSe policy list.	Click on a ROLES cell. A drop-down menu appears from which you can select a role.
SRC	Source network matching.	Double-click on an SRC cell. The Source Network Condition dialog box appears.
STA	Indicates whether statistics accounting is enabled or disabled.	Click the check box. Checking the box enables accounting. Removing the check disables accounting.
SVC	Protocol and port matching.	Double-click on an SVC cell. The Protocol Condition dialog box appears.
TOS	Type of service matching.	Double-click on a TOS cell. The TOS Condition dialog box appears.

Configuring Policy Lists

When you add a policy list, you specify whether the policy list is for JUNOS routing platforms, JUNOSe routers, or a CMTS device (PCMM in Policy Editor). The type of policy list that you add controls the type of policy rules that you can add to the policy list.

To add a policy list:

1. In the Policy Editor navigation pane, right-click a policy group, and select **New > PolicyList**. Then select **JUNOS**, **JUNOSE**, or **PCMM**. If you select **JUNOSE**, then select either **IPv4** or **IPv6**.



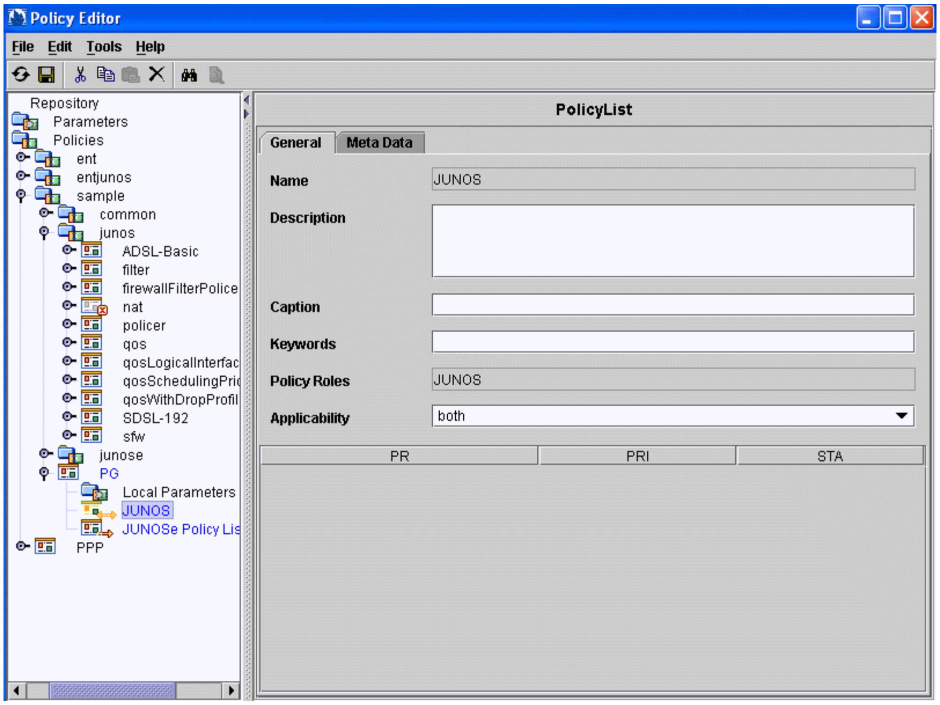
The PolicyList Name dialog box appears.

2. Enter the policy list name, and click **OK**.

The new policy list appears in the navigation pane.

3. Select the new policy list name.

   The PolicyList pane appears.



Name: JUNOS
Description:
Caption:
Keywords:
Policy Roles: JUNOS
Applicability: both

4. Edit or accept the default values for the policy list fields.

   See *Policy Folder Fields* on page 285.

5. Select **File** > **Save**.

Policy List Fields

In Policy Editor, you can modify the following fields in the PolicyList content pane.

Description

- Description of the policy list.
- Value—Text
- Default—No value

Caption

- Short description of the policy list.
- Value—Text
- Default—No value

Keywords

- Series of words that Policy Editor uses as a filter for keyword searches.
- Value—Text
- Default—No value

Policy Roles

- Indicates whether the policy list is a JUNOS policy list, a JUNOSe policy list (for IPv4 or IPv6), or a PCMM policy list. You cannot change this value.

Applicability

- Indicates where the policy is applied on the router or, for PCMM policies, indicates whether the policy applies to the upstream or downstream channel. For JUNOS routing platforms, applicability determines the types of policy rules that you can create. For example, if you select both, you can create a JUNOS ASP or a JUNOS scheduler policy rule, but you cannot create a JUNOS filter.
- Value
    - input—Policy is applied to the input (ingress) side of the router interface. For PCMM policies, indicates that the policy is provisioned on upstream service flows (from the cable modem to the CMTS device).
    - output—Policy is applied to the output (egress) side of the router interface. For PCMM policies, indicates that the policy is provisioned on the downstream channel (from the CMTS device to the cable modem).
    - both—Policy is applied to both the input (ingress) and output (egress) side of the interface, or it is attached implicitly to the interface without indicating direction. *Both* is not valid for PCMM policies.

      In the case of JUNOS ASP policy rules, the policy is attached to both sides of the interface; for JUNOS scheduler policy rules, the policy is attached implicitly to the interface without indicating direction.
- Default
    - JUNOS policy lists—Both
    - JUNOSe IPv4 policy lists—Input
    - JUNOSe IPv6 policy lists—Input
    - PCMM policy lists—Input

Using the PolicyList Summary Table

The PolicyList pane contains a table that summarizes the policy rules that are within the policy list. It contains one row for each policy action that the policy list contains. The fields in the table vary depending on the type of policy rules that are contained in the policy list. You can modify policy rules from within the summary table, or you can modify them by selecting objects from the navigation pane. The fields in the summary table are explained in Table 25 on page 287.

Configuring Policy Rules

The type of policy rule that you can create depends on the type and applicability of the policy list in which you create the policy rule. There is only one type of policy rule for JUNOSe policy lists and PCMM policy lists. For JUNOS policy lists, you can create the following policy rule types:

- JUNOS ASP—Applicability of policy list must be both input and output.
- JUNOS FILTER—Applicability of policy list must be input or output.
- JUNOS POLICER—Applicability of policy list must be input or output.
- JUNOS SCHEDULER—Applicability of policy list must be both.
- JUNOS SHAPING—Applicability of policy list must be both.

Before You Configure JUNOS Policy Rules

The following are prerequisites to using policy rules on JUNOS routing platforms.

JUNOS Scheduler and JUNOS Shaping Policy Rules

Before you use the JUNOS scheduler and JUNOS shaping policy rules, check that your Physical Interface Card (PIC) supports JUNOS scheduling and shaping rate. Also, check that your interface supports the per-unit-scheduler.

You must enable the per-unit-scheduler on the interface. To do so, on the JUNOS routing platform, include the **per-unit-scheduler** statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
per-unit-scheduler;
```

JUNOS ASP Policy Rules

Before you use the Adaptive Services PIC (ASP) policy rule to create a stateful firewall or NAT policy, you must configure the Adaptive Services PIC on the JUNOS routing platform. For example:

```
sp-0/1/0 {
    unit 0 {
        family inet {
            address 10.10.1.1/32;
        }
    }
}
```

For more information about configuring AS PICs, see the *JUNOS Services Interfaces Configuration Guide*.

Setting the Policy Rule Precedence

Policy lists can have more than one policy rule. Policy rules are assigned a precedence that determines the order in which the policy manager applies policy rules. Rules are evaluated from lowest to highest precedence value. For JUNOSe policies, rules with equal precedence are evaluated in the order of creation. For JUNOS policies, rules with equal precedence are evaluated in random order.

Note that for JUNOS SCHEDULER and JUNOS POLICER policy rules, precedence is not a factor.

The router classifies packets beginning with the classify condition in the policy list that has the policy rule with the lowest precedence.

- If the packet matches the condition, the router applies the policy rule actions to the packet and does not continue to examine further conditions.
- If the packet does not match the condition, the router tries to match the packet with the classify condition in the policy rule with the next higher precedence.
- If the packet does not match any of the classify conditions, it is forwarded. There are some exceptions. For example, in the case of a JUNOS ASP stateful firewall, packets that do not match the classify conditions are dropped. Only matching packets are forwarded.

For JUNOSe routers, if you want the router to take two corresponding actions on a packet, you would create a JUNOSe policy list that has more than one policy rule with the same precedence. For example, you may want a policy rule that marks a packet and a policy rule that forwards the packet to the next interface. Or you could have a policy rule that applies a traffic class and a policy rule that forwards the packet to the next hop.

Adding a Policy Rule

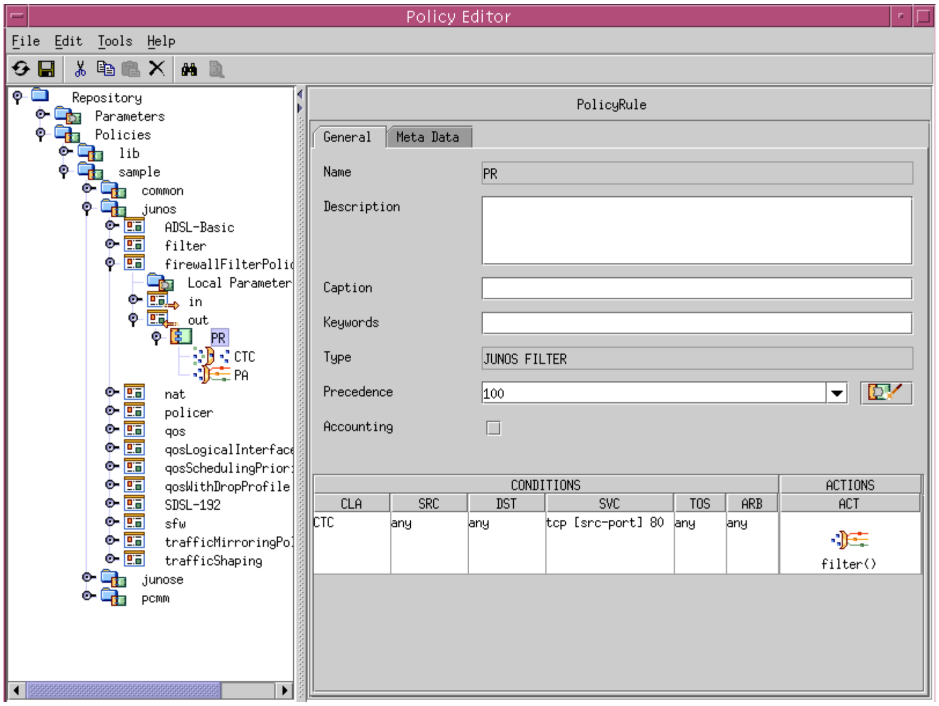
To add a policy rule:

1. In the navigation pane, right-click a policy list.
2. Select **New > PolicyRule**, and select a policy rule from the list.

   The PolicyRule Name dialog box appears.
3. Enter the Policy Rule name, and click **OK**.

   The new policy rule appears in the navigation pane.
4. Select the new Policy Rule object in the navigation pane.

   The PolicyRule pane appears.



Name: PR

Description:

Caption:

Keywords:

Type: JUNOS FILTER

Precedence: 100

Accounting ☐

CONDITIONS						ACTIONS
CLA	SRC	DST	SVC	TOS	ARB	ACT
CTC	any	any	tcp [src-port] 80	any	any	filter()

5. Edit or accept the default values for the policy rule fields.

   See *Policy Rule Fields* on page 293.

6. Select **File > Save**.

Policy Rule Fields

In Policy Editor, you can modify the following fields in the PolicyRule content pane.

Description

- Description of the policy rule.
- Value—Text
- Default—No value

Caption

- Short description of the policy rule.
- Value—Text
- Default—No value

Keywords

- Series of words that Policy Editor uses as a filter for keyword searches.
- Value—Text
- Default—No value

Precedence

- Precedence in which the policy rule is evaluated. Rules are evaluated from lowest to highest precedence value. Precedence is not a factor for JUNOS SCHEDULER and JUNOS POLICER policy rules. Precedence has meaning only if two rules have different classifiers and if those classifiers overlap. If this is the case and a packet is received that satisfies both classifiers, then only the action of the rule with the lower precedence value is performed. (See *Setting the Policy Rule Precedence* on page 292.)
- Value
  - For JUNOS and JUNOSe policies, integer in the range 0–32767
  - For PCMM policies, integer in the range 64–191
  - Parameter of type prPrecedence
- Default—100

Accounting

- Specifies whether accounting data is collected for the actions specified in the rule. (See *Collecting Accounting Statistics* on page 146.)
- Value—Checked or unchecked
- Default—Unchecked

Using the PolicyRule Summary Table

The PolicyRule pane contains a table that summarizes the conditions and actions that are within the policy rule. It contains one row for each action that the policy rule contains. The fields in the table vary depending on the type of conditions and actions that are contained in the policy rule. You can modify conditions and actions from within the summary table, or you can modify them by selecting objects from the navigation pane. The fields in the summary table are explained in Table 25 on page 287.

Configuring Classify-Traffic Conditions

You can create classify-traffic conditions in JUNOSe policy rules, in JUNOS ASP and JUNOS filter policy rules, and in PCMM policy rules. To create a classify-traffic condition:

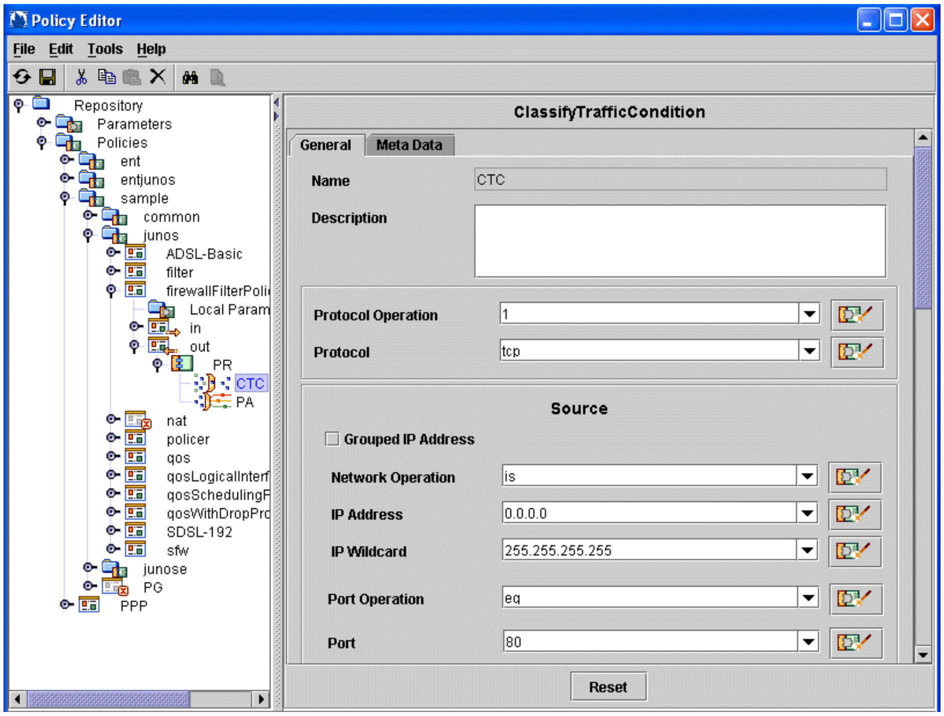
1. In the Policy Editor navigation pane, right-click a policy rule object, and select **New > Condition > ClassifyTrafficCondition**.

   The ClassifyTrafficCondition Name dialog box appears.

2. Enter a name, and click **OK**.

3. Select the new classify-traffic condition in the navigation pane.

   The new ClassifyTrafficCondition content pane appears.



Name: CTC

Description:

Protocol Operation: 1

Protocol: tcp

Source

☐ Grouped IP Address

Network Operation: is

IP Address: 0.0.0.0

IP Wildcard: 255.255.255.255

Port Operation: eq

Port: 80

4. Edit or accept the default values for the classify-traffic condition fields.

   See *Classify-Traffic Condition Fields* on page 298.

   For information about configuring port ranges for traffic classifiers, see *Specifying Port Access for Traffic Classification* on page 296.

5. Select **File > Save**.

If you are configuring classifiers for PCMM policies, you can specify whether the classifier will be used in a PCMM I02 or I03 network. By default, the software translates classify-traffic conditions into PCMM I02 classifiers.

- See *Specifying the PCMM Classifier Type* on page 296.

For JUNOSe policies, you can specify that the SAE expands the classifier into multiple classifiers before it installs the policy on the router.

- See *Enabling Expansion of JUNOSe Classify-Traffic Conditions* on page 218.

Specifying the PCMM Classifier Type

To specify which version of the PCMM classifiers that you are using, configure the Router.pcmm.disableI03policy property in the SAE property file.

See *Modifying the SAE Property File* in *SRC-PE Subscribers and Subscriptions Guide, Chapter 5, Configuring Subscriber–Related Properties on the SAE on a Solaris Platform*.

For more information about PCMM classifiers, see *PCMM Classifiers* on page 160.

Router.pcmm.disableI03policy

- Specifies whether or not the SAE sends classifiers to the router that comply with PCMM 103.
- Value
  - true—The SAE sends classifiers that comply with PCMM I02 to the router.
  - false—The SAE sends classifiers that comply with PCMM I03 to the router.
- Guidelines—Set this property to false if your network deployment has CMTS devices that do not support PCMM I03.
- Default—true

Specifying Port Access for Traffic Classification

In the SRC software, the manner in which you specify a range of port numbers greater than or less than a specific value in a traffic classifier is different than the way you define a range in the configuration on JUNOSe routers.

In Policy Editor in the ClassifyTrafficCondition content pane, you specify ranges by setting values in the Port Operation field.

For information about accessing the configuration in the ClassifyTrafficCondition content pane, see *Configuring Classify-Traffic Conditions* on page 295.

For information about the Port Operation and Port fields, see *Source and Destination Network Fields* on page 300.

To specify a range of port numbers greater or less than a specified value, you can:

- Define the full set of port numbers in the range to be allowed
- Define the full set of port numbers in the range not allowed

To configure port numbers greater than a defined value by specifying which values are allowed:

1. In the **Port Operation** field, enter **eq**.
2. In the **Port** field, enter the range of ports allowed.

   For example, to specify access to all port numbers greater than 10, specify 11..65535.

To configure port number greater than a define value by specifying which values are not allowed:

1. In the **Port Operation** field, enter **neq**.
2. In the **Port** field, enter the range of ports not allowed.

   For example, to specify access to all port numbers greater than 10, specify 1..9.

To configure port numbers less than a defined value by specifying which values are allowed:

1. In the **Port Operatio**n field, enter **eq**.
2. In the **Port** field, enter the range of ports.

   For example, to specify access to all port numbers less than 10, specify 1..9.

To configure port numbers less than a defined value by specifying which values are not allowed:

1. In the **Port Operation** field, enter **neq**.
2. In the **Port** field, enter the range of ports.

   For example, to specify access to all port numbers less than 10, specify 11..65535.

Classify-Traffic Condition Fields

In Policy Editor, you can modify the fields described in this section in the ClassifyTrafficCondition content pane.

The fields displayed in the ClassifyTrafficCondition pane change depending on the type of policy rule that holds the condition and on the type of protocol that you select in the Protocol field, as well as whether you select the Grouped IP Address and Raw check boxes. The classify-traffic condition fields are all described in the following sections:

- Direction Field on page 299
- Network Protocol Fields on page 299
- Source and Destination Network Fields on page 300
- Packet Length Field on page 303
- IP Protocol Fields on page 304
- ToS Byte on page 306
- TCP, ICMP, IGMP, and IPSec Protocol Fields on page 307
- JUNOS Filter Condition Fields on page 309
- Application Protocol Fields on page 311

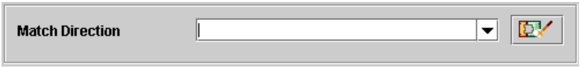
NOTE: PCMM classifiers support only the following fields:

- Source and destination IP addresses
- Network protocol
- Source or destination port
- Type-of-service (ToS) byte and ToS mask

The policy engine ignores all other values.

Direction Field

Appears only in JUNOS ASP policy rules.



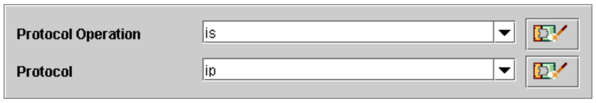
Match Direction

Match Direction

- Matches packets based on the direction of the packet flow. For stateful firewall actions, this value is used in place of the setting in the Applicability field of the policy list.
- Value
  - Predefined global parameter:
    - both—Valid only for stateful firewall actions
    - input
    - output
  - String expression
  - Parameter of type matchDirection
- Default—No value

Network Protocol Fields

This section of the pane specifies how protocols are matched.



Protocol Operation: is

Protocol: ip

Protocol Operation

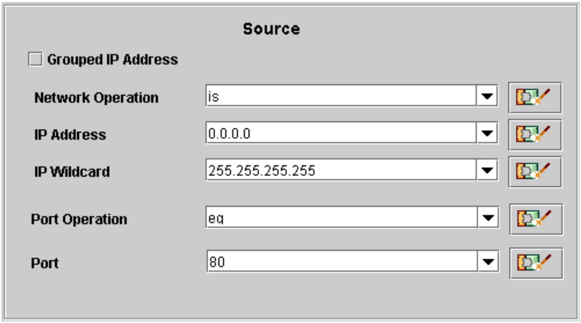
- Matches packets with the protocol that is either equal or not equal to the specified protocol.
- Value
  - Predefined global parameter:
    - is—Matches packets that are equal to the specified protocol
    - is_not—Matches any packets except those that are equal to the specified protocol
  - Boolean expression:
    - 1—is
    - 0—is_not
  - Parameter of type protocolOperation
- Default—1

Protocol

- Protocol matched by this classifier list.
- Value
  - Predefined global parameter—Select a protocol from the drop-down list
  - Protocol number in the range 0–257
  - For PCMM classifiers, there are two special protocol values:
    - 256 matches traffic that has any IP protocol value
    - 257 matches both TCP and UDP traffic
  - String expression
  - Parameter of type protocol

Source and Destination Network Fields

This section of the pane specifies source and destination networks. The Port Operation field appears only if you selected to match the TCP or UDP protocols. The Port field appears after you specify a port operation.


Source

☐ Grouped IP Address

Network Operation: is

IP Address: 0.0.0.0

IP Wildcard: 255.255.255.255

Port Operation: eq

Port: 80

Grouped IP Address

- If checked, the network operation, IP address, and IP wildcard attributes are grouped into one field called Network.
- For JUNOS ASP policy rules, you must check this box and enter IP addresses in prefix format; that is, IP address/prefix length.
- For JUNOSe IPv6 policy rules, you must check this box and enter IPv6 addresses with an IP mask in prefix length format. The network operation attribute is not supported.
- Value—Checked or unchecked
- Default—Unchecked

Network Operation

- Matches packets with an IP address that is either equal or not equal to the specified address and mask.
- Value
  - is—Matches the specified IP address and mask
  - not—Matches any IP address and mask except the specified address and mask
  - Parameter of type networkOperation
- Default—is

IP Address

- Number of the source or destination network or host.
- Value
  - IP address
  - Predefined global parameter:
    - ❑ gateway_ipAddress—IP address of the gateway as specified by the service object
    - ❑ interface_ipAddress—IP address of the router interface
    - ❑ service_ipAddress—IP address of the service as specified by the service object
    - ❑ user_ipAddress—IP address of the subscriber
    - ❑ virtual_ipAddress—Virtual portal address of the SSP that is used in redundant redirect server installations
  - Expression—For NAT actions, you can enter a range of addresses; for example, 10.10.13.1..10.10.13.100
  - Parameter of type address
- Default 0.0.0.0

IP Wildcard/IP Mask

- IP address mask applied to the IP address.
- Value
  - IP address mask
  - Predefined global parameter:
    - ❑ interface_ipMask—IP mask of the interface
    - ❑ service_ipMask—IP mask of the service as specified by the service object
    - ❑ user_ipMask—IP mask of the subscriber
  - Parameter of type addressMask
- Default—255.255.255.255

Network

- Network operation and IP subnets. This field appears only if the Grouped IP Address check box is checked.
- For JUNOS ASP policy rules, you must enter IP addresses in the format <address>/<prefix length>. The <address>/<mask> format is rejected by the router.
- For JUNOSe IPv6 policy rules, you must enter IPv6 addresses in the format <address>/<prefix length>. The network operation attribute is not supported.
- Value—Specify the subnet in one of the following formats:
  - [not] <address>/<mask> or <address>/<prefix length>
    - not is optional; include it to indicate that the condition matches every address that is not in the specified subnet
    - <address> and <mask> use dotted decimal notation
    - <prefix length> is a number in the range 0–32, and specifies how many of the first bits in the address specify the network
  - Expression—For example, pubIp/32

    where pubIp is a local address parameter and 32 is the prefix length
  - Parameter of type network
- Default—0.0.0.0/0.0.0.0

Port Operation

- Matches packets with a port that is either equal or not equal to the specified port.
- Value
  - Predefined global parameter:
    - eq—Matches packets that contain the specified port number
    - neq—Matches any packet except those that contain the specified port number
  - String
  - Parameter of type portOperation
- Guidelines—You can specify a range of port numbers as eq or neq to effectively specify a range greater than a specific value, or less than a specific value. For example to specify a port range greater than 49, you can specify eq for the port range 49..65536 or neq for the range 1..48.
- Default—No value

Port

- Source or destination ports.
- Value
    - Predefined global parameter:
        - service_port—Port of the service as specified by the service object
    - Integer in the range 0–65535
    - Expression—A range of port numbers; for example 10..20.

      Use a range of ports to specify port numbers that are greater than or less than a specified port number. For example:

        - To set a range of ports that is greater than 10, use 11..65535.
        - To set a range of ports that is less than 200, use 0..199.

      Note that PCMM 102 classifiers do not support port ranges. PCMM I03 classifiers do support port ranges.

    - Parameter of type port
- Guidelines—PCMM I02 does not support port ranges. If you are using PCMM 102 and you enter a range of port numbers, the software cannot translate the port, and it throws an exception.
- Default—No value

Packet Length Field

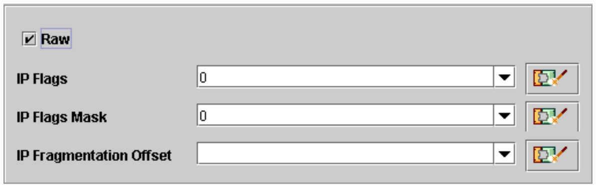
Matches packets according to packet length. This field appears only in JUNOS policy rules.

Packet Length (bytes)

- Matches on length of the packet. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead.
- Value
    - Number of bytes; all positive numbers and 0 are valid
    - Parameter of type packetLength
- Default—No value

IP Protocol Fields

In this section of the screen, you can configure values to match fields in the IP header.

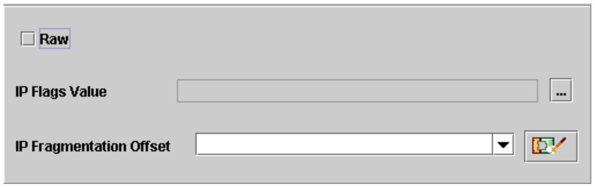


☑ Raw

IP Flags: 0

IP Flags Mask: 0

IP Fragmentation Offset:



☐ Raw

IP Flags Value:

IP Fragmentation Offset:

Raw

- Changes the view of the IP Flags section of the screen. You can configure IP flags and masks by number or by selecting values in a dialog box.
- Value—Checked or unchecked
- Default—Checked

IP Flags

- Value of the IP flags field in the IP header.
- Value
  - 0—Reserved
  - 1—Don’t-fragment
  - 2—More fragments
  - Numeric expression
  - Parameter of type ipFlags
- Default—0

IP Flags Mask

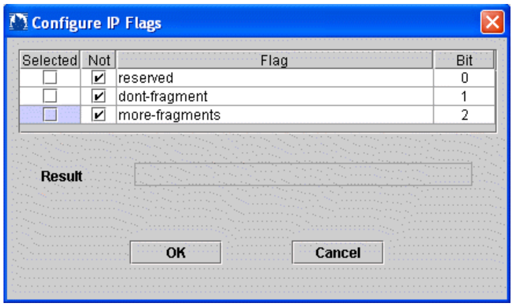
- Mask that is associated with the IP flag.
- Value
  - Integer in the range 0–7
  - Numeric expression
  - Parameter of type ipFlagsMask
- Default—0

IP Fragmentation Offset

- Value of the fragment offset field.
- Value
  - For JUNOSe routers:
    - eq 0—Equal to 0
    - eq 1—Equal to 1
    - gt 1—Greater than 1
    - any—Any value
  - For JUNOS routing platforms, integer in the range 0–8191
  - Numeric expression
  - Parameter of type fragOffset
- Default—No value

IP Flags Value

- If you deselect the Raw check box, Policy Editor displays the IP Flags Value field. Click ... next to the field to configure an IP flag. The Configure IP Flags dialog box appears.



Configure IP Flags

Selected	Not	Flag	Bit
☐	☑	reserved	0
☐	☑	dont-fragment	1
☐	☑	more-fragments	2

Result

To configure the IP flags:

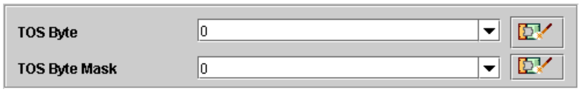
1. In the Selected column, select the IP flags that you want as part of the result string.
2. In the Not column, select the Not operator(s) that you want applied to the corresponding flag in the result string.

   You cannot check boxes in the Not column unless the check box in the corresponding Selected column is checked.
3. Click **OK**.

ToS Byte

Use this condition to define a particular traffic flow to the service's network for the DA IP field in the IP packet.

The CoS feature on JUNOS routing platforms supports DiffServ as well as six-bit IP header ToS byte settings. The DiffServ protocol uses the ToS byte in the IP header. The most significant six bits of this byte form the Differentiated Services code point (DSCP). The CoS feature uses DSCPs to determine the forwarding class associated with each packet. It also uses the ToS byte and ToS byte mask to determine IP precedence.



TOS Byte: 0

TOS Byte Mask: 0

TOS Byte

- Matches the value of the ToS byte in the IP packet header.
- Value
  - Integer in the range 0–255; uses whole 8 bits of the ToS byte
  - Numeric expression
  - Parameter of type tosByte
- Default—0

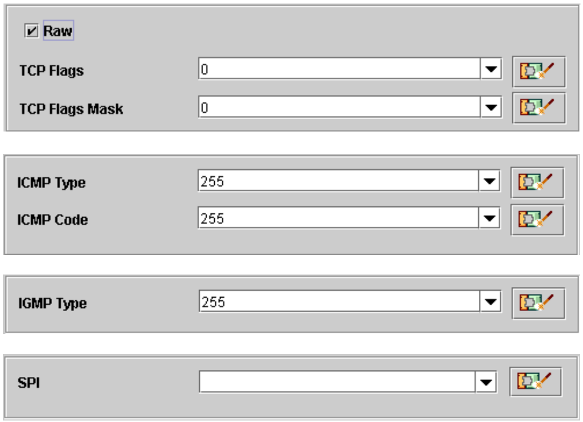
TOS Byte Mask

- Mask associated with the ToS byte.
- Value
  - Integer—Valid values are 0, 224, 252, 255
  - Numeric expression
  - Parameter of type tosByteMask
- Default—0

TCP, ICMP, IGMP, and IPSec Protocol Fields

If you specified the TCP, ICMP, IGMP, or the AH or ESP IPSec protocols, you can also specify the corresponding condition as shown in Figure 30.

Figure 30: Classify Conditions for TCP, ICMP, IGMP, and IPSec Protocols



☑ Raw

TCP Flags: 0

TCP Flags Mask: 0

ICMP Type: 255

ICMP Code: 255

IGMP Type: 255

SPI:

Raw

- Changes the view of the TCP section of the pane. You can configure TCP flags and masks by number or by selecting values in a dialog box.
- Value—Checked or unchecked
- Default—Checked

TCP Flags

- Value of the TCP flags field in the IP header.
- Value
  - Integer in the range 0–63
  - Numeric expression
  - Parameter of type tcpFlags
- Default—0

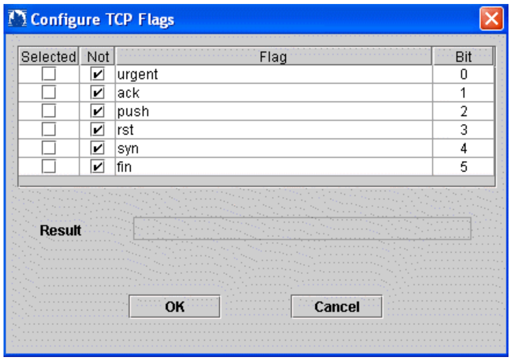
TCP Flags Mask

- Mask associated with TCP flags.
- Value
  - Integer in the range 0–63
  - Numeric expression
  - Parameter of type tcpFlagsMask
- Default—0

TCP Flags Value

- If you deselect the Raw check box, Policy Editor displays the IP Flags Value field. Click ... next to the field to configure a TCP flag.

  The Configure TCP Flags dialog box appears.



Selected	Not	Flag	Bit
☐	☑	urgent	0
☐	☑	ack	1
☐	☑	push	2
☐	☑	rst	3
☐	☑	syn	4
☐	☑	fin	5

To configure the TCP flags:

1. In the Selected column, select the TCP flags that you want as part of the result string.
2. In the Not column, select the Not operator(s) that you want applied to the corresponding flag in the result string.

   You cannot check boxes in the Not column unless the check box in the corresponding Selected column is checked.
3. Click **OK**.

ICMP Type

- Matches Internet Control Message Protocol (ICMP) packet type.
- Value
  - Integer in the range 0–255 that represents an ICMP packet type supported on the router or CMTS device
  - Numeric expression
  - Parameter of type icmpType
- Default—255

ICMP Code

- Matches ICMP code.
- Value
  - Integer in the range 0–255 that represents an ICMP code supported on the router or CMTS device
  - Numeric expression
  - Parameter of type icmpCode
- Default—255

IGMP Type

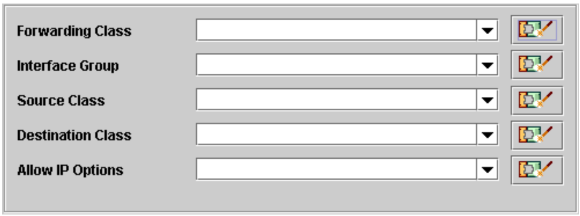
- IGMP packets that can be filtered by IGMP packet type or message name.
- Value
  - Integer in the range 0–255
  - Numeric expression
  - Parameter of type igmpType
- Default—255

SPI

- For IPSec classifiers, specifies the authentication header (AH) or the encapsulating security payload (ESP) security parameter index (SPI). This field appears only in JUNOS policy rules.
- Value
  - Integer in the range 0–255
  - Parameter of type ipSecSpi
- Default—No value

JUNOS Filter Condition Fields

The conditions described in this section appear only in JUNOS filter policy rules.



Forwarding Class

- Matches packets based on the name of a forwarding class.
- Value
  - String expression that matches a forwarding class on the router; for example, “assured-forwarding,” “best-effort,” “expedited-forwarding,” or “network-control”
  - Parameter of type forwardingClass
- Default—No value

Interface Group

- Matches packets based on the interface group on which the packet was received.
- Value
  - Integer in the range 0–4294967295
  - Numeric expression
  - Parameter of type interfaceGroup
- Default—No value

Source Class

- Matches packets based on source class. A source class is a set of source prefixes grouped together and given a class name. You would usually match source and destination classes for output firewall filters.
- Note that you cannot match on both source class and destination class at the same time. You must choose one or the other.
- Value
  - String expression that matches a source class that is configured on the router; for example, “gold-class”
  - Parameter of type trafficClassSpec
- Default—No value

Destination Class

- Matches packets based on destination class. A destination class is a set of destination prefixes grouped together and given a class name. You would usually match source and destination classes for output firewall filters.
- Note that you cannot match on both source class and destination class at the same time. You must choose one or the other.
- Value
  - String expression that matches a destination class that is configured on the router; for example, “gold-class”
  - Parameter of type trafficClassSpec
- Default—No value

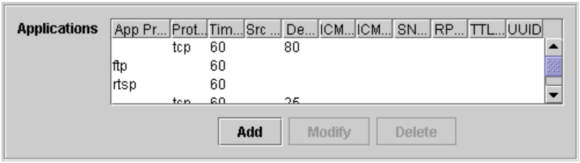
Allow IP Options

- Matches on IP options.
- Value
  - Numeric value of the IP option
  - String expression that matches a text synonym of an IP option on the router; for example, “loose-source-route,” “record-route,” “router-alert,” “strict-source-route,” or “timestamp”
  - Parameter of type allowIpOptions
- Default—No value

Application Protocol Fields

You can define application protocols for the stateful firewall and NAT services to use in match condition rules. An application protocol defines application parameters by using information from network layer 3 and above. Examples of such applications are FTP and H.323.

The ClassifyTrafficCondition pane displays a table with configured application protocol conditions.



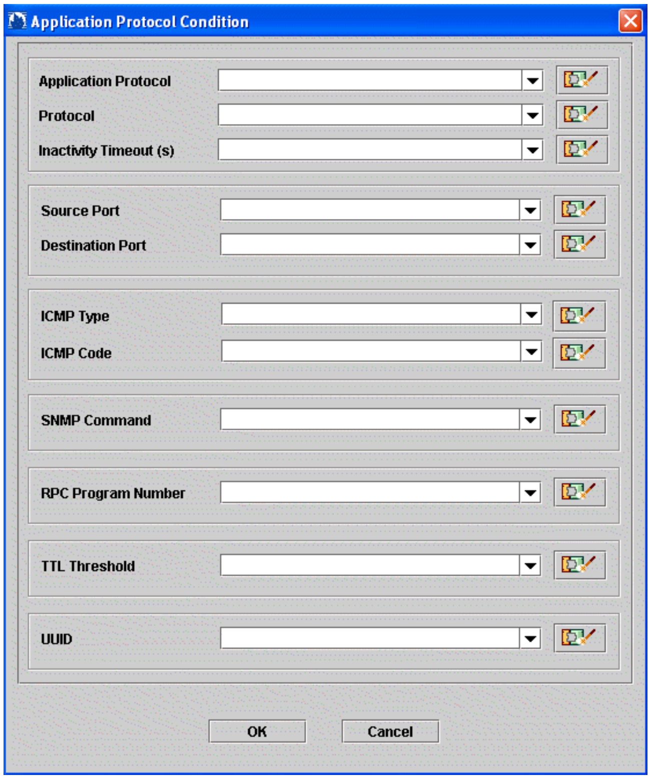
App Pr...	Prot...	Tim...	Src ...	De...	ICM...	ICM...	SN...	RP...	TTL...	UUID
	tcp	60		80						
ftp		60								
rtsp		60								
	tcp	60		25						

Configure the table as follows:

- To add an application protocol condition, click **Add**. Policy Editor displays the Application Protocol Condition dialog box.
- To modify a condition, select the condition, and click **Modify**. Policy Editor displays the Application Protocol Condition dialog box.
- To delete a condition, select the condition, and click **Delete**.

The Application Protocol Condition dialog box changes depending on the application protocol and protocol conditions that you select. Figure 31 shows an example of the dialog box with all possible fields.

Figure 31: Application Protocol Condition Dialog Box



Using Map Expressions in Application Protocol Conditions

The application protocol condition is a case in which you might use a map expression to define multiple attributes in one field—the Application Protocol field. Maps are a list of attributeName = value pairs separated by commas and enclosed in curly brackets. For example, the map {applicationProtocol = “ftp”, sourcePort = 123, inactivityTimeout = 60} supplies the application protocol, source port, and inactivity timeout in one field. “

Another map {applicationType = “tcp”, inactivityTimeout = 60, destinationPort = 80} supplies the protocol, inactivity timeout, and destination port.

You can enter the map expressions in the Application Protocol field.

You can also create a local parameter, add a map expression as the default value of the parameter, and then select the local parameter in the Application Protocol field.

Filling in Application Protocol Fields

This section describes the fields in the Application Protocol Condition dialog box.

Application Protocol

- Application protocol to match.
- Value
  - Predefined global parameter—Select a protocol from the pull-down list
  - String expression that matches an application protocol name supported on the router
  - Map expression—See *Using Map Expressions in Application Protocol Conditions* on page 312
  - Parameter of type applicationProtocol
- Default—No value

Protocol

- Network protocol to match.
- Value
  - Predefined global parameter—Select a protocol from the drop-down list
  - Integer in the range 0–255
  - Numeric expression
  - Parameter of type protocol
- Default—No value

Inactivity Timeout (s)

- Length of time the application is inactive before it times out.
- Value
  - Number of seconds in the range 4–65535
  - Numeric expression
  - Parameter of type timeout
- Default—Unspecified; the router's default value is used

Source Port

- TCP or UDP source port.
- Value
  - Predefined parameter:
    - service_port—Service port as specified by the service object
  - Integer in the range 0–65535
  - String expression that matches a port name supported on the router; for example, “http”
  - Parameter of type port
- Default—No value

Destination Port

- TCP or UDP destination port.
- Value
  - Predefined parameter:
    - service_port—Service port as specified by the service object
  - Integer in the range 0–65535
  - String expression that matches a port name or number supported on the router; for example, “http”
  - Parameter of type port
- Default—No value

ICMP Type

- ICMP packet type.
- Value
  - Integer in the range 0–255 that represents an ICMP packet type supported on the router
  - Numeric expression
  - Parameter of type icmpType
- Default—No value

ICMP Code

- ICMP code.
- Value
  - Integer in the range 0–255 that represents an ICMP code supported on the router
  - Numeric expression
  - Parameter of type icmpCode
- Default—No value

SNMP Command

- SNMP command for packet matching.
- Value
  - Predefined parameter:
    - ☐ get
    - ☐ get_next
    - ☐ set
    - ☐ trap
  - String expression that matches an SNMP command supported on the router
  - Parameter of type snmpCommand
- Default—No value

RPC Program Number

- For the remote procedure call (RPC) application protocol, specifies an RPC program number.
- Value
  - Integer—RPC or DCE program number in the range 100000–400000
  - Numeric expression
  - Parameter of type rpcProgramNumber
- Default—No value

TTL Threshold

- For the traceroute application protocol, specifies the traceroute time-to-live (TTL) threshold value. This value sets the acceptable level of network penetration for trace routing.
- Value
  - Integer in the range 0–255
  - Numeric expression
  - Parameter of type traceRouteTtlThreshold
- Default—No value

UUID

- For the DCE RPC application protocol, specifies the universal unique identifier (UUID).

  For information about UUIDs, see http://www.opengroup.org/onlinepubs/9629399/apdxa.htm.
- Value
  - Hexadecimal value
  - Numeric expression
  - Parameter of type dceRpcUuid
- Default—dceRpcUuid

Configuring QoS Conditions

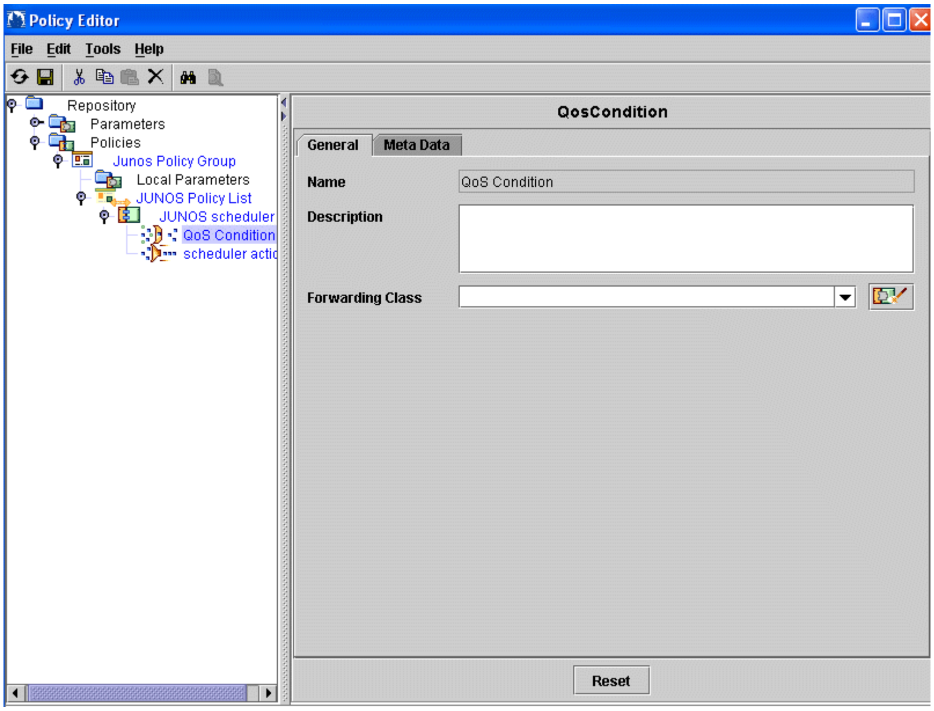
You can create QoS conditions within JUNOS scheduler policy rules. To create a QoS condition:

1. In the navigation pane, right-click a JUNOS scheduler policy rule object, and select **New > Condition > QosCondition**.

   The QosConditon Name dialog box appears.
2. Enter a name, and click **OK**.

3. Select the new QoS condition in the navigation pane.

   The QosConditon pane appears.



Name: QoS Condition

Description:

Forwarding Class:

4. Edit or accept the default values for the QoS condition fields.

   See *QoS Condition Fields* on page 317.

5. Select **File** > **Save**.

QoS Condition Fields

In Policy Editor, you can modify the following fields in the QoSCondition content pane.

Description

- Description of the QoS condition.
- Value—Text
- Default—No value

Forwarding Class

- Matches packets based on forwarding class.
- Value
  - String expression that matches forwarding classes that are configured on the router; for example, “assured-forwarding,” “best-effort,” “expedited-forwarding,” or “network-control”
  - Parameter of type forwardingClass
- Default—No value

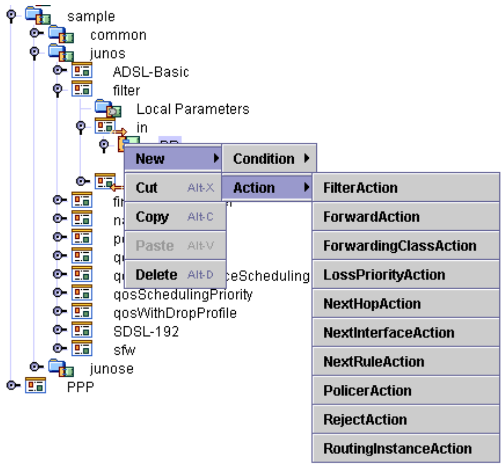
Configuring Actions

Actions define the action taken on packets that match conditions in a policy rule. You create actions within policy rules. The type of action that you can create depends on the type of policy rule. See *Supported Conditions and Actions* on page 150.

Adding Actions

To add an action:

1. In the navigation pane, right-click a policy rule.
2. Click **New > Action,** and select an action from the list.



   The <Action> Name dialog box appears.

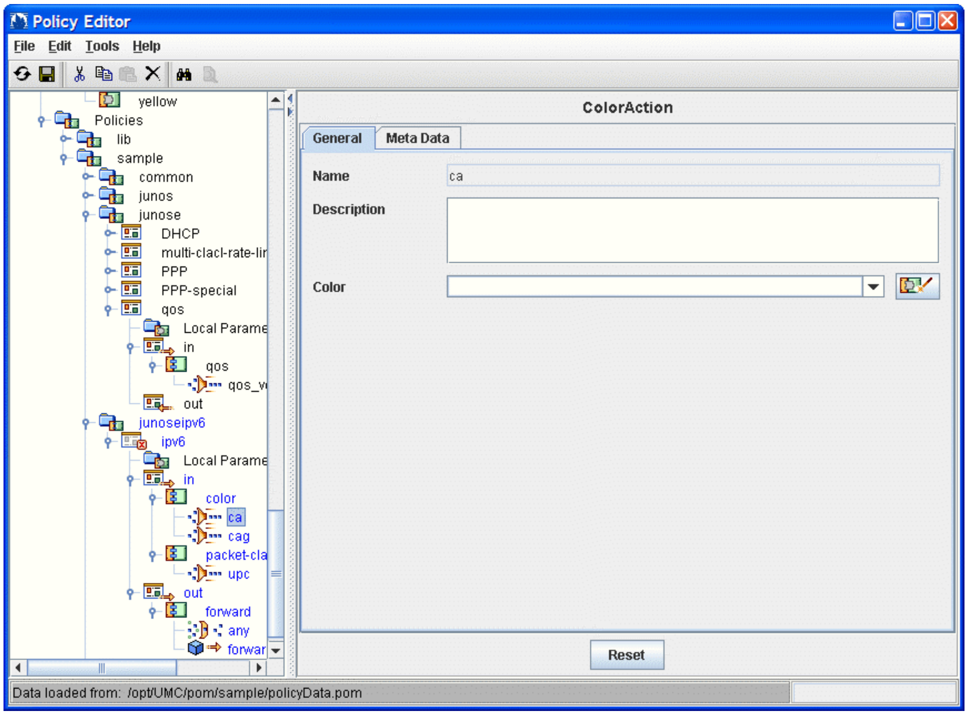
3. Enter a name, and click **OK**.
4. Select the new action in the navigation pane.

5. Configure the action as described in the following sections:

   - Configuring Color Actions on page 320
   - Configuring DOCSIS Actions on page 321
   - Configuring Filter Actions on page 325
   - Configuring FlowSpec Actions on page 326
   - Configuring Forward Actions on page 329
   - Configuring Forwarding Class Actions on page 330
   - Configuring GateSpec Actions on page 331
   - Configuring Loss Priority Actions on page 333
   - Configuring Mark Actions on page 334
   - Configuring NAT Actions on page 335
   - Configuring Next-Hop Actions on page 337
   - Configuring Next-Interface Actions on page 339
   - Configuring Next-Rule Actions on page 341
   - Configuring Policer Actions on page 342
   - Configuring QoS Profile Attachment Actions on page 344
   - Configuring Rate-Limit Actions on page 346
   - Configuring Reject Actions on page 350
   - Configuring Routing Instance Actions on page 351
   - Configuring Scheduler Actions on page 352
   - Configuring Service Class Name Actions on page 358
   - Configuring Stateful Firewall Actions on page 359
   - Configuring Traffic-Class Actions on page 360
   - Configuring Traffic-Mirror Actions on page 361
   - Configuring Traffic-Shape Actions on page 363
   - Configuring User Packet Class Actions on page 364

Configuring Color Actions

You can configure color actions for JUNOSe IPv6 policy rules.



Name: ca

Color:

Data loaded from: /opt/UMC/pom/sample/policyData.pom

Description

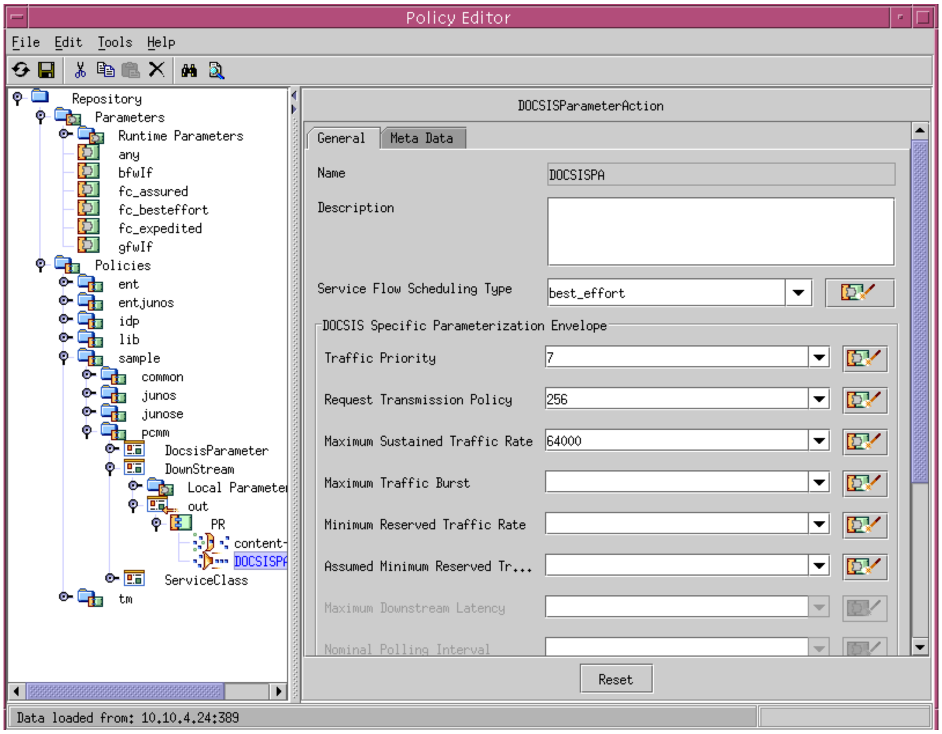
- Description of the action.
- Value—Text
- Default—No value

Color

- Color that is applied to a packet when it passes through the router.
- Value
  - Integer in the range 1–3
    - 1 is green; indicating a low drop preference
    - 2 is yellow; indicating a medium drop preference
    - 3 is red; indicating a high drop preference
  - Parameter of type color
- Default—No value

Configuring DOCSIS Actions

You can configure Data over Cable Service Interface Specifications (DOCSIS) actions for *PacketCable Multimedia Specification* (PCMM) policy rules.



Name: DOCSISPA
Description:
Service Flow Scheduling Type: best_effort
Traffic Priority: 7
Request Transmission Policy: 256
Maximum Sustained Traffic Rate: 64000
Maximum Traffic Burst:
Minimum Reserved Traffic Rate:
Assumed Minimum Reserved Tr...:
Maximum Downstream Latency:
Nominal Polling Interval:

Data loaded from: 10.10.4.24:389

Service Flow Scheduling Type

- Scheduling types for service flows. The scheduling type that you select determines which fields are available in the DOCSIS action.
- Value
  - Predefined global parameter. For information about each DOCSIS service scheduling type, see Table 12 on page 157.
    - best_effort
    - unsolicited_grant
    - down_stream
    - unsolicited_grant_with_activity_detection
    - real_time
    - non_real_time
  - Parameter of type trafficProfileType
- Default—No value

Traffic Priority

- Priority for the service flow. If two traffic flows are identical in all QoS parameters except priority, the higher priority service flow is given preference.
- Value
  - Number in the range 0–7, where 0 is the lowest priority and 7 is the highest priority
  - Parameter of type trafficPriority
- Default—No value

Request Transmission Policy

- Interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow, and specifies whether requests can be piggybacked with data. Also, for data packets transmitted on this service flow, specifies whether packets can be concatenated, fragmented, or have their payload headers suppressed. For UGS service flows, this field also specifies how to treat packets that do not fit into the UGS grant.
- Value
  - 4-byte bit field; the valid range is 0–511
  - Parameter of type requestTransmissionPolicy
- Default—No value

Maximum Sustained Traffic Rate

- Maximum sustained rate at which traffic can operate over the service flow.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's DOCSIS interface
  - Number of bits per second in the range 0–4294967295
  - Numeric expression
  - Parameter of type rate
- Default—No value

Maximum Traffic Burst

- Maximum burst size for the service flow. This parameter has no effect unless you configure a nonzero value for the maximum traffic rate.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's DOCSIS interface
  - Number of bytes in the range 1522–4294967295
  - Numeric expression
  - Parameter of type burst
- Default—No value

Minimum Reserved Traffic Rate

- Guaranteed minimum rate that is reserved for the service flow.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's DOCSIS interface
  - Number of bits per second in the range 0–4294967295; a value of 0 means that no bandwidth is reserved for the service flow
  - Numeric expression
  - Parameter of type rate
- Default—No value

Assumed Minimum Reserved Traffic Rate Packet Size

- Assumed minimum packet size for which the minimum reserved traffic rate is provided. If a packet is smaller than the assumed minimum packet size, the software treats the packet as if its size is equal to the value specified in this field.
- Value
  - Number of bytes in the range 0–65535
  - Numeric expression
  - Parameter of type packetLength
- Default—No value

Maximum Downstream Latency

- Maximum latency for downstream service flows. It is the maximum latency for a packet that passes through the CMTS device, from the time that the CMTS device's network side interface receives the packet until the CMTS device forwards the packet on its radio frequency (RF) interface.
- Value
  - Number of microseconds in the range 0–4294967295
  - Numeric expression
  - Parameter of type maxLatency
- Default—No value

Nominal Polling Interval

- Nominal interval between successive unicast request opportunities for this service flow.
- Value
  - Number of microseconds in the range 0–4294967295
  - Numeric expression
  - Parameter of type interval
- Default—No value

Tolerated Poll Jitter

- Maximum amount of time that unicast request intervals can be delayed beyond the nominal polling interval. Delaying requests allows the service flow scheduler to fit as much data as possible in an upstream packet, thereby reducing fragmentation.
- Value
  - Number of microseconds in the range 0–4294967295
  - Numeric expression
  - Parameter of type jitter
- Default—No value

Unsolicited Grant Size

- Size of the individual data grants provided to the service flow.
- Value
  - Number of bytes in the range 0–65535
  - Numeric expression
  - Parameter of type grantSize
- Default—No value

Grants Per Interval

- Actual number of data grants given to the service flow during each nominal grant interval.
- Value
  - Integer in the range 0—127
  - Numeric expression
  - Parameter of type interval
- Default—No value

Nominal Grant Interval

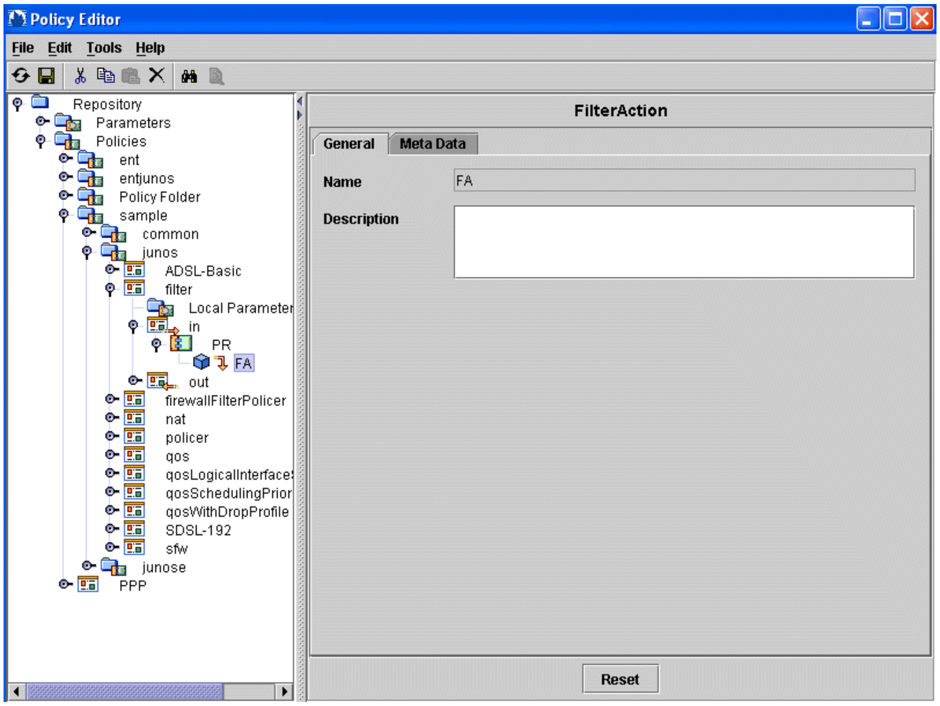
- Nominal interval between successive unsolicited data grant opportunities for this service flow.
- Value
  - Number of microseconds in the range 0–4294967295
  - Numeric expression
  - Parameter of type interval
- Default—No value

Tolerated Grant Jitter

- Maximum amount of time that the transmission opportunities can be delayed beyond the nominal grant interval.
- Value
  - Number of microseconds in the range 0–4294967295
  - Numeric expression
  - Parameter of type jitter
- Guidelines—A jitter buffer can stop latency, but an improperly sized buffer can cause additional latency.
- Default—No value

Configuring Filter Actions

Use this action to discard packets. You can configure filter actions for JUNOS filters and JUNOSe policy rules.



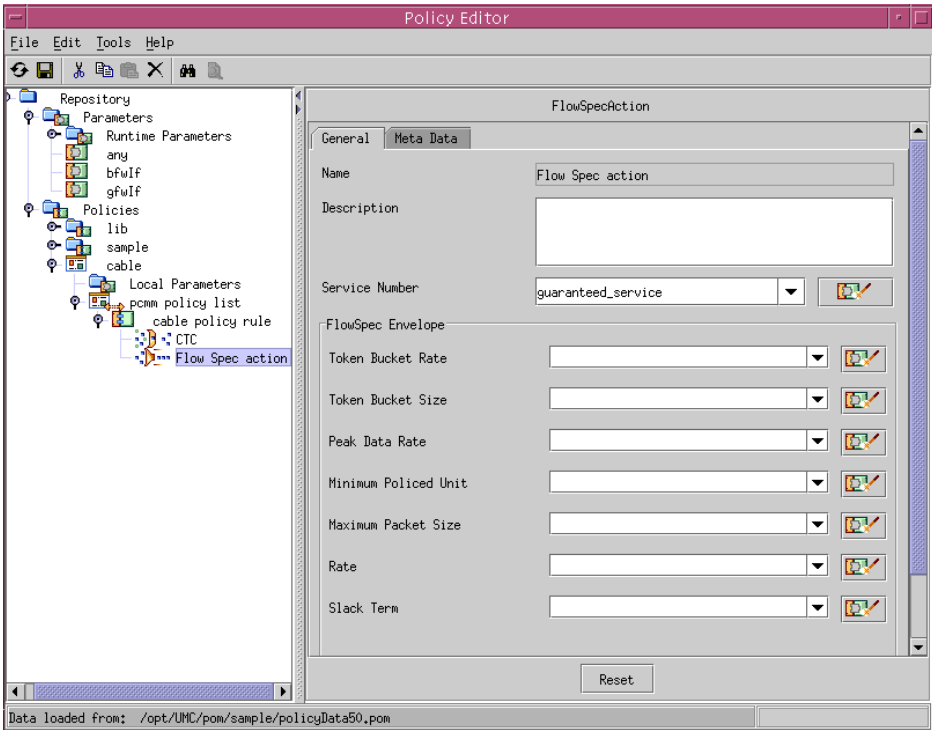
Name: FA

Description

- Description of the action.
- Value—Text
- Default—No value

Configuring FlowSpec Actions

You can configure FlowSpec actions for PCMM policy rules.



Name: Flow Spec action
Description:
Service Number: guaranteed_service
Token Bucket Rate:
Token Bucket Size:
Peak Data Rate:
Minimum Policed Unit:
Maximum Packet Size:
Rate:
Slack Term:

Data loaded from: /opt/UMC/pom/sample/policyData50.pom

Service Number

- Type of FlowSpec service.
- Value
  - Predefined global parameter:
    - controlled_load_service—Provides minimum bandwidth guarantees, but not latency and delay guarantees. A controlled-load service can contain only traffic specification (TSpec) token-bucket parameters, and not service request specification (RSpec) parameters.
    - guaranteed_service—Provides both bandwidth and latency and delay guarantees. A guaranteed service can contain both TSpec and RSpec parameters.
  - Parameter of type serviceNumber
- Default—No value

Token Bucket Rate

- Guaranteed minimum rate that is reserved for the service flow. Token bucket rate is a TSpec parameter.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's DOCSIS interface
  - Number of bits per second in the range 0–4294967295
  - Numeric expression
  - Parameter of type rate
- Default—No value

Token Bucket Size

- Maximum burst size for the service flow. Token bucket size is a TSpec parameter.
- Value
  - Number of bits per second in the range 1522–4294967295
  - Numeric expression
  - Parameter of type tokenBucketSize
- Guidelines—This parameter has no effect unless you configure a nonzero value for the maximum traffic rate.
- Default—No value

Peak Data Rate

- Amount of bandwidth over the committed rate that is allocated to accommodate excess traffic flow over the committed rate. Peak data rate is a TSpec parameter.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's DOCSIS interface
  - Number of bits per second in the range 0–4294967295
  - Numeric expression
  - Parameter of type rate
- Default—No value

Minimum Policed Unit

- Assumed minimum-reserved-rate packet size. If a packet is smaller than the minimum policed unit, the software treats the packet as if its size is equal to the value specified in this field. Minimum policed unit is a TSpec parameter.
- Value
  - Number of bytes in the range 0–65535
  - Numeric expression
  - Parameter of type policedUnit
- Default—No value

Maximum Packet Size

- Maximum packet size for the FlowSpec. Maximum packet size is a TSpec parameter.
- Value
  - Number of bytes in the range 0–4294967295
  - Numeric expression
  - Parameter of type packetLength
- Default—No value

Rate

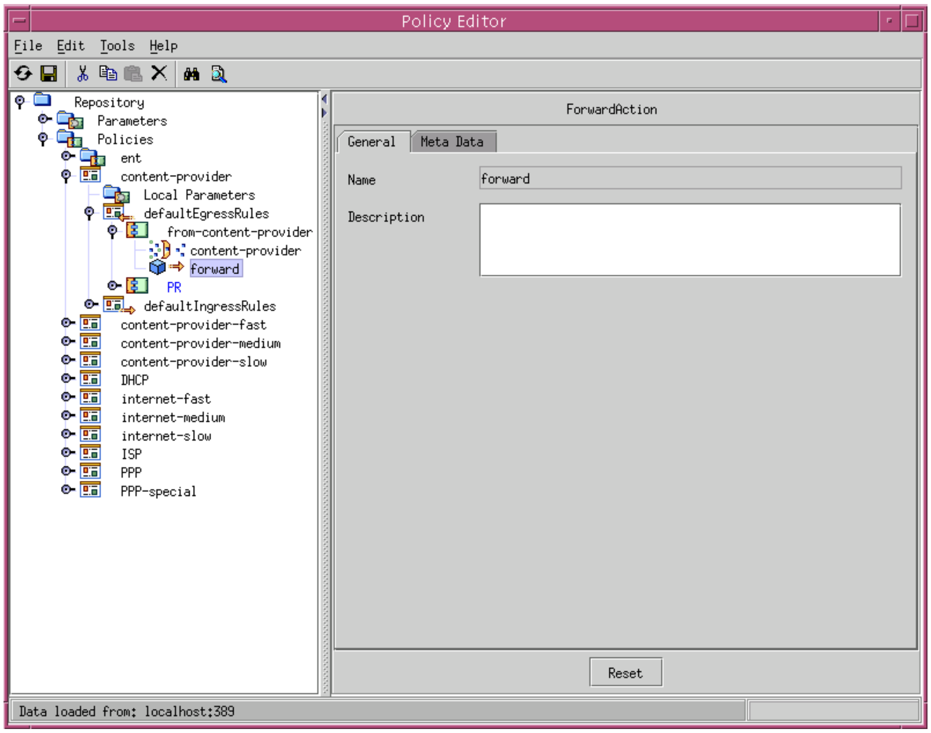
- Average rate. Rate is an RSpec parameter.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's DOCSIS interface
  - Number of bits per second in the range 0–4294967295
  - Numeric expression
  - Parameter of type rate
- Default—No value

Slack Term

- Amount of slack in the bandwidth reservation that can be used without redefining the reservation. Slack is the difference between the desired delay and the actual delay obtained with the current bandwidth reservation. It allows some flexibility in bandwidth reservations. Slack term is an RSpec parameter.
- Value
  - Integer in the range 0–4294967295
  - Numeric expression
  - Parameter of type slackTerm
- Default—No value

Configuring Forward Actions

Use this action to forward packets, such as packets that are sent by means of a routing table. You can configure forward actions for JUNOS filters and JUNOSe policy rules.



Name: forward

Description:

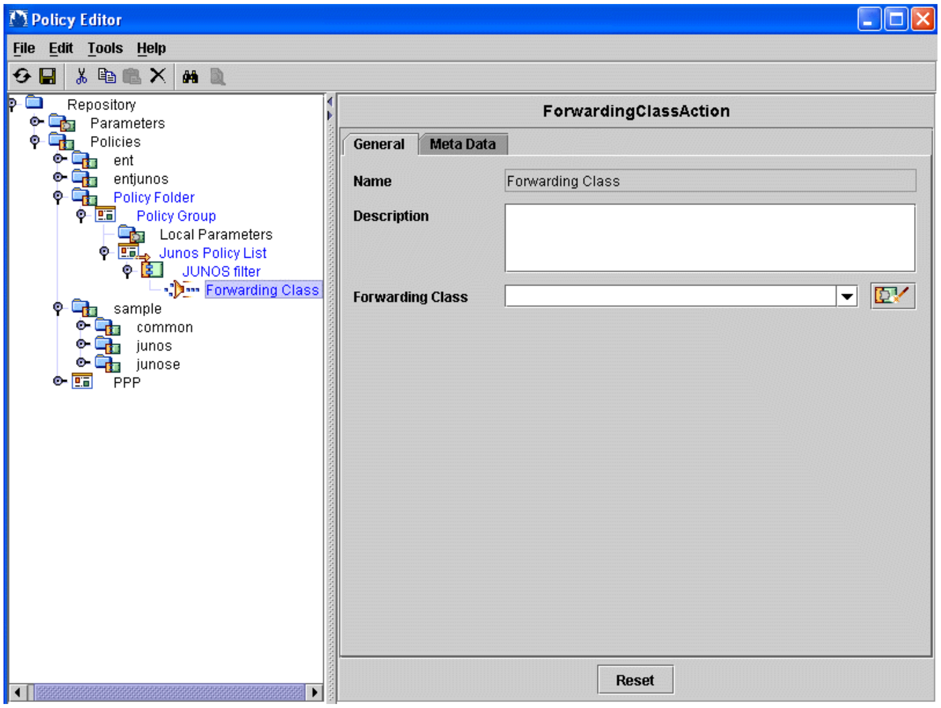
Data loaded from: localhost:389

Description

- Description of the action.
- Value—Text
- Default—No value

Configuring Forwarding Class Actions

You can configure forwarding class actions for JUNOS filter policy rules. The forwarding class action causes the router to assign a forwarding class to packets that match the associated classify-traffic condition.



Name: Forwarding Class

Description:

Forwarding Class:

Description

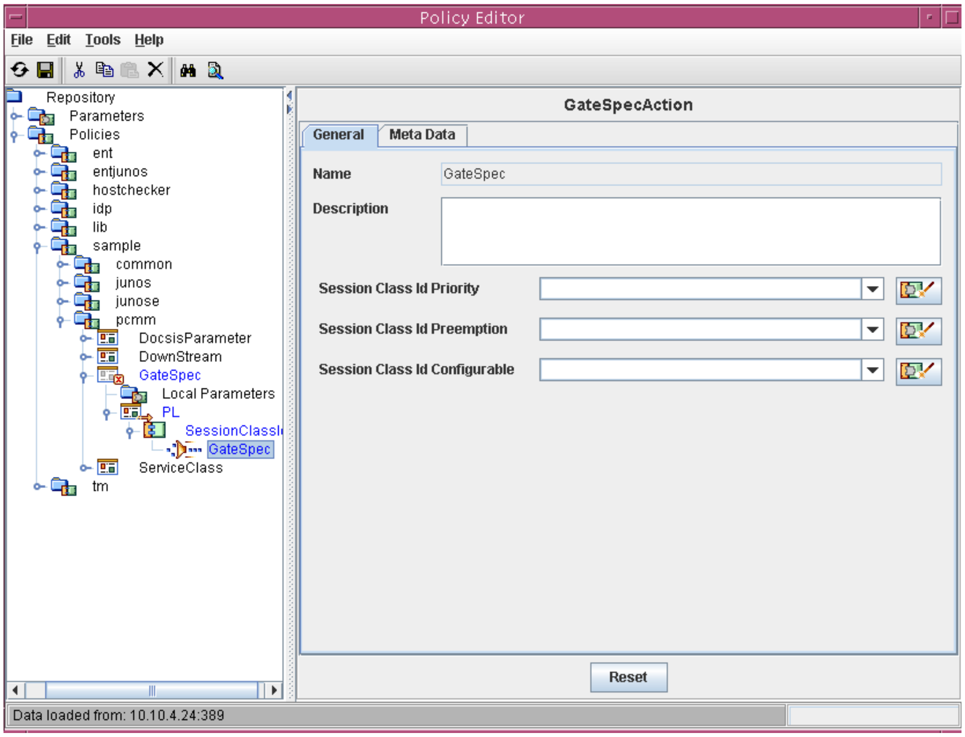
- Description of the action.
- Value—Text
- Default—No value

Forwarding Class

- Name of the forwarding class assigned to packets.
- Value
  - String expression that matches a forwarding class that is configured on the router; for example, “assured-forwarding,” “best-effort,” “expedited-forwarding,” or “network-control”
  - Parameter of type forwardingClass
- Default—No value

Configuring GateSpec Actions

You can configure GateSpec actions for PCMM policy rules. See *Session Class ID* on page 159 for more information.



Name GateSpec

Data loaded from: 10.10.4.24:389

Description

- Description of the action.
- Value—Text
- Default—No value

Session Class Id Priority

- Priority bits in the session class ID. The priority field describes the relative importance of the session as compared with other sessions generated by the same policy decision point.
- Value
    - Number in the range 0–7, where 0 is low priority and 7 is high priority
    - String expression
    - Parameter of type sessionClassIdPriority
- Default—No value

Session Class Id Preemption

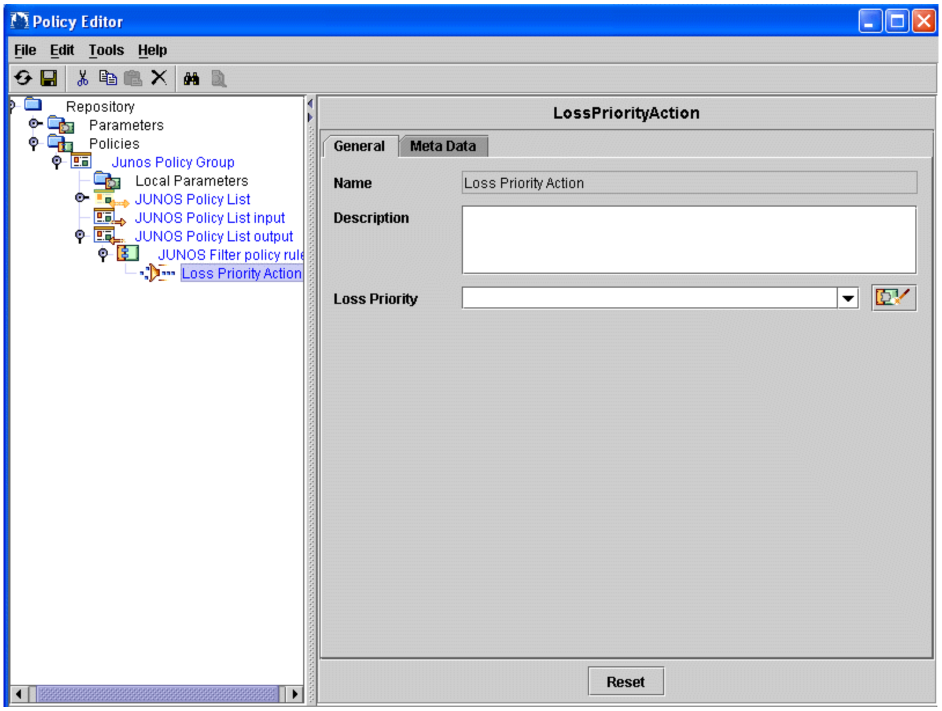
- Preemption bit in the session class ID. Use the preemption bit to allocate bandwidth to lower-priority sessions.
- Value
    - Number in the range 0–1
        - 0—Enables preemption
        - 1—Disables preemption
    - String expression
    - Parameter of type sessionClassIdPreemption
- Default—No value

Session Class Id Configurable

- Configurable bit in the session class ID. Application managers that provide novel services may use this value to specify new session classes. Use this field if your policy server supports configurable policies based on this value or if your CMTS device implements a novel session class based on this value.
- Value
    - Number in the range 0–15
    - String expression
    - Parameter of type sessionClassIdConfigurable
- Default—No value

Configuring Loss Priority Actions

You can configure loss priority actions for JUNOS filter policy rules. The loss priority action causes the router to assign a packet loss priority to packets that match the associated classify-traffic condition.



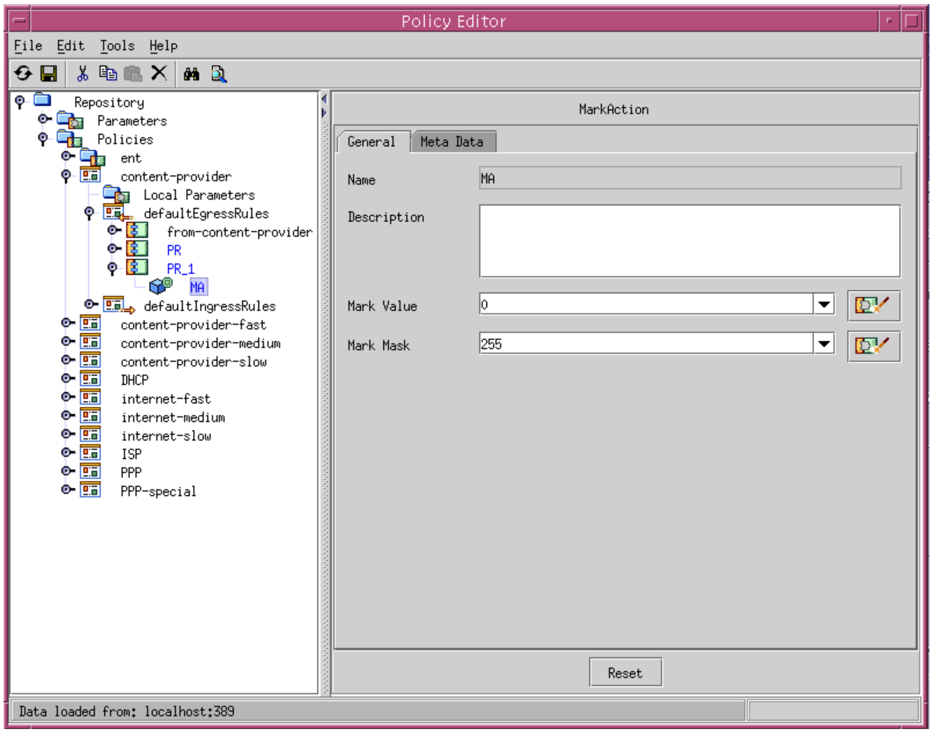
Name: Loss Priority Action

Loss Priority

- Sets the packet loss priority (PLP).
- Value
  - Predefined global parameter:
    - any_priority—Do not select this value for loss priority. This parameter appears in this field because it is a global packetLossPriority parameter. However, in this context, a value of any_priority is not valid.
    - high_priority—Sets the PLP to high
    - low_priority—Sets the PLP to low
  - String expression that matches valid values on the router; for example, “high” or “low”
  - Parameter of type packetLossPriority
- Default—No value

Configuring Mark Actions

Use this action to mark packets. You can configure mark actions for JUNOSe and PCMM policy rules.



Name: MA

Mark Value: 0

Mark Mask: 255

Data loaded from: localhost:389

Description

- Description of the action.
- Value—Text
- Default—No value

Mark Value

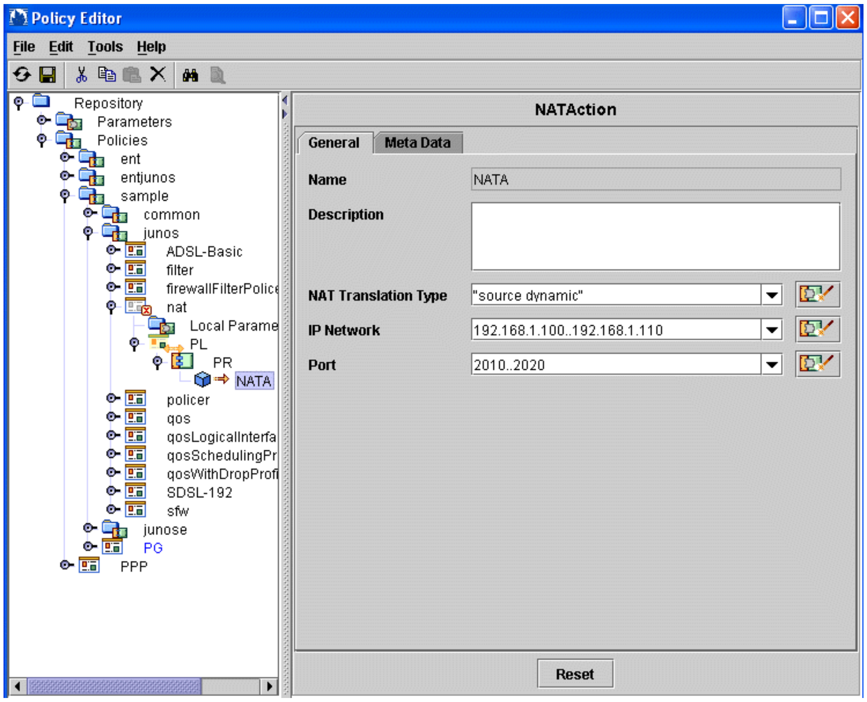
- For IPv4 packets, sets the ToS field in the IP header. For IPv6 packets, sets the traffic-class field in the IP header
- Value
    - Integer in the range 0–255
    - Parameter of type tosByte
- Default—0

Mark Mask

- Mask associated with the mark value.
- Value
  - Integer in the range 0–255
  - Parameter of type tosByteMask
- Default—255

Configuring NAT Actions

You can configure NAT actions for JUNOS ASP policy rules.



Name: NATA

Description:

NAT Translation Type: "source dynamic"

IP Network: 192.168.1.100..192.168.1.110

Port: 2010..2020

NAT Translation Type

- Type of network address translation that is used.
- Value
  - String expression that matches a NAT type on the router; for example:
    - “destination static”—Implements address translation for destination traffic without port translation; makes selected private servers accessible
    - “source dynamic”—Implements address translation for source traffic with port translation
    - “source static”—Implements address translation for source traffic without port mapping
  - Parameter of type natTranslationType
- Default—No value

IP Network

- IP address ranges.
- Value
  - An IP address with or without a prefix
  - Expression that indicates an address range (low to high); for example, 92.168.1.100..192.168.1.110; address ranges are limited to 32 addresses
  - Predefined global parameter:
    - any—Do not select this value for IP network. This parameter appears in this field because it is a global network parameter. However, in this context, a value of any is not valid.
  - Parameter of type network
  - Parameter of type address/prefix; for example, pubIp/32

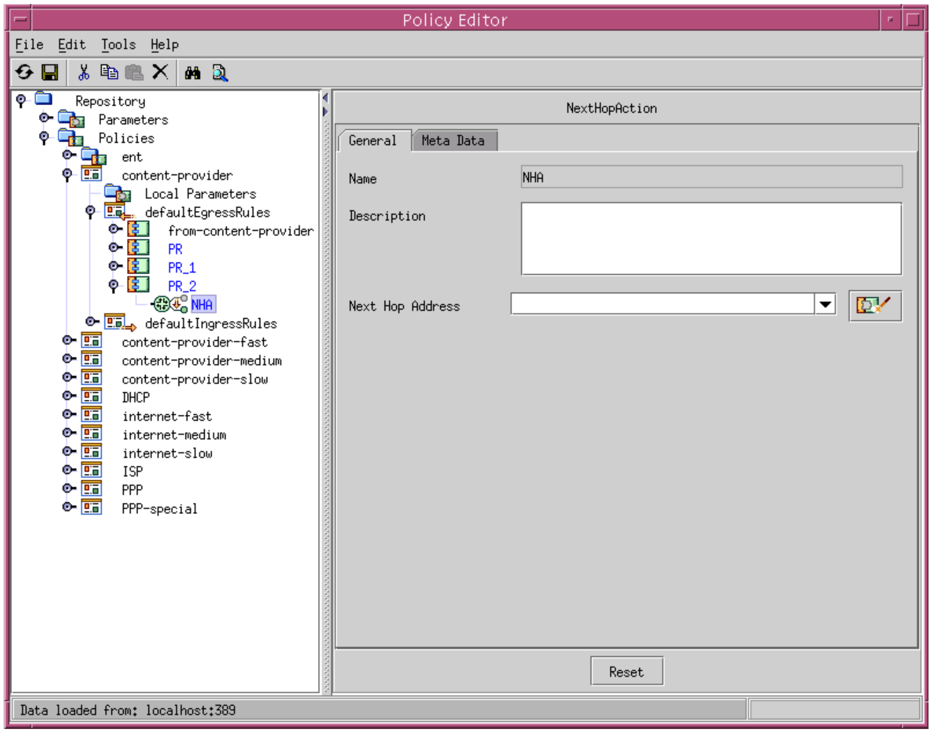
    where pubIp is a local address parameter and 32 is the prefix length
- Default—0.0.0.0/0.0.0.0

Port

- Port range to restrict port translation when NAT is configured in dynamic-source mode.
- Value
  - Predefined global parameter:
    - service_port—Port of the service as specified by the service object
  - Integer in the range 0–64000
  - Numeric expression that indicates a range of ports; for example, 2010..2020
  - 0..65535—Provides the same effect as the automatic option. JUNOS routing platforms support a port option called automatic, which means that it is a router-assigned port.
  - Parameter of type port
- Default—No value

Configuring Next-Hop Actions

Use this action for the ingress side of the interface to specify the next IP address where the classified packets should go. You can configure next-hop actions for JUNOS filters and JUNOSe policy rules.



Name NHA

Data loaded from: localhost:389

Description

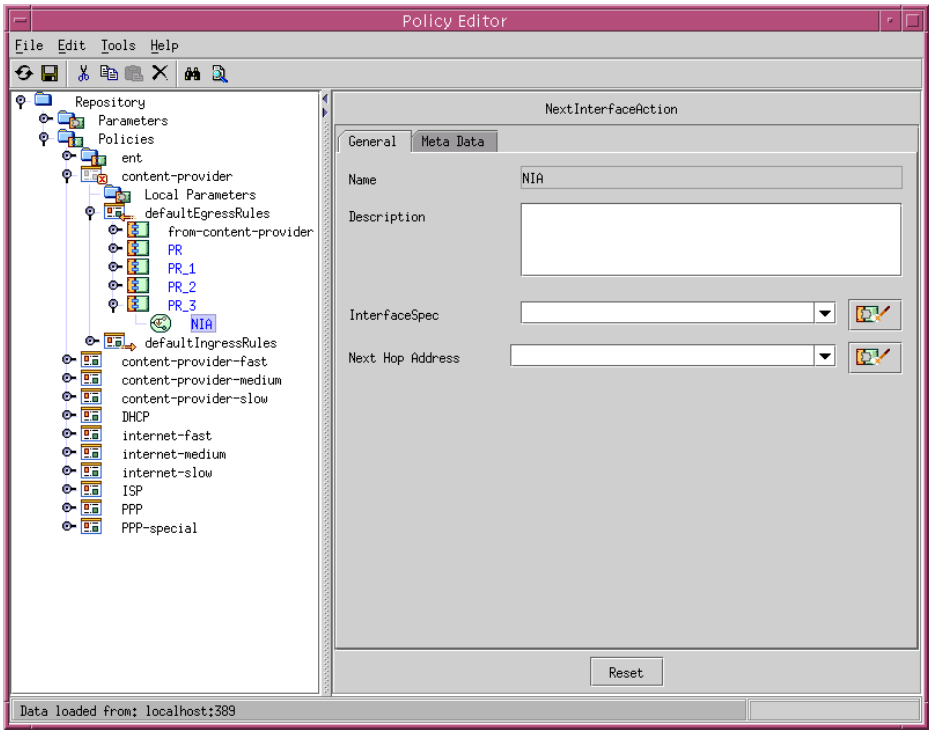
- Description of the action.
- Value—Text
- Default—No value

Next Hop Address

- Next IP address where the classified packets should go.
- Value
  - IP address
  - Predefined global parameter:
    - gateway_ipAddress—IP address of the gateway as specified by the service object
    - interface_ipAddress—IP address of the router interface
    - service_ipAddress—IP address of the service as specified by the service object
    - user_ipAddress—IP address of the subscriber
    - virtual_ipAddress—Virtual portal address of the SSP that is used in redundant redirect server installations
  - Parameter of type address
- Default—0

Configuring Next-Interface Actions

Use this action to forward packets to a particular interface and/or a next-hop address. You can configure next-interface actions for JUNOS filters and JUNOSe policy rules. On JUNOSe routers, you can use this action for both ingress and egress parts of the interface.



Name: NIA

Data loaded from: localhost:389

Description

- Description that is inherited from the managed element.
- Value—Text description
- Default—No value

InterfaceSpec

- IP interface to be used as the next interface for packets.
- Value
  - For JUNOSe interfaces:
    - Enter interface specifiers in the format:

      ‘<type of specifier> = <value>’

      where< type of specifier> is the interface name, alias, description, or uid

      For example: name=’fastEthernet3/0’

      For lists of valid interface specifiers for JUNOSe routers, see *Interface Types and Specifiers* in the *JUNOSe Command Reference Guides*.
  - For JUNOS interfaces:
    - Enter interface specifiers in the format:

      ‘name= <mediatype>-<slot>/<pic>/<port>.<unit>’

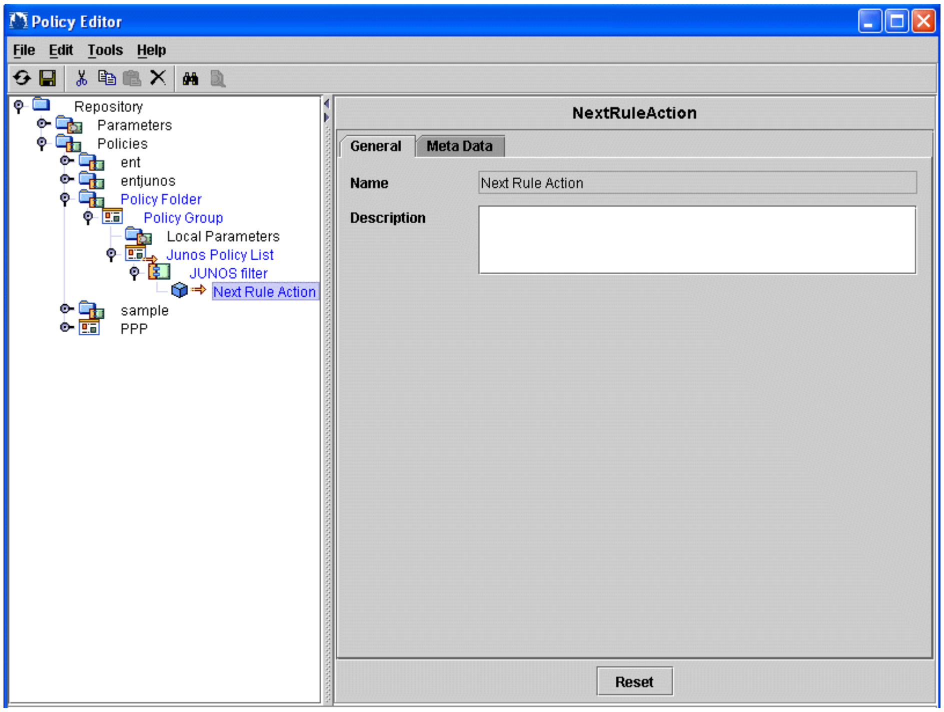
      For example: ‘name=AT-0/1/0.0’
  - Parameter of type interfaceSpec
- Default—No value

Next Hop Address

- Next IP address where the classified packets should go. This field is available only in JUNOSe policy rules.
- Value
  - IP address
  - Predefined global parameter:
    - gateway_ipAddress—IP address of the gateway as specified by the service object
    - interface_ipAddress—IP address of the router interface
    - service_ipAddress—IP address of the service as specified by the service object
    - user_ipAddress—IP address of the subscriber
    - virtual_ipAddress—Virtual portal address of the SSP that is used in redundant redirect server installations
  - Parameter of type address
- Default—No value

Configuring Next-Rule Actions

You can configure next-rule actions for JUNOS filter policy rules. If a packet matches the classify-traffic condition, the next-rule action causes the router to continue to the next rule in the policy list for evaluation.



Name Next Rule Action

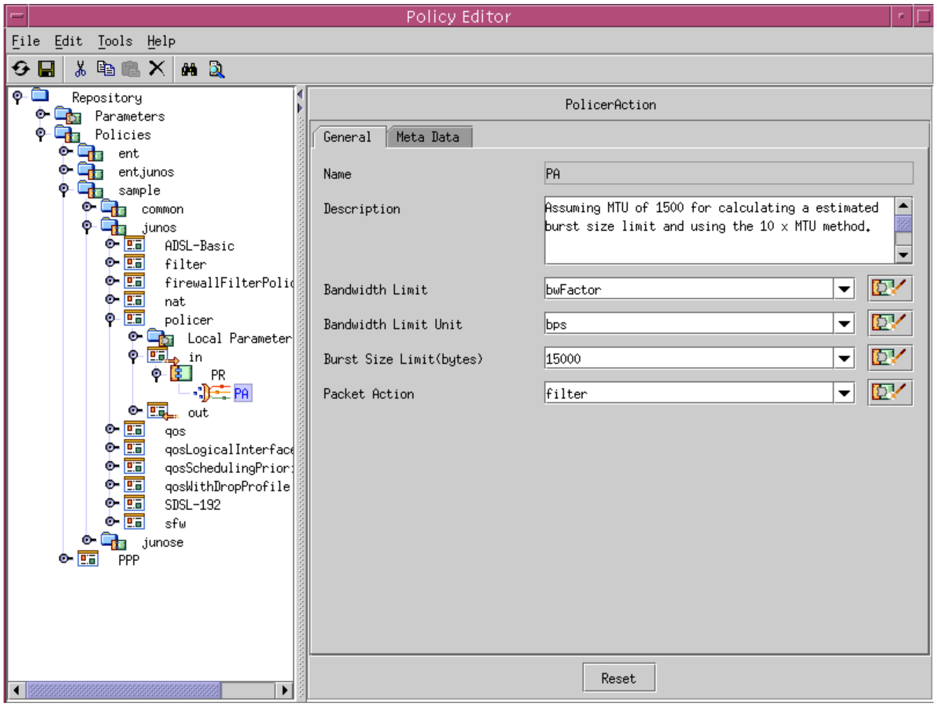
Description

Description

- Description of the action.
- Value—Text
- Default—No value

Configuring Policer Actions

The policer action specifies rate and burst size limits and the action taken if a packet exceeds those limits. You can create policer actions in JUNOS policer and JUNOS filter policy rules.



Name: PA

Description: Assuming MTU of 1500 for calculating a estimated burst size limit and using the 10 x MTU method.

Bandwidth Limit: bwFactor

Bandwidth Limit Unit: bps

Burst Size Limit(bytes): 15000

Packet Action: filter

Description

- Description of the action.
- Value—Text
- Default—No value

Bandwidth Limit

- Traffic rate, that if exceeded, causes the router to take the indicated packet action.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's router interface
  - Integer that represents:
    - rate in bps
    - percentage of bandwidth
  - Numeric expression
  - Parameter of type rate

- Default—No value
- Example—bw * 1 / 5 sets a bandwidth limit of 1/5 of total bandwidth

  where bw is a local parameter that has a value of 1024 * 1920

Bandwidth Limit Unit

- Indicates the type of value entered for bandwidth limit.
- Value
  - Predefined global parameter:
    - bps—Value entered for bandwidth limit is bps
    - percent—Value entered for bandwidth limit is a percentage of the port speed
  - String expression
  - Parameter of type bandwidthSizeUnit
- Default—No value

Burst Size Limit (bytes)

- Maximum burst size. The minimum recommended value is the maximum transmission unit (MTU) of the IP packets being policed.
- Value
  - Number of bytes
  - Numeric expression; for example 8*64000
  - Parameter of type burst
- Default—No value
- Example—8*qosRate sets the burst size limit to 8 times the value of qosRate

  where qosRate is a local parameter of type rate

Packet Action

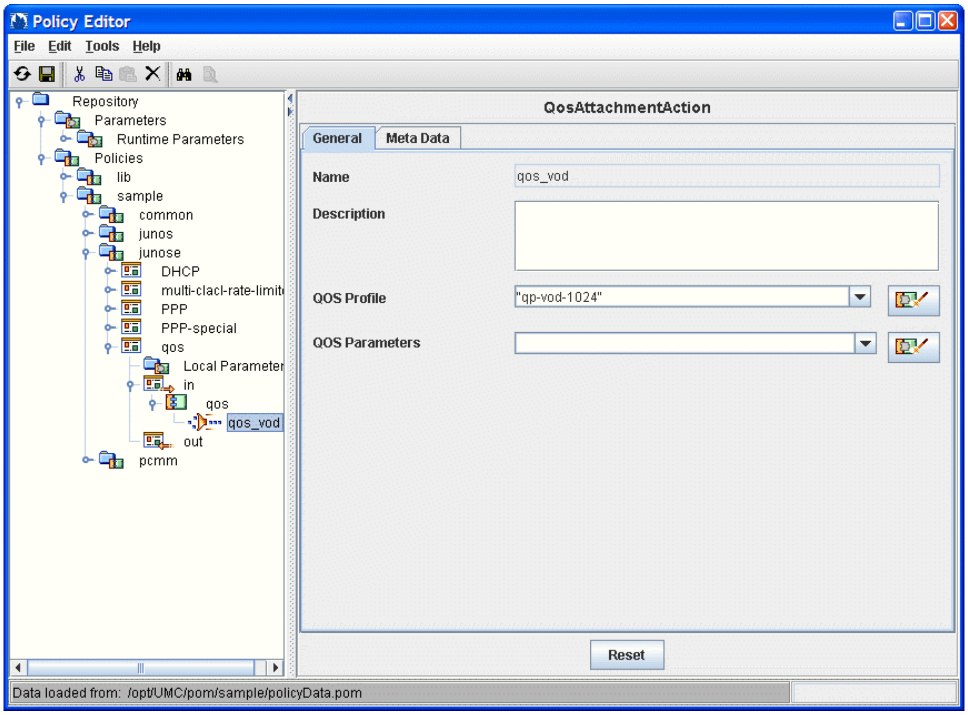
- Action taken on a packet that exceeds its rate limits.
- Value
  - filter—Packet is discarded
  - forwardingClass—Packet is assigned to a forwarding class
  - lossPriority—Packet’s loss priority level is set to low or high
  - String expression
  - Parameter of type packetOperation
- Default—No value

Configuring QoS Profile Attachment Actions

Use this action to specify the QoS profile and the QoS parameters to attach to the router interface when this action is taken. The QoS profile and the QoS parameters must be configured on the router. You can configure QoS actions for JUNOSe policy rules.

The router allows only one QoS profile to be attached to an interface at one time. Therefore, as a subscriber activates and deactivates different services, the QoS profile running on the interface needs to change. The SRC software provides a QoS-tracking plug-in (QTP) that you can use to ensure that as a subscriber activates and deactivates services, the required QoS profile is attached to the subscriber interface. See *SRC-PE Solutions Guide, Chapter 1, Managing Tiered and Premium Services with QoS on JUNOSe Routers with the SRC CLI*.

The QoS parameters allow you to specify rates in QoS profiles as parameters instead of fixed values. The actual values for the parameters can be specified for each interface. Therefore, you can share a QoS profile among different interfaces with different rates.



Name: qos_vod

Description:

QOS Profile: "qp-vod-1024"

QOS Parameters:

Data loaded from: /opt/UMC/pom/sample/policyData.pom

Description

- Description of the action.
- Value—Text
- Default—No value

QoS Profile

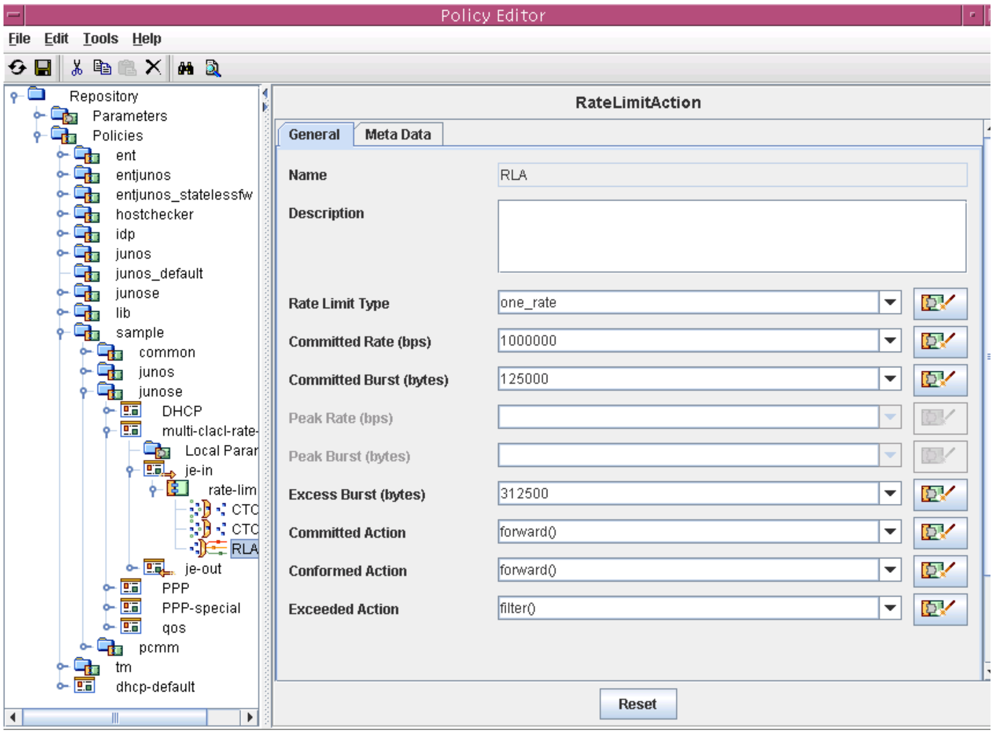
- Name of the QoS profile to attach to the JUNOSe interface when this action is taken.
- Value
  - Name of a QoS profile that is configured on the router. Enclose the name in double quotation marks to indicate that it is a literal string and not a parameter.
  - Parameter of type qosProfileSpec
- Default—No value

QoS Parameters

- Names and values of the QoS parameters to attach to the JUNOSe interface when this action is taken. The parameters are configured on the JUNOSe router and referenced in the scheduler profiles referred to by the QoS profile.
- Value
  - The name = value pair that defines a QoS parameter; use map expressions to define multiple QoS parameters. For example, the map expression {max-bw = 512000, shape-rate = 1000000} supplies two QoS parameters.
  - Parameter of type map
- Default—No value

Configuring Rate-Limit Actions

Use this action to define the quality of service. You can configure rate-limit actions for JUNOSe policy rules.



Name RLA

Description

Rate Limit Type one_rate

Committed Rate (bps) 1000000

Committed Burst (bytes) 125000

Excess Burst (bytes) 312500

Committed Action forward()

Conformed Action forward()

Exceeded Action filter()

Description

- Description of the profile.
- Value—Text
- Default—No value

Rate Limit Type

- Specifies that the rate-limit profile is either one rate or two rate. The one-rate rate-limit profile provides a hard-limit rate limiter or a TCP-friendly rate limiter. The two-rate rate-limit profile provides a two-rate, three-color marking mechanism.

- Value
  - Predefined global parameter:
    - one rate—Uses a single-rate committed rate with two burst parameters: committed burst and excess burst; supports a TCP-friendly rate limiter
    - two rate—Uses committed rate and peak rate, each with a burst parameter
  - Parameter of type rateLimitType
- Default—Two rate

Committed Rate (bps)

- Target rate for the traffic that the policy covers.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's router interface
  - Number of bits per second in the range 0–4294967295
  - Parameter of type rate
- Default—0

Committed Burst (bytes)

- Amount of bandwidth allocated to burst traffic in bytes.
- Value
  - Number of bytes in the range 8192–4294967295
  - Numeric expression
  - Parameter of type burst
- Default—16384
- Example—max(qos*0.1/8, 16384) – sets the burst size to the maximum of 100-ms burst at committed rate (qos*0.1) in bytes (/8) or 16384

  where qos is a local parameter that represents the committed rate

Peak Rate (bps)

- For two-rate rate-limit profiles, specifies the amount of bandwidth allocated to excess traffic flow over the committed rate.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's router interface
  - Number of bits per second in the range 0–4294967295
  - Numeric expression
  - Parameter of type rate
- Default—0
- Example—qos*1.5 – sets the peak rate to 1.5 times the committed rate

  where qos is a local parameter that represents the committed rate

Peak Burst (bytes)

- For two-rate rate-limit profiles, specifies the amount of bandwidth allocated to burst traffic in excess of the peak rate.
- Value
  - Number of bytes in the range 8192–4294967295
  - Numeric expression
  - Parameter of type burst
- Default—16384
- Example—max(qos*1.5*0.1/8, 16384)

  where qos is a local parameter that represents the committed rate

Excess Burst (bytes)

- For one-rate rate-limit profiles, specifies the amount of bandwidth allocated to accommodate burst traffic.
- Value
  - Number of bytes in the range <0 |[Committed Burst + 1, 4294967295]>
  - Numeric expression
  - Parameter of type burst
- Default—No value

Committed Action

- Policy action if traffic flow does not exceed the committed rate.
- Value
  - filter()—Drops the packet
  - forward()—Transmits the packet
  - mark()—Marks the packet by setting the ToS byte (IP) or traffic-class field (IPv6) to the specified 8-bit value, and transmits the packet. Specify the ToS byte in the parenthesis.

    The ToS byte can be an integer in the range 0–255 or parameter of type tosByte
  - Parameter of type packetOperation
- Default—Forward

Conformed Action

- Policy action if traffic flow exceeds the committed rate but remains below the peak rate.
- Value
  - filter()—Drops the packet
  - forward()—Forwards the packet
  - mark()—Marks the packet by setting the ToS byte (IP) or traffic-class field (IPv6) to the specified 8-bit value, and transmits the packet. Specify the ToS byte in the parenthesis.

    The ToS byte can be an integer in the range 0–255 or parameter of type tosByte
  - Parameter of type packetOperation
- Default—Forward

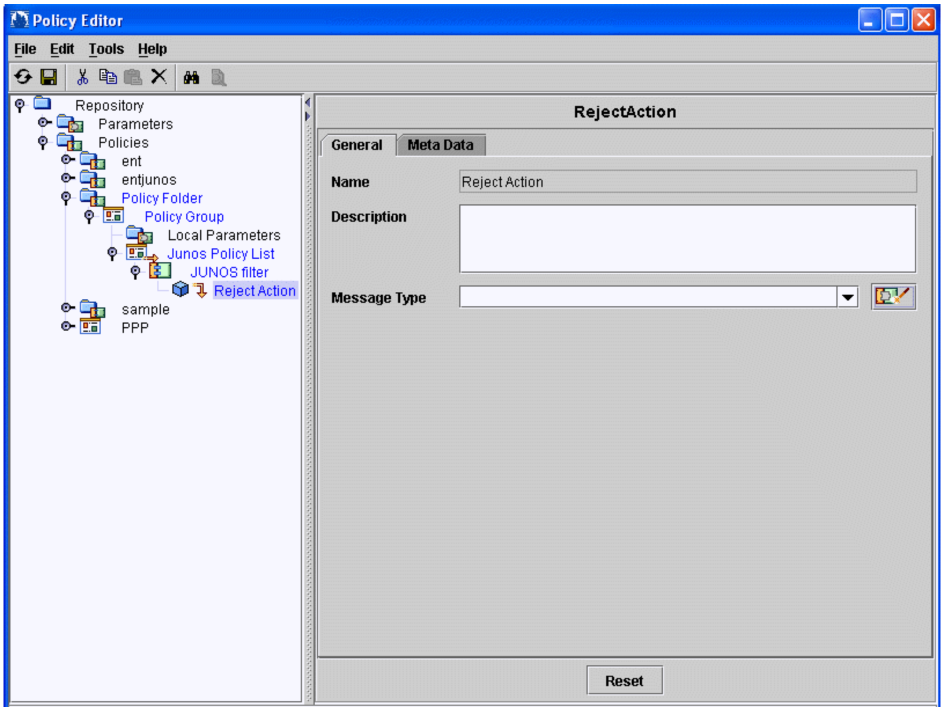
Exceeded Action

- Policy action if traffic flow exceeds the peak rate.
- Value
  - filter()—Drops the packet
  - forward()—Transmits the packet
  - mark()—Marks the packet by setting the ToS byte (IP) or traffic-class field (IPv6) to the specified 8-bit value, and transmits the packet. Specify the ToS byte in the parenthesis.

    The ToS byte can be an integer in the range 0–255 or parameter of type tosByte
  - Parameter of type packetOperation
- Default—Forward

Configuring Reject Actions

You can configure reject actions for JUNOS filter policy rules. The reject action causes the router to discard a packet and send an ICMP destination unreachable message.



Name Reject Action

Description

- Description of the action.
- Value—Text
- Default—No value

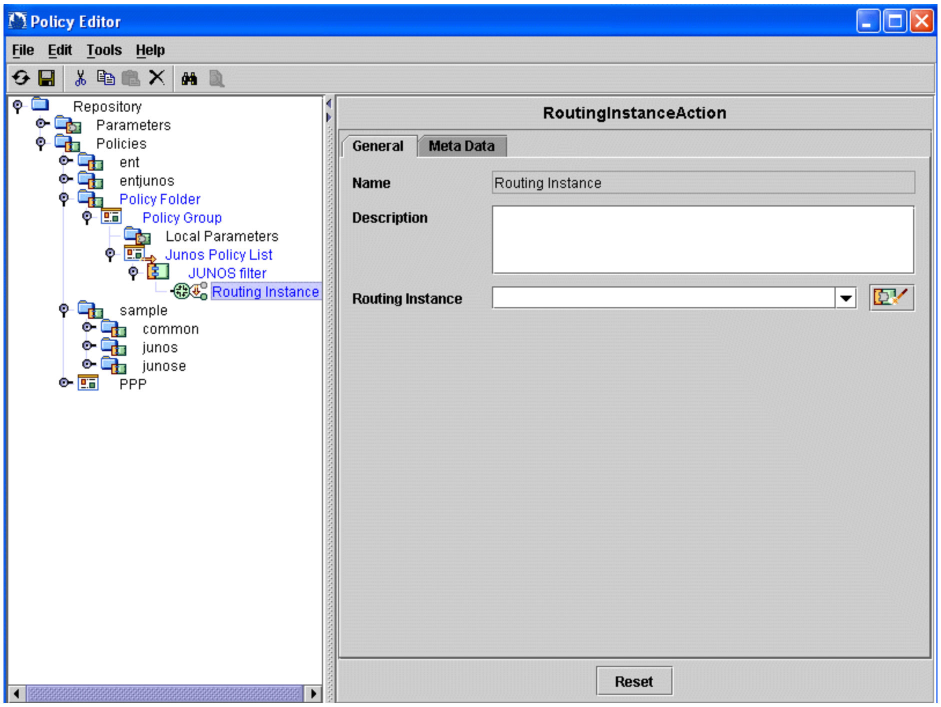
Message Type

- Type of ICMP destination unreachable message sent to the client.
- Value
  - String expression that matches a type of ICMP destination unreachable message supported on the router; for example:
    - “administratively-prohibited”
    - “bad-host-tos”
    - “bad-network-tos”
    - “host-prohibited”
    - “host-unknown”
    - “host-unreachable”
    - “network-prohibited”

        - “network-unknown”
        - “network-unreachable”
        - “port-unreachable”
        - “precedence-cutoff”
        - “precedence-violation”
        - “protocol-unreachable”
        - “source-host-isolated”
        - “source-route-failed”
        - “tcp-reset”—If you specify tcp-reset, a TCP reset message is sent if the packet is a TCP packet. Otherwise, nothing is sent.
    - Parameter of type messageType
- Default—No value

Configuring Routing Instance Actions

You can configure routing instance actions for JUNOS filter policy rules. Use routing instance actions for filter-based forwarding to direct traffic to a specific routing instance configured on the router.



Name: Routing Instance

Description:

Routing Instance:

Description

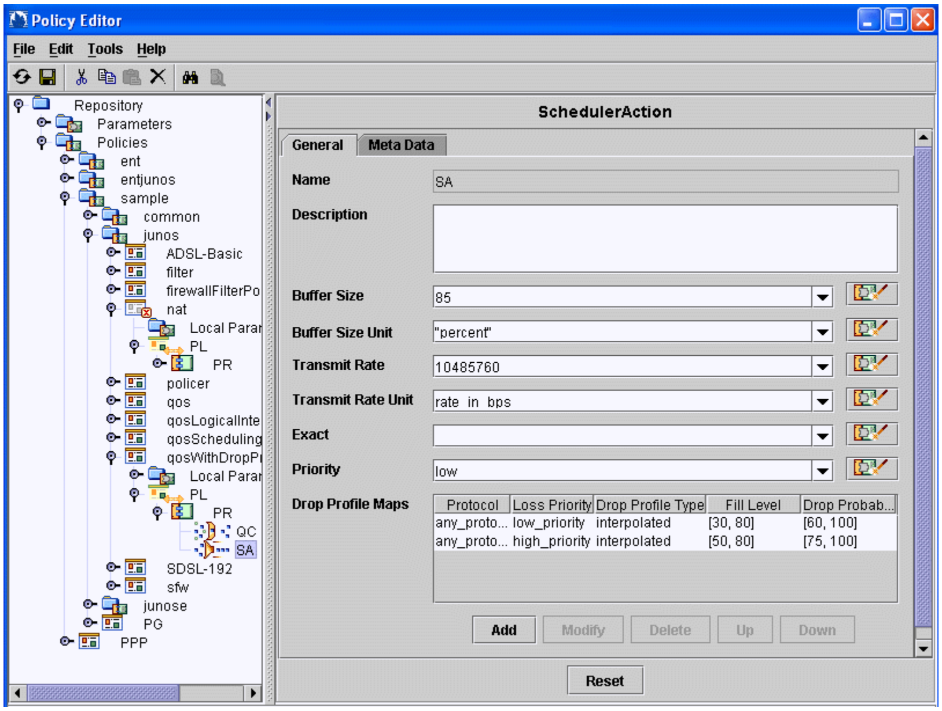
- Description of the action.
- Value—Text
- Default—No value

Routing Instance

- Routing instance to which packets are forwarded. The routing instance must be configured on the router.
- Value
    - String expression that matches the name of a routing instance configured on the router; for example “isp2-route-table”
    - Parameter of type routingInstance
- Default—No value

Configuring Scheduler Actions

You use scheduler actions along with QoS conditions and traffic-shape actions to configure transmission scheduling and rate control. Schedulers define the priority, bandwidth, delay buffer size, rate control status, and random early detection (RED) drop profiles to be applied to a particular class of traffic. You can create scheduler actions in JUNOS scheduler policy rules.



Name SA

Description

Buffer Size 85

Buffer Size Unit "percent"

Transmit Rate 10485760

Transmit Rate Unit rate in bps

Exact

Priority low

Drop Profile Maps

Protocol	Loss Priority	Drop Profile Type	Fill Level	Drop Probab...
any_proto...	low_priority	interpolated	[30, 80]	[60, 100]
any_proto...	high_priority	interpolated	[50, 80]	[75, 100]

Description

- Description of the action.
- Value—Text
- Default—No value

Buffer Size

- Buffer size.
- Value
  - Integer that represents:
    - microseconds
    - percentage of total buffer size
  - “remainder”—Uses available buffer that is not assigned to other queues
  - Expression
  - Parameter of type schedulerBufferSize
- Default—No value

Buffer Size Unit

- Indicates the type of value that you entered for buffer size.
- Value
  - Predefined global parameter:
    - buffer_size_percentage—The value is a percentage of the total buffer.
    - buffer_size_remainder—The value is the remaining buffer available.
    - temporal—The value is temporal, in microseconds.
  - String expression; for example, “percent”
  - Parameter of type schedulerBufferSizeUnit
- Default—No value

Transmit Rate

- Transmit rate.
- Value
  - Integer that represents:
    - Rate in bps
    - Percentage of bandwidth
  - “remainder”—Uses remaining rate available
  - Numeric expression
  - Parameter of type schedulerTransmitRate
- Default—No value
- Example—4/10*bandwidth sets the transmit rate to 4/10 of transmission bandwidth that is allocated to the logical interface unit

  where bandwidth is a local parameter of type any

Transmit Rate Unit

- Indicates the type of value entered for transmit rate.
- Value
    - Predefined global parameter:
        - rate_in_bps—Transmission rate in bps
        - rate_in_percentage—Percentage of transmission capacity
        - rate_in_remainder—Uses remaining rate available
    - String expression
    - Parameter of type schedulerTransmitRateUnit
- Default—No value

Exact

- Specifies whether or not to enforce the exact transmission rate. Under sustained congestion, a rate-controlled queue that goes into negative credit fills up and eventually drops packets.
- Value
    - true
    - false
    - Parameter of type boolean
- Default—No value

Priority

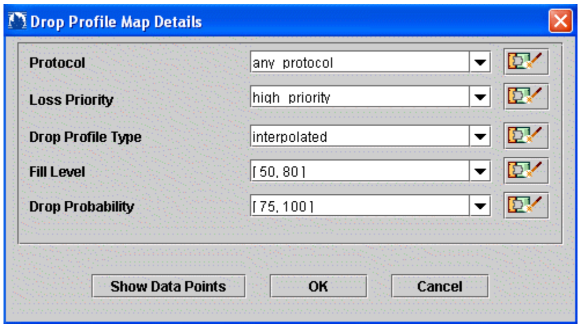
- Packet-scheduling priority. The priority determines the order in which an output interface transmits traffic from the queues.
- Value
    - Predefined global parameter:
        - low
        - medium_low
        - medium_high
        - high—Assigning high priority to a queue prevents the queue from being starved by traffic in a strict high-priority queue
        - strict_high—Configure a high-priority queue with unlimited transmission bandwidth available to it. As long as it has traffic to send, the strict high-priority queue receives precedence over low, medium-low, and medium-high priority queues, but not high-priority queues. You can configure strict high-priority on only one queue per interface.
    - String expression—For example, “strict-high”
    - Parameter of type schedulerPriority
- Default—No value

Configuring Drop Profile Maps

The scheduler drop profile defines the drop probabilities across the range of delay-buffer occupancy, thereby supporting the RED process. For a packet to be dropped, it must match the drop profile. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet. Depending on the drop probabilities, RED might drop packets aggressively long before the buffer becomes full, or it might drop only a few packets even if the buffer is almost full.

The SchedulerAction pane displays a table with configured drop profile maps. To configure the table:

- To add a drop profile map, click **Add**. Policy Editor displays the Drop Profile Map Details dialog box.
- To modify a map, select the map, and click **Modify**. Policy Editor displays the Drop Profile Map Details dialog box for that map.
- To delete a map, select the map, and click **Delete**.
- To move a map up, select the map, and click **Up**.
- To move a map down, select the map, and click **Down**.



Protocol: any protocol
Loss Priority: high priority
Drop Profile Type: interpolated
Fill Level: [50, 80]
Drop Probability: [75, 100]

Protocol

- Specify the protocol type for the drop protocol.
- Value
    - Predefined global parameter:
        - any_protocol—Accepts any protocol type
        - non_tcp—Accepts any protocol type other than TCP/IP
        - tcp_only—Accepts only TCP/IP protocol
    - String expression
    - Parameter of type dropProfileProtocol
- Default—No value

Loss Priority

- Sets the packet loss priority (PLP).
- Value
  - Predefined global parameter:
    - any_priority—Drop profile applies to packets with any PLP.
    - high_priority—Drop profile applies to packets with high PLP.
    - low_priority—Drop profile applies to packets with low PLP.
  - String expression
  - Parameter of type packetLossPriority
- Default—No value

Drop Profile Type

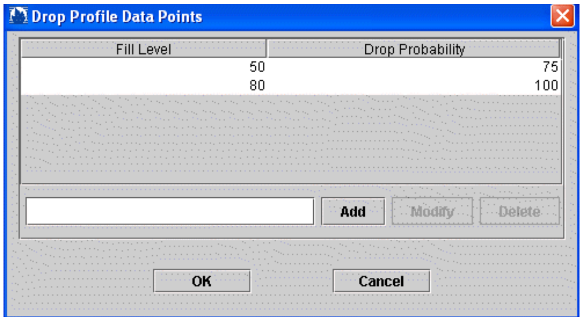
- Relationship between the fill level and drop probability.
- Value
  - Predefined global parameter:
    - interpolated—Specifies values for interpolating relationship between queue fill level and drop probability
    - segmented—Specifies fill level and drop probability as percentages
  - Parameter of type dropProfileType
- Default—No value

Setting Fill Level and Drop Probability

In drop profiles you configure fill level and drop probability as paired values. The values can be either percentage values (segmented) or data points (interpolated). These two alternatives enable you to configure each drop probability at up to 64 fill-level/drop-probability paired values, or to configure a profile represented as a series of line segments. For more information about configuring fill level and drop probabilities, see the JUNOS routing platform documentation.

You can set these value pairs by clicking Show Data Points on the Drop Profile Map Details screen. To add a value pair:

1. In the data entry field, enter the value for the fill level, press the space bar, and then enter the drop probability value.
2. Click **Add**.



Fill Level	Drop Probability
50	75
80	100

Fill Level

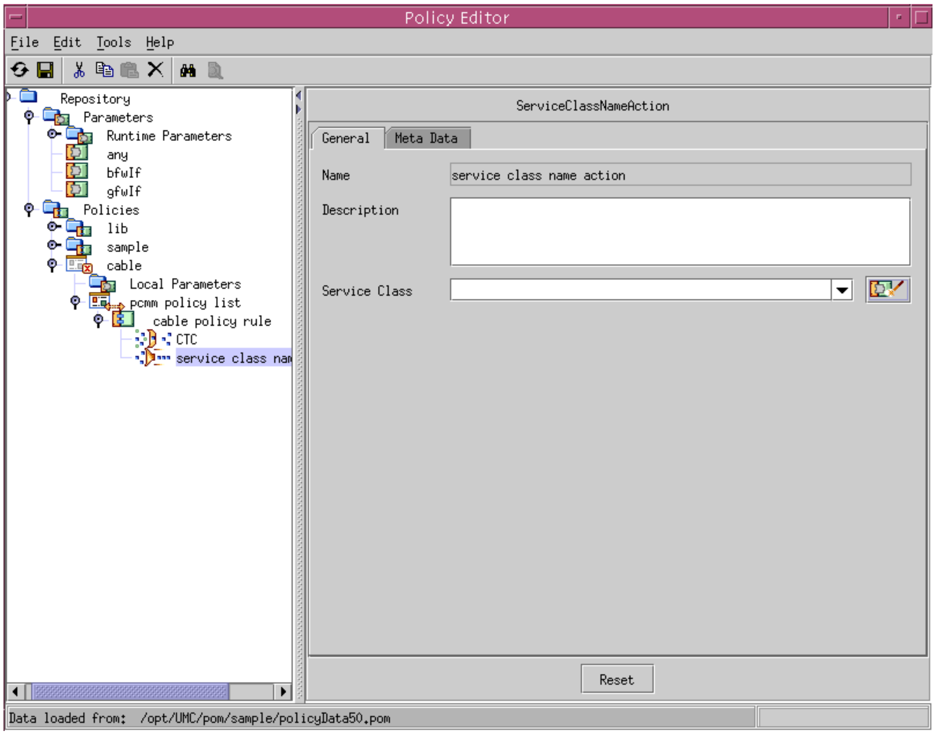
- Fill level of the queue.
- Value
    - If the drop profile type is segmented, specify how full the queue is as a percentage.
    - If the drop profile type is interpolated, specify a data point for mapping the queue fill percentage in the range 0–100.
    - Parameter of type percent
- Default—No value

Drop Probability

- Probability that a packet will be dropped.
- Value
    - If the drop profile type is segmented, specify the drop probability as a percentage. A value of 0 means that a packet will never be dropped, and a value of 100 means that all packets will be dropped. The range is 0–100.
    - If the drop profile type is interpolated, specify a data point for packet drop probability in the range 0–100.
    - Parameter of type percent
- Default—No value

Configuring Service Class Name Actions

You can configure service class name actions for PCMM policy rules.



Name: service class name action

Data loaded from: /opt/UMC/pom/sample/policyData50.pom

Description

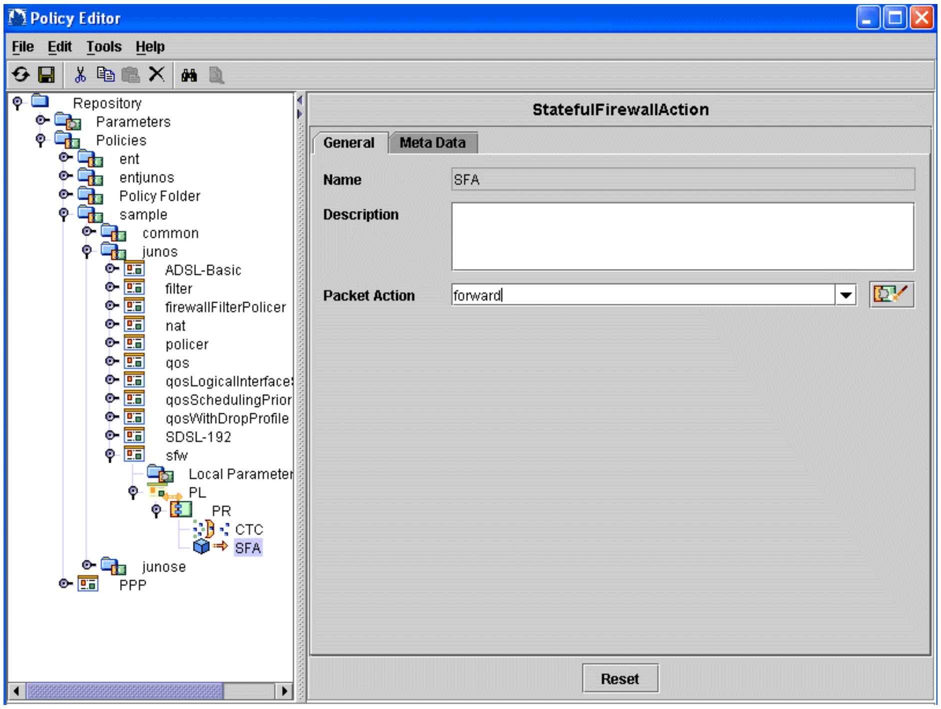
- Description of the action.
- Value—Text
- Default—No value

Service Class

- Name of a service class on the CMTS device that specifies QoS parameters for a service flow.
- Value
  - Name of a service class
  - String expression
  - Parameter of type serviceClassName
- Default—No value

Configuring Stateful Firewall Actions

You can configure stateful firewall actions for JUNOS ASP policy rules. Stateful firewall actions specify the action to take on packets that match the classify-traffic condition.



StatefulFirewallAction

Name: SFA

Description:

Packet Action: forward

Description

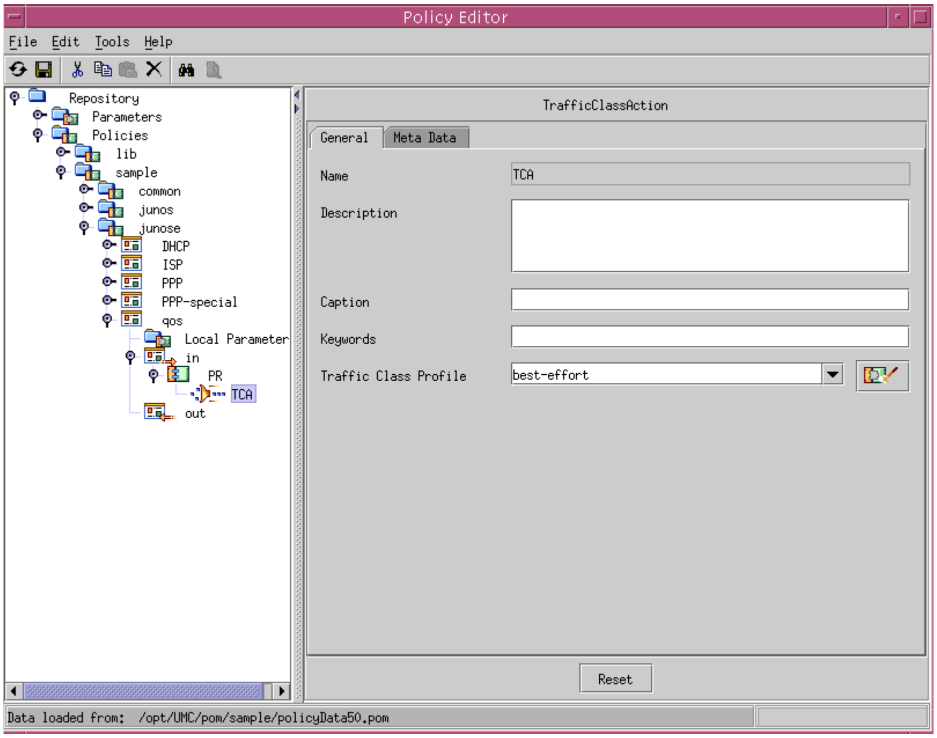
- Description of the action.
- Value—Text
- Default—No value

Packet Action

- Action taken on packets.
- Value
  - filter—Packet is not accepted and is not processed further
  - forward—Packet is accepted and sent to its destination
  - reject—Packet is not accepted, and a rejection message is returned; UDP sends an ICMP unreachable code, and TCP sends RST
  - String expression
  - Parameter of type packetOperation
- Default—No value

Configuring Traffic-Class Actions

Use this action to put packets in a particular traffic class. You can configure traffic-class actions for JUNOSe policy rules.



Name: TCA

Description:

Caption:

Keywords:

Traffic Class Profile: best-effort

Data loaded from: /opt/UMC/pom/sample/policyData50.pom

Description

- Description of the action.
- Value—Text
- Default—No value

Caption

- Short description of the action.
- Value—Text
- Default—No value

Keywords

- Series of words that the system uses as a filter for keyword searches that are inherited from the policy.
- Value—Text
- Default—No value

Traffic-Class Profile

- Name of the traffic-class profile that is applied to a packet when it passes through the router.
- Value
    - Name of a traffic-class profile that is configured on the router
    - Parameter of type trafficClassSpec
- Default—No value

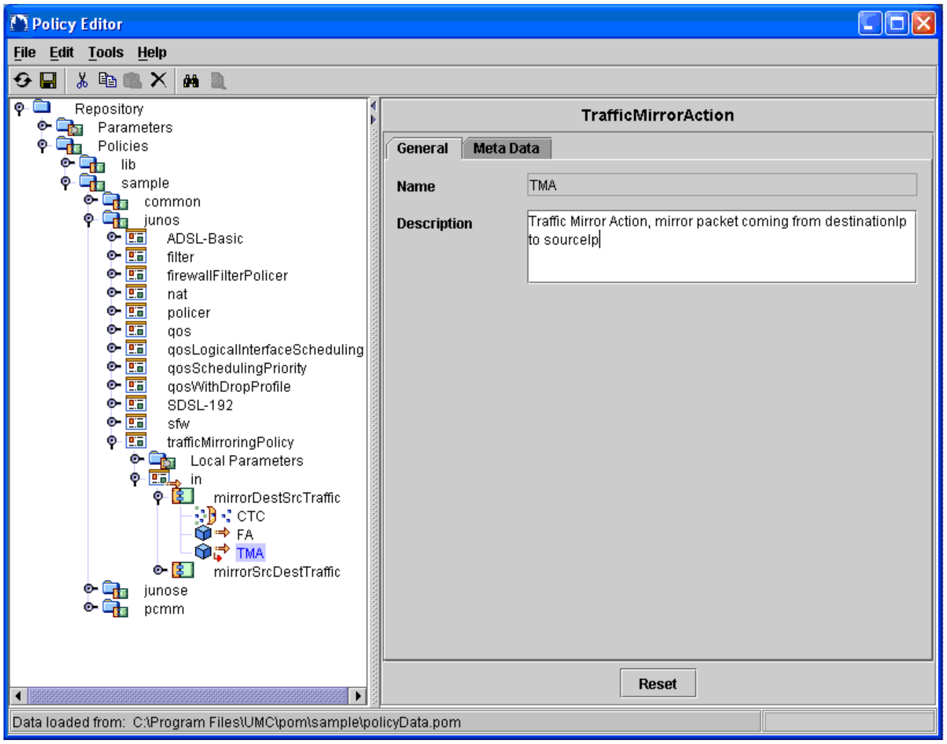
Configuring Traffic-Mirror Actions

Use this action to mirror traffic from a destination to a source or from a source to a destination. You can configure traffic-mirror actions only for JUNOS input policy rules.

Before you use traffic-mirror actions, you must configure forwarding options on JUNOS routing platforms for port mirroring and next-hop group. For information about how these features work on the router, see the *JUNOS Policy Framework Configuration Guide*.

The rule containing a traffic-mirror action must comply with these conditions:

- It must be combined with forward actions in the same rule. One of the forward actions must accept the traffic if the source and/or destination IP addresses do not match the conditions.
- It contains either no classify-traffic condition or only one classify-traffic condition.
- It can be marked for accounting.



Name TMA

Description Traffic Mirror Action, mirror packet coming from destinationIp to sourceIp

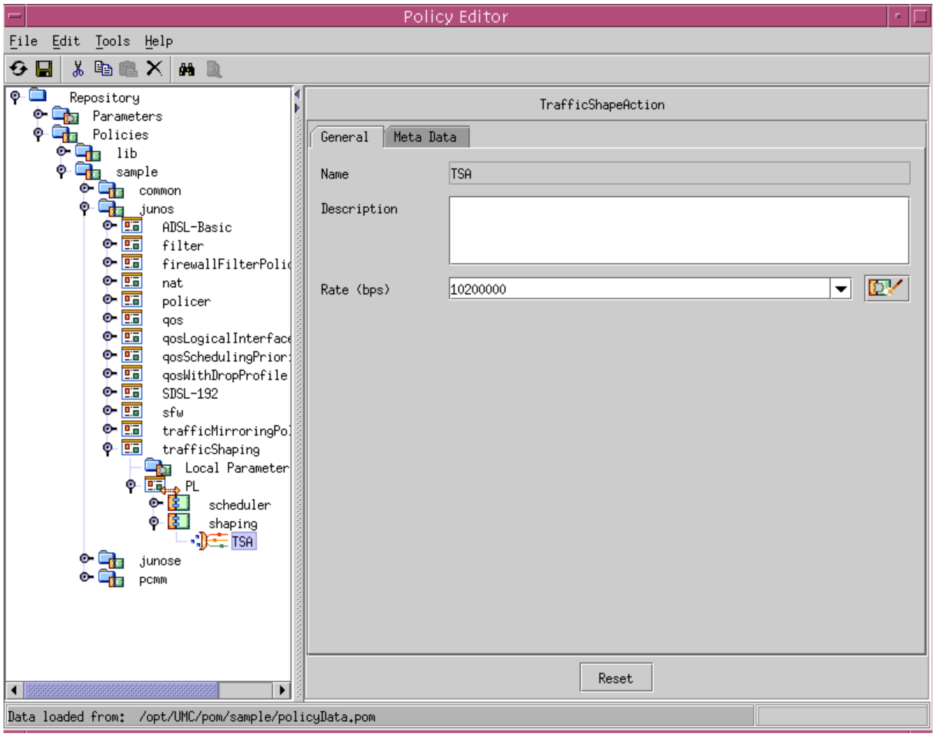
Data loaded from: C:\Program Files\UMC\pom\sample\policyData.pom

Description

- Description of the action.
- Value—Text
- Default—No value

Configuring Traffic-Shape Actions

Traffic-shape actions specify the maximum rate of traffic transmitted on an interface. You can create traffic-shape actions in JUNOS shaping policy rules.



Name: TSA

Description:

Rate (bps): 10200000

Data loaded from: /opt/UMC/pom/sample/policyData.pom

Description

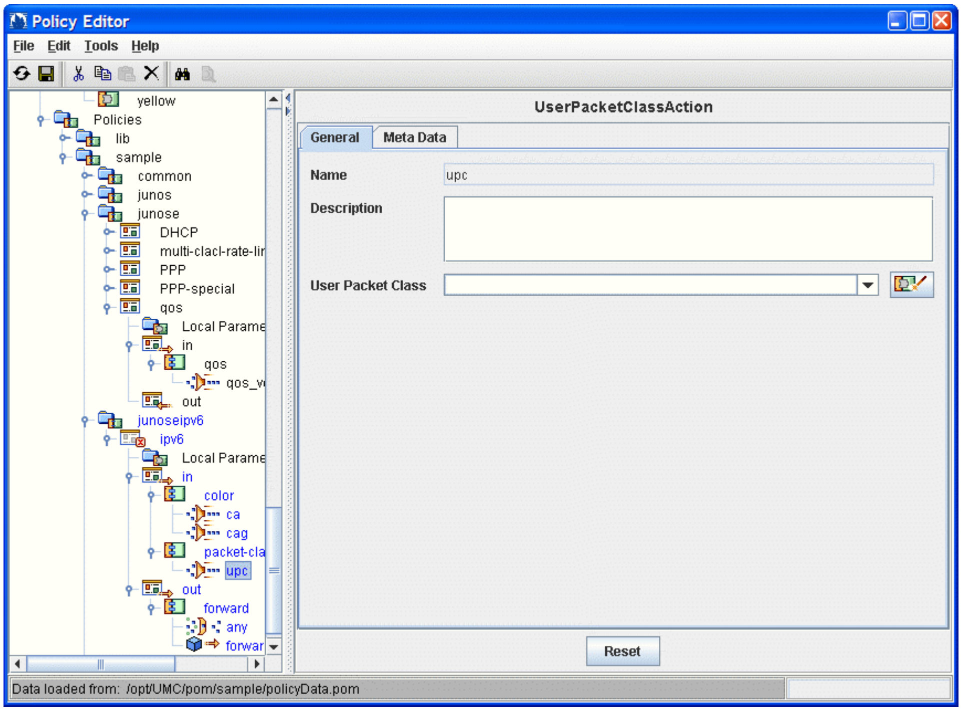
- Description of the action.
- Value—Text
- Default—No value

Rate (bps)

- Sets the maximum transmission rate.
- Value
  - Predefined global parameter:
    - interface_speed—Speed of the subscriber's router interface
  - Bits per second in the range 1000–32000000000
  - Numeric expression
  - Parameter of type rate
- Default—No value

Configuring User Packet Class Actions

Use this action to put packets in a particular user packet class. You can configure user packet class actions for JUNOSe IPv6 policy rules.



Name: upc

Data loaded from: /opt/UMC/pom/sample/policyData.pom

Description

- Description of the action.
- Value—Text
- Default—No value

User Packet Class

- User packet class that is applied to a packet when it passes through the router.
- Value
    - User packet class value that is configured on the router, in the range 0–15
    - Parameter of type userPacketClass
- Default—No value

Modifying Policy Objects in the Directory

This section shows how to modify policy groups by changing the policyGroup, policyList, and policyRule objects in the directory.

Once a policy is in use, we recommend that you do not modify the policy by deleting and recreating it. Doing so results in an error message being logged for each interface or active service session that currently uses the policy. If you delete a default policy that is running on an interface, the SRC software leaves the policy running and logs an error message. When a new interface that uses the policy as a default policy is created, every service activation for a service that uses the policy fails until the new definition of the policy is loaded. This condition lasts until DES polls the directory, detects the change, and provides the change to the policy engine.

Modifying Policy Groups

To modify an existing policyGroup and trigger the policy engine to update policies on JUNOSe routers:

1. Make the required changes to the policyList and policyRule objects that are contained in the policyGroup entry.

2. Make a modification to the policyGroup entry. For instance, change its description or set its deleted attribute to FALSE.

   This step triggers the policy engine to reload the new policy definition. All interfaces that currently use the policy as a default policy are updated, and all active service sessions that use the policy are updated.

Adding Policy Groups

To add a policy group and load it onto the JUNOSe router:

1. Make sure that a policyGroup object with the same name does not already already exist with its deleted attribute set to TRUE.

2. Create the policyGroup, and set the deleted attribute to TRUE.

3. Configure the policyGroup as desired, and configure its policyLists and policyRules.

4. Trigger the policy engine to load the new policy by setting the deleted attribute in the policyGroup to FALSE.

Deleting and Purging Policy Groups from the Directory

To delete a policyGroup entry from the directory, make sure that the umcDeletionAuxClass is in the object class, and set the deleted attribute to TRUE. At the next DES polling interval, the policy is removed from the policy engine. As mentioned above, take care not to delete policyGroups that are in use.

After you set the deleted attribute in the policyGroup to TRUE, you can purge the policyLists and policyRules underneath the policyGroup. Once you are sure that the deletion of policyLists and policyRules is replicated to all directories and that the SAE has been triggered to make the change, you can purge the policyGroup.

We recommend that you purge only deleted policyGroups. You can perform this operation very infrequently (perhaps once a month). Before performing this operation, use SAE Web Admin to check each SAE to be sure that the policyGroups to be purged are not included in the SAE's memory. If a deleted policy remains in the SAE's memory, ensure that it has its deleted attribute set to TRUE or that it does not exist in the SAE's connected directory. If the deleted policy:

- Has its deleted attribute set to TRUE, use SAE Web Admin to reload the policies from the directory.
- Does not exist in the SAE's connected directory, directory replication is not working properly and should be checked.