Chapter 11

Configuring and Managing Policies with the SRC CLI

This chapter describes how to use the SRC CLI to configure and manage policies. You can also use Policy Editor to configure and manage policies. See *Chapter 12, Configuring and Managing Policies with Policy Editor*.

Topics in this chapter include:

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 configure policies, 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.

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 options can take expressions in addition to literal values. If you can enter an expression for an option, the expression type is noted in the documentation for the command. For information about using and formatting expressions, see *Expressions* on page 406.

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 the 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, the policy software 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 you specify a value greater than 100,000,000, 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.

Enabling the Policy Configuration on the SRC CLI

Before you can configure policies with the SRC CLI, you must enable the policy, service, and subscriber editor on the SRC CLI. To do so:

In operational mode, enter the following command:

user@host> **enable component editor**

Configuring Policy Folders

You use policy folders to organize policy groups. Use the following configuration statement to create a policy folder:

policies folder *name* ...

To create a policy folder:

- From configuration mode, enter the edit policies folder statement. For example, to create a folder called junos_default:

  user@host# **edit policies folder junos_default**

Configuring Policy Groups

Policy groups hold policy lists. You can create policy groups within policy folders. Use the following configuration statement to create a policy group:

```
policies group name {
    description description;
}
```

To create a policy group:

1. From configuration mode, enter the edit policies group statement. For example, to create a folder called dhcp-default:

   ```
   user@host# edit policies group dhcp-default
   ```

2. (Optional) Enter a description for the policy group.

   ```
   [edit policies group dhcp-default]
   user@host# set description description
   ```

3. (Optional) Verify your policy group configuration.

   ```
   [edit policies group dhcp-default]
   user@host#show
   description "Default policy for JUNOSe routers";
   ```

Configuring Policy Lists

When you add a policy list, you specify whether the policy list is for JUNOS routing platforms, JUNOSe routers (junose-ipv4), or a CMTS device (pcmm). The type of policy list that you add controls the type of policy rules that you can add to the policy list.

You create policy lists within policy groups. Use the following configuration statements to create a policy list:

```
policies group name list name {
    role (junos | junose-ipv4 | pcmm);
    applicability (input | output | both);
    description description;
}
```

To add a policy list:

1. From configuration mode, create a policy list. For example, to create a policy list called in within a policy group called dhcp:

   ```
   user@host# edit policies group dhcp list in
   ```

2. Specify the type of policy list. You must configure the type of policy list before you can add rules to the list.

   ```
   [edit policies group dhcp list in]
   user@host# set role junose-ipv4
   ```

3. Specify where the policy is applied on the router or, for PCMM policies, indicates whether the policy applies to the upstream or downstream channel.

   [edit policies group dhcp list in]
   user@host# **set applicability input**

4. (Optional) Provide a description of the policy list.

   [edit policies group dhcp list in]
   user@host# **set description** *description*

5. (Optional) Verify your policy list configuration.

```
[edit policies group dhcp list in]
user@host# show
role junose-ipv4;
applicability input;
description "input policy list for JUNOSe DHCP";
```

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.
- 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 Adaptive Services 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

You create policy rules within policy lists. Use the following configuration statements to create a policy rule:

```
policies group name list name rule name {
    type type;
    precedence precedence;
    accounting;
    description description;
}
```

To add a policy rule:

1. From configuration mode, create a policy rule inside a policy list that has already been created and configured. For example, to create a policy rule called forward-dhcp within policy list input:

   ```
   user@host# edit policies group dhcp list input rule forward-dhcp
   ```

2. Specify the type of policy rule.

   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.

   ```
   [edit policies group dhcp list input rule forward-dhcp]
   user@host# set type type
   ```

3. (Optional) Specify the order in which the policy manager applies rules.

   ```
   [edit policies group dhcp list input rule forward-dhcp]
   user@host# set precedence precedence
   ```

4. (0ptional) Specify whether accounting data is collected for the actions specified in the rule.

   ```
   [edit policies group dhcp list input rule forward-dhcp]
   user@host# set accounting
   ```

5. (Optional) Provide a description of the policy rule.

   ```
   [edit policies group dhcp list input rule forward-dhcp]
   user@host# set description description
   ```

6. (Optional) Verify your policy rule configuration.

   ```
   [edit policies group dhcp list input rule forward-dhcp]
   user@host# show
   type junose-ipv4;
   precedence 200;
   accounting;
   description "Forward all dhcp packets from client to server";
   ```

Configuring Classify-Traffic Conditions

You create classify-traffic conditions in JUNOSe policy rules, in JUNOS ASP and JUNOS filter policy rules, and in PCMM policy rules.

The available configuration statements change depending on the type of policy rule that holds the condition and on the type of protocol that you specify.

To configure a classify-traffic condition, do the following:

1. Create a classify-traffic condition. See:
   - Creating a Classify-Traffic Condition on page 222
2. Configure source networks. You can configure source networks in one of two formats. See:
   - Configuring Source Networks on page 223
   - Configuring Source Grouped Networks on page 224
3. Configure destination networks. You can configure destination networks in one of two formats. See:
   - Configuring Destination Networks on page 225
   - Configuring Destination Grouped Networks on page 226
4. Configure protocol conditions. The type of protocol condition that you use depends on your configuration.
   - To configure protocol conditions that do not include ports, see:
     - Configuring Protocol Conditions on page 227
   - To configure protocol conditions that include ports, see:
     - Configuring Protocol Conditions with Ports on page 228
   - To configure protocol conditions in which the protocol that you specify is a parameter, see:
     - Configuring Protocol Conditions with Parameters on page 231
   - To configure protocol conditions in which the protocol is TCP, see:
     - Configuring TCP Conditions on page 235
   - To configure protocol conditions in which the protocol is ICMP, see:
     - Configuring ICMP Conditions on page 238
   - To configure protocol conditions in which the protocol is IGMP, see:
     - Configuring IGMP Conditions on page 239

- To configure protocol conditions in which the protocol is IPSec, see:
  - Configuring IPSec Conditions on page 240
- To configure a ToS byte condition, see:
  - Configuring ToS Byte Conditions on page 242

5. For JUNOS filter policies, configure a JUNOS filter condition. See:
   - Configuring JUNOS Filter Conditions on page 243
6. For the stateful firewall and NAT policies, configure an application protocol condition. See:
   - Configuring Application Protocol Conditions on page 244

NOTE: PCMM classifiers support only the following classifiers:

- 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.

Before You Configure Classify-Traffic Conditions

If you are configuring classifiers for PCMM policies, you can specify whether the classifier will be used in a PCMM IO2 or IO3 network. By default, the software translates classify-traffic conditions into PCMM IO2 classifiers.

- See *Specifying the PCMM Classifier Type* on page 220.

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

- See *Enabling Expansion of JUNOSe Classify-Traffic Conditions* on page 220.

Enabling Expansion of JUNOSe Classify-Traffic Conditions

For information about expanded classifiers, see *Expanded Classifiers* on page 153.

Use the following configuration statement to enable or disable the expansion of JUNOSe classifiers.

```
shared sae configuration policy-management-configuration {
    enable-junose-classifier-expansion;
}
```

To enable or disable the expansion of JUNOSe classifiers:

1. From configuration mode, access the configuration statement that configures policy management properties on the SAE.

   user@host# **edit shared sae configuration policy-management-configuration**

2. Specify whether or not the SAE expands the JUNOSe classify-traffic conditions into multiple classifiers before it installs the policy on the router.

   [edit shared sae configuration policy-management-configuration]
   user@host# **set enable-junose-classifier-expansion**

Specifying the PCMM Classifier Type

Use the following configuration statement to specify which version of the PCMM classifiers you are using:

```
shared sae configuration driver pcmm {
    disable-pcmm-iO3-policy disable-pcmm-iO3-policy;
}
```

To specify whether or not the SAE sends classifiers to the router that comply with PCMM IO3:

1. From configuration mode, access the configuration statement that configures the PCMM driver.

   user@host# **edit shared sae configuration driver pcmm**

2. Enable or disable the SAE to send classifiers to the router that comply with PCMM IO3. Disable this option if your network deployment has CMTS devices that do not support PCMM IO3.

   [edit shared sae configuration driver pcmm]
   user@host# **set disable-pcmm-iO3-policy** *disable-pcmm-iO3-policy*

Specifying Port Access for Traffic Classification

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

In the SRC CLI, you specify ranges by setting values in the port-operation options in command statements.

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. For the port-operation option, enter **eq**.
2. For the from-port option, enter the range of ports allowed.

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

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

1. For the port-operation option, enter **neq**.
2. For the from-port option, 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. For the port-operation option, enter **eq**.
2. For the from-port option, 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. For the port-operation option, enter **neq**.
2. For the from-port option, enter the range of ports.

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

Creating a Classify-Traffic Condition

You create classify-traffic conditions within policy rules. Use the following configuration statements to create a classify-traffic condition:

```
policies group name list name rule name traffic-condition name {
    match-direction match-direction;
    description description;
}
```

To add a classify-traffic condition:

1. From configuration mode, create a classify-traffic condition inside a policy rule that has already been created and configured. For example, to create a traffic-condition called ctc within policy rule nat:

   ```
   user@host# edit policies group junos list staticnat rule nat traffic-condition ctc
   ```

2. (Optional) For JUNOS ASP policy rules, specify the direction of the packet flow on which you want to match packets.

   ```
   [edit policies group junos list staticnat rule nat traffic-condition ctc]
   user@host# set match-direction match-direction
   ```

3. (Optional) Provide a description of the classify-traffic condition.

   ```
   [edit policies group junos list staticnat rule nat traffic-condition ctc]
   user@host# set description description
   ```

4. (Optional) Verify your classify-traffic condition configuration.

   ```
   [edit policies group junos list staticnat rule nat traffic-condition ctc]
   user@host# show
   match-direction output;
   description "Static NAT destination classifier";
   ```

Configuring Source Networks

Use the following configuration statements to add source networks to a classify-traffic condition:

```
policies group name list name rule name traffic-condition name source-network network
{
    ip-address ip-address;
    ip-mask ip-mask;
    ip-operation ip-operation;
}
```

To add a source network to a classify-traffic condition:

1. From configuration mode, enter the source network within a classify-traffic condition. For example:

   ```
   user@host# edit policies group dhcp list in rule forward-dhcp traffic-condition
   client-dhcp source-network network
   ```

2. (Optional) Configure the IP address of the source network or host.

   ```
   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp
   source-network network]
   user@host# set ip-address ip-address
   ```

3. (Optional) Configure the IP mask of the source network or host.

   ```
   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp
   source-network network]
   user@host# set ip-mask ip-mask
   ```

4. (Optional) Specify whether the software matches packets with an IP address that is equal or not equal to the specified address and mask.

   ```
   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp
   source-network network]
   user@host# set ip-operation ip-operation
   ```

5. (Optional) Verify your source network configuration.

   ```
   [edit policies group dhcp list in rule forward-dhcp traffic-condition
   client-dhcp source-network network]
   user@host# show
   ip-address interface_ipAddress;
   ip-mask interface_ipMask;
   ip-operation is_not;
   ```

Configuring Source Grouped Networks

You can configure source networks in grouped format. For JUNOS ASP policy rules, you must enter source networks in grouped format.

Use the following configuration statement to add source networks in a grouped format to a classify-traffic condition:

policies group *name* list *name* rule *name* traffic-condition *name* source-network group-network {
    network-specifier *network-specifier*;
}

To add a grouped source network to a classify-traffic condition:

1. From configuration mode, enter the source network within a classify-traffic condition. For example:

   user@host# **edit policies folder junose group dhcp list in rule forward-dhcp traffic-condition client-dhcp source-network group-network**

2. (Optional) Configure the IP address of the source network or host.

   For JUNOS ASP policies rules, you must enter networks in the format <ip address>/<prefix length>. The <ip address>/<mask> format is rejected by the router.

   [edit policies folder junose group dhcp list in rule forward-dhcp traffic-condition client-dhcp source-network group-network]
   user@host# **set network-specifier** *network-specifier*

3. (Optional) Verify your source network configuration.

```
[edit policies folder junose group dhcp list in rule forward-dhcp
traffic-condition client-dhcp source-network group-network]
user@host# show
network-specifier gateway_ipAddress;
```

Configuring Destination Networks

Use the following configuration statements to add destination networks to a classify-traffic condition:

policies group *name* list *name* rule *name* traffic-condition *name* destination-network network {
    ip-address *ip-address*;
    ip-mask *ip-mask*;
    ip-operation *ip-operation*;
}

To add a destination network to a classify-traffic condition:

1. From configuration mode, enter the destination network within a classify-traffic condition. For example:

   user@host# **edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp destination-network network**

2. (Optional) Configure the IP address of the destination network or host.

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp destination-network network]
   user@host# **set ip-address** *ip-address*

3. (Optional) Configure the IP mask of the destination network or host.

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp destination-network network]
   user@host# **set ip-mask** *ip-mask*

4. (Optional) Specify whether the software matches packets with an IP address that is equal or not equal to the specified address and mask.

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp destination-network network]
   user@host# **set ip-operation** *ip-operation*

5. (Optional) Verify your destination network configuration.

```
[edit policies group dhcp list in rule forward-dhcp traffic-condition
client-dhcp destination-network network]
user@host# show
ip-address interface_ipAddress;
ip-mask interfac_ipMask;
ip-operation is;
```

Configuring Destination Grouped Networks

You can configure destination networks in grouped format. For JUNOS ASP policies rules, you must enter destination networks in grouped format.

Use the following configuration statements to add destination networks in a grouped format to a classify-traffic condition:

policies group *name* list *name* rule *name* traffic-condition *name* destination-network group-network {
    network-specifier *network-specifier*;
}

To add a grouped destination network to a classify-traffic condition:

1. From configuration mode, enter the destination network within a classify-traffic condition. For example:

   user@host# **edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp destination-network group-network**

2. (Optional) Configure the IP address of the destination network or host.

   For JUNOS ASP policies rules, you must enter networks in the format "<ip address>/<prefix length>".

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp destination-network group-network]
   user@host# **set network-specifier** *network-specifier*

3. (Optional) Verify your destination network configuration.

```
[edit policies group dhcp list in rule forward-dhcp traffic-condition
client-dhcp destination-network group-network]
user@host# show
network-specifier any;
```

Configuring Protocol Conditions

The procedure in this sections shows how to configure general protocol conditions.

- If your condition includes port numbers, use the procedure in *Configuring Protocol Conditions with Ports* on page 228.
- If your condition consists of a protocol that is assigned with a parameter value, use the procedure in *Configuring Protocol Conditions with Parameters* on page 231.

Use the following configuration statements to add general protocol conditions to a classify-traffic condition:

```
policies group name list name rule name traffic-condition name protocol-condition {
    protocol protocol;
    protocol-operation protocol-operation;
    ip-flags ip-flags;
    ip-flags-mask ip-flags-mask;
    fragment-offset fragment-offset;
    packet-length packet-length;
}
```

To add general protocol conditions to a classify-traffic condition:

1. From configuration mode, enter the general protocol condition configuration. For example:

   user@host# **edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp protocol-condition**

2. Configure the protocol matched by this classify-traffic condition.

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp protocol-condition]
   user@host# **set protocol** *protocol*

3. Configure the policy to match packets with the protocol that is either equal or not equal to the specified protocol.

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp protocol-condition]
   user@host# **set protocol-operation** *protocol-operation*

4. (Optional) Configure the value of the IP flags field in the IP header.

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp protocol-condition]
   user@host# **set ip-flags** *ip-flags*

5. (Optional) Configure the mask that is associated with the IP flag.

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp protocol-condition]
   user@host# **set ip-flags-mask** *ip-flags-mask*

6. (Optional) Configure the value of the fragment offset field.

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp protocol-condition]
   user@host# **set fragment-offset** *fragment-offset*

7. (Optional) Configure the packet length on which to match. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead.

   [edit policies group dhcp list in rule forward-dhcp traffic-condition client-dhcp protocol-condition]
   user@host# **set packet-length** *packet-length*

8. (Optional) Verify your protocol condition configuration.

```
[edit policies group dhcp list in rule forward-dhcp traffic-condition
client-dhcp protocol-condition]
user@host# show
protocol 0;
protocol-operation 1;
ip-flags 0;
ip-flags-mask 0;
fragment-offset any;
```

Configuring Protocol Conditions with Ports

Use the following configuration statements to add general protocol conditions with ports to a classify-traffic condition:

policies group *name* list *name* rule *name* traffic-condition *name* protocol-port-condition {
    protocol *protocol*;
    protocol-operation *protocol-operation*;
    ip-flags *ip-flags*;
    ip-flags-mask *ip-flags-mask*;
    fragment-offset *fragment-offset;*
    packet-length *packet-length*;
}

policies group *name* list *name* rule *name* traffic-condition *name* protocol-port-condition destination-port *port* {
    port-operation *port-operation*;
    from-port *from-port*;
}

policies group *name* list *name* rule *name* traffic-condition *name* protocol-port-condition source-port *port* {
    port-operation *port-operation*;
    from-port *from-port*;
}

To add general protocol conditions with ports to a classify-traffic condition:

1. From configuration mode, enter the protocol port condition configuration. For example:

   user@host# **edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition**

2. Configure the protocol matched by this classify-traffic condition.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition]
   user@host# **set protocol** *protocol*

3. Configure the policy to match packets with the protocol that is either equal or not equal to the specified protocol.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition]
   user@host# **set protocol-operation** *protocol-operation*

4. (Optional) Configure the value of the IP flags field in the IP header.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition]
   user@host# **set ip-flags** *ip-flags*

5. (Optional) Configure the mask that is associated with the IP flag.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition]
   user@host# **set ip-flags-mask** *ip-flags-mask*

6. (Optional) Configure the value of the fragment offset field.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition]
   user@host# **set fragment-offset** *fragment-offset*

7. (Optional) Configure the packet length on which to match. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition
   user@host# **set packet-length** *packet-length*

8. (Optional) Enter the destination port configuration for the protocol port configuration.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition]
   user@host# **edit destination-port**

9. (Optional) Configure the policy to match packets with a port that is either equal or not equal to the specified port.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition destination-port port]
   user@host# **set port-operation** *port-operation*

10. (Optional) Configure the destination port.

    [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition destination-port port]
    user@host# **set from-port** *from-port*

11. (Optional) Enter the source port configuration for the protocol port configuration.

    user@host# **up**

    [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition]
    user@host# **edit source-port**

12. (Optional) Configure the policy to match packets with a port that is either equal or not equal to the specified port.

    [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition source-port port]
    user@host# **set port-operation** *port-operation*

13. (Optional) Configure the source port.

    [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition source-port port]
    user@host# **set from-port** *from-port*

    [edit policies group junos list bodVpn rule pr traffic-condition ctc protocol-port-condition source-port port]
    user@host# **up**

14. (Optional) Verify your protocol condition configuration.

```
[edit policies group junos list bodVpn rule pr traffic-condition ctc
protocol-port-condition]
user@host# show
protocol 17;
protocol-operation 1;
ip-flags ipFlags;
ip-flags-mask ipFlagsMask;
fragment-offset ipFragOffset;
packet-length packetLength;
destination-port {
  port {
    port-operation eq;
    from-port service_port;
  }
}
```

```
source-port {
  port {
    port-operation eq;
    from-port service_port;
  }
}
```

Configuring Protocol Conditions with Parameters

Use the following configuration statements to configure classify-traffic conditions that contain a parameter value for the protocol:

policies group *name* list *name* rule *name* traffic-condition *name*
parameter-protocol-condition {
    protocol *protocol*;
    protocol-operation *protocol-operation*;
    tcp-flags *tcp-flags*;
    tcp-flags-mask *tcp-flags-mask*;
    spi *spi*;
    ip-flags *ip-flags*;
    ip-flags-mask *ip-flags-mask*;
    fragment-offset *fragment-offset*;
    packet-length *packet-length*;
}

policies group *name* list *name* rule *name* traffic-condition *name*
parameter-protocol-condition proto-attr {
    icmp-type *icmp-type*;
    icmp-code *icmp-code*;
    igmp-type *igmp-type*;
}

policies group *name* list *name* rule *name* traffic-condition *name*
parameter-protocol-condition proto-attr destination-port port {
    port-operation *port-operation*;
    from-port *from-port*;
}

policies group *name* list *name* rule *name* traffic-condition *name*
parameter-protocol-condition proto-attr source-port port {
    port-operation *port-operation*;
    from-port *from-port*;
}

To configure a protocol condition that contains a parameter value for the protocol:

1. From configuration mode, enter the parameter protocol condition configuration. For example:

   user@host# **edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition**

2. Assign a parameter as the protocol matched by this classify-traffic condition.

   Before you assign a parameter, you must create a parameter of type protocol and commit the parameter configuration.

   [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
   user@host# **set protocol** *protocol*

3. (Optional) Configure the policy to match packets with the protocol that is either equal or not equal to the specified protocol.

   [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
   user@host# **set protocol-operation** *protocol-operation*

4. (Optional) Configure the value of the TCP flags field in the IP header.

   [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
   user@host# **set tcp-flags** *tcp-flags*

5. (Optional) Configure the mask associated with TCP flags.

   [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
   user@host# **set tcp-flags-mask** *tcp-flags-mask*

6. (Optional) Specify the authentication header (AH) or the encapsulating security payload (ESP) security parameter index (SPI).

   [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
   user@host# **set spi** *spi*

7. (Optional) Configure the value of the IP flags field in the IP header.

   [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
   user@host# **set ip-flags** *ip-flags*

8. (Optional) Configure the mask that is associated with the IP flag.

   [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
   user@host# **set ip-flags-mask** *ip-flags-mask*

9. (Optional) Configure the value of the fragment offset field.

   [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
   user@host# **set fragment-offset** *fragment-offset*

10. (Optional) Configure the packet length on which to match. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
    user@host# **set packet-length** *packet-length*

11. (Optional) Enter the protocol attribute configuration.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
    user@host# **edit proto-attr**

12. (Optional) Configure the ICMP packet type.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr]
    user@host# **set icmp-type** *icmp-type*

13. (Optional) Configure the ICMP code.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr]
    user@host# **set icmp-code** *icmp-code*

14. (Optional) Configure the IGMP packet type on which to match.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr]
    user@host# **set igmp-type** *igmp-type*

15. (Optional) Enter the destination port configuration.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr]
    user@host# **edit destination-port port**

16. (Optional) Configure the policy to match packets with a port that is either equal or not equal to the specified port.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr destination-port port]
    user@host# **set port-operation** *port-operation*

17. (Optional) Configure the TCP or UDP destination port.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr destination-port port]
    user@host# **set from-port** *from-port*

18. (Optional) Enter the source port configuration.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr destination-port port]
    user@host# **up**
    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc param-proto-condition proto-attr]
    user@host# **edit source-port port**

19. (Optional) Configure the policy to match packets with a port that is either equal or not equal to the specified port.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr source-port port]
    user@host# **set port-operation** *port-operation*

20. (Optional) Configure the TCP or UDP source port.

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr source-port port]
    user@host# **set from-port** *from-port*

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr source-port port]
    user@host# **up**

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr source-port]
    user@host# **up**

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition proto-attr]
    user@host# **up**

    [edit policies group junose list dhcp rule forward-dhcp traffic-condition ctc parameter-protocol-condition]
    user@host# **up**

21. (Optional) Verify the parameter protocol configuration.

```
[edit policies group junose list dhcp rule forward-dhcp traffic-condition
ctc parameter-protocol-condition]
user@host# show
protocol protocol;
protocol-operation is;
tcp-flags 0;
tcp-flags-mask 0;
ip-flags 0;
ip-flags-mask 0;
proto-attr {
  icmp-type 255;
  icmp-code 255;
```

```
    destination-port {
      port {
        port-operation eq;
        from-port outsidePort;
      }
    }
  }
```

Configuring TCP Conditions

Use the following configuration statements to add TCP conditions to a classify-traffic condition:

policies group *name* list *name* rule *name* traffic-condition *name* tcp-condition {
    tcp-flags *tcp-flags*;
    tcp-flags-mask *tcp-flags-mask*;
    protocol *protocol*;
    protocol-operation *protocol-operation*;
    ip-flags *ip-flags*;
    ip-flags-mask *ip-flags-mask*;
    fragment-offset *fragment-offset*;
    packet-length *packet-length*;
}

Because the protocol is already set to TCP, do not change the protocol or protocol-operation options.

policies group *name* list *name* rule *name* traffic-condition *name* tcp-condition destination-port port {
    port-operation *port-operation*;
    from-port *from-port*;
}

policies group *name* list *name* rule *name* traffic-condition *name* tcp-condition source-port port {
    port-operation *port-operation*;
    from-port *from-port*;
}

To add TCP conditions to a classify-traffic condition:

1. From configuration mode, enter the TCP configuration. For example:

   user@host# **edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition**

2. (Optional) Configure the value of the TCP flags field in the IP header.

   [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition]
   user@host# **set tcp-flags** *tcp-flags*

3. (Optional) Configure the mask associated with TCP flags.

   [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition]
   user@host# **set tcp-flags-mask** *tcp-flags-mask*

4. (Optional) Configure the value of the IP flags field in the IP header.

   [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition]
   user@host# **set ip-flags** *ip-flags*

5. (Optional) Configure the mask that is associated with the IP flag.

   [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition]
   user@host# **set ip-flags-mask** *ip-flags-mask*

6. (Optional) Configure the value of the fragment offset field.

   [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition]
   user@host# **set fragment-offset** *fragment-offset*

7. (Optional) For JUNOS filter policies, configure the packet length on which to match. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead.

   [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition]
   user@host# **set packet-length** *packet-length*

8. (Optional) Enter the destination port configuration for the TCP configuration.

   [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition]
   user@host# **edit destination-port port**

9. (Optional) Configure the policy to match packets with a port that is either equal or not equal to the specified port.

   [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition destination-port port]
   user@host# **set port-operation** *port-operation*

10. (Optional) Configure the destination port.

    [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition destination-port port]
    user@host# **set from-port** *from-port*

11. (Optional) Enter the source port configuration for the TCP configuration.

    [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition destination-port port]
    user@host# **up**

    [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition]
    user@host# **edit source-port port**

12. (Optional) Configure the policy to match packets with a port that is either equal or not equal to the specified port.

    [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition source-port port]
    user@host# **set port-operation** *port-operation*

13. (Optional) Configure the source port.

    [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition source-port port]
    user@host# **set from-port** *from-port*

    [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition source-port port]
    user@host# **up**

    [edit policies group junos list tcpCondition rule pr traffic-condition ctc tcp-condition source-port]
    user@host# **up**

14. (Optional) Verify the TCP condition configuration.

```
[edit policies group junos list tcpCondition rule pr traffic-condition ctc
tcp-condition]
user@host# show
tcp-flags 0;
tcp-flags-mask 0;
protocol tcp;
protocol-operation is;
ip-flags 0;
ip-flags-mask 0;
destination-port {
  port {
    port-operation eq;
    from-port service_port;
  }
}
source-port {
  port {
    port-operation eq;
    from-port service_port;
  }
}
```

Configuring ICMP Conditions

Use the following configuration statements to add ICMP conditions to a classify-traffic condition:

```
policies group name list name rule name traffic-condition name icmp-condition {
    protocol protocol;
    protocol-operation protocol-operation;
    ip-flags ip-flags;
    ip-flags-mask ip-flags-mask;
    fragment-offset fragment-offset;
    packet-length packet-length;
    icmp-type icmp-type;
    icmp-code icmp-code;
}
```

Because the protocol is already set to ICMP, do not change the protocol or protocol-operation options.

To add ICMP conditions to a classify-traffic condition:

1. From configuration mode, enter the ICMP configuration. For example:

   user@host# **edit policies group bod list input rule pr traffic-condition ctc icmp-condition**

2. (Optional) Configure the value of the IP flags field in the IP header.

   [eedit policies group bod list input rule pr traffic-condition ctc icmp-condition]
   user@host# **set ip-flags** *ip-flags*

3. (Optional) Configure the mask that is associated with the IP flag.

   [edit policies group bod list input rule pr traffic-condition ctc icmp-condition]
   user@host# **set ip-flags-mask** *ip-flags-mask*

4. (Optional) Configure the value of the fragment offset field.

   [edit policies group bod list input rule pr traffic-condition ctc icmp-condition]
   user@host# **set fragment-offset** *fragment-offset*

5. (Optional) Configure the packet length on which to match. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead.

   [edit policies group bod list input rule pr traffic-condition ctc icmp-condition]
   user@host# **set packet-length** *packet-length*

6. (Optional) Configure the ICMP packet type on which to match. The packet type must be supported by the router or CMTS device.

   [edit policies group bod list input rule pr traffic-condition ctc icmp-condition]
   user@host# **set icmp-type** *icmp-type*

7. (Optional) Configure the ICMP code on which to match. The ICMP code must be supported by the router or CMTS device.

   [edit policies group bod list input rule pr traffic-condition ctc icmp-condition]
   user@host# **set icmp-code** *icmp-code*

8. (Optional) Verify the ICMP condition configuration.

```
[edit policies group bod list input rule pr traffic-condition ctc
icmp-condition]
user@host# show
protocol icmp;
protocol-operation 1;
ip-flags ipFlags;
ip-flags-mask ipFlagsMask;
fragment-offset ipFragOffset;
icmp-type icmpType;
icmp-code icmpCode;
```

Configuring IGMP Conditions

Use the following configuration statements to add IGMP conditions to a classify-traffic condition:

policies group *name* list *name* rule *name* traffic-condition *name* igmp-condition {
    protocol *protocol*;
    protocol-operation *protocol-operation*;
    ip-flags *ip-flags;*
    ip-flags-mask *ip-flags-mask*;
    fragment-offset *fragment-offset*;
    packet-length *packet-length*;
    igmp-type *igmp-type*;
}

Because the protocol is already set to IGMP, do not change the protocol or protocol-operation options.

To add IGMP conditions to a classify-traffic condition:

1. From configuration mode, enter the IGMP configuration. For example:

   user@host# **edit policies group junose list pl rule pr traffic-condition ctc igmp-condition**

2. (Optional) Configure the value of the IP flags field in the IP header.

   [edit policies group junose list pl rule pr traffic-condition ctc igmp-condition]
   user@host# **set ip-flags** *ip-flags*

3. (Optional) Configure the mask that is associated with the IP flag.

   [edit policies group junose list pl rule pr traffic-condition ctc igmp-condition]
   user@host# **set ip-flags-mask** *ip-flags-mask*

4. (Optional) Configure the value of the fragment offset field.

   [edit policies group junose list pl rule pr traffic-condition ctc igmp-condition]
   user@host# **set fragment-offset** *fragment-offset*

5. (Optional) Configure the packet length on which to match. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead.

   [edit policies group junose list pl rule pr traffic-condition ctc igmp-condition]
   user@host# **set packet-length** *packet-length*

6. (Optional) Configure the IGMP packet type on which to match.

   [edit policies group junose list pl rule pr traffic-condition ctc igmp-condition]
   user@host# **set igmp-type** *icmp-type*

7. (Optional) Verify the IGMP condition configuration.

```
[edit policies group junose list pl rule pr traffic-condition ctc
igmp-condition]
user@host# show
protocol igmp;
protocol-operation 1;
ip-flags 0;
ip-flags-mask 0;
fragment-offset 0;
igmp-type igmpType;
```

Configuring IPSec Conditions

You can configure IPSec conditions for JUNOS policy rules. Use the following configuration statements to add IPSec conditions to a classify-traffic condition:

policies group *name* list *name* rule *name* traffic-condition *name* ipsec-condition {
    spi *spi*;
    ip-flags *ip-flags*;
    ip-flags-mask *ip-flags-mask*;
    fragment-offset *fragment-offset*;
    packet-length *packet-length*;
    protocol *protocol*;
    protocol-operation *protocol-operation;*
}

To add IPSec conditions to a classify-traffic condition:

1. From configuration mode, enter the IPSec configuration. For example:

   user@host# **edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition**

2. (Optional) Specify the authentication header (AH) or the encapsulating security payload (ESP) security parameter index (SPI).

   [edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
   user@host# **set spi** *spi*

3. (Optional) Configure the value of the IP flags field in the IP header.

   [edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
   user@host# **set ip-flags** *ip-flags*

4. (Optional) Configure the mask that is associated with the IP flag.

   [edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
   user@host# **set ip-flags-mask** *ip-flags-mask*

5. (Optional) Configure the value of the fragment offset field.

   [edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
   user@host# **set fragment-offset** *fragment-offset*

6. (Optional) Configure the packet length on which to match. The length refers only to the IP packet, including the packet header, and does not include any layer 2 encapsulation overhead.

   [eedit policies group vpn list input rule pr traffic-condition ctc ipsec-condition]
   user@host# **set packet-length** *packet-length*

7. Configure the protocol matched by this classify-traffic condition.

   [edit policies group vpn list input rule pr traffic-condition ctc ipsec-condition
   user@host# **set protocol** *protocol*

8. (Optional) Verify the IPSec condition configuration.

```
[edit policies group vpn list input rule pr traffic-condition ctc
ipsec-condition
user@host# show
spi 2;
ip-flags 0;
ip-flags-mask 0;
fragment-offset 0;
packet-length packetLength;
protocol ah;
protocol-operation 1;
```

Configuring ToS Byte Conditions

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.

Use the following configuration statements to add ToS conditions to a classify-traffic condition:

policies group *name* list *name* rule *name* traffic-condition *name* tos {
    tos-byte *tos-byte*;
    tos-byte-mask *tos-byte-mask*;
}

To add ToS conditions to a classify-traffic condition:

1. From configuration mode, enter the ToS configuration. For example:

   user@host# **edit policies group junos list bodVpn rule pr traffic-condition ctc tos**

2. (Optional) Configure the value of the ToS byte in the IP packet header.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc tos]
   user@host# **set tos-byte** *tos-byte*

3. (Optional) Configure the mask associated with the ToS byte.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc tos]
   user@host# **set tos-byte-mask** *tos-byte-mask*

4. (Optional) Verify the ToS condition configuration.

```
[edit policies group junos list bodVpn rule pr traffic-condition ctc tos]
user@host# show
tos-byte tosByte;
tos-byte-mask tosMask;
```

Configuring JUNOS Filter Conditions

Use the following configuration statements to configure JUNOS filter conditions.

```
policies group name list name rule name traffic-condition name traffic-match-condition {
    forwarding-class forwarding-class;
    interface-group interface-group;
    source-class source-class;
    destination-class destination-class;
    allow-ip-options allow-ip-options;
}
```

To add JUNOS filter conditions to a classify-traffic condition:

1. From configuration mode, enter the application protocol configuration. For example:

   user@host# **edit policies group junos list bodVpn rule pr traffic-condition ctc traffic-match-condition**

2. (Optional) Configure the name of a forwarding class to match.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc traffic-match-condition]
   user@host# **set forwarding-class** *forwarding-class*

3. (Optional) Configure the condition to match packets based on the interface group on which the packet was received.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc traffic-match-condition
   user@host# **set interface-group** *interface-group*

4. (Optional) Configure the condition to match packets based on source class. A source class is a set of source prefixes grouped together and given a class name. You usually match source and destination classes for output firewall filters.

   You cannot match on both source class and destination class at the same time. You must choose one or the other.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc traffic-match-condition]
   user@host# **set source-class** *source-class*

5. (Optional) Configure the condition to match packets based on destination class. A destination class is a set of destination prefixes grouped together and given a class name. You usually match source and destination classes for output firewall filters.

   You cannot match on both source class and destination class at the same time. You must choose one or the other.

   [edit policies group junos list bodVpn rule pr traffic-condition ctc traffic-match-condition]
   user@host# **set destination-class** *destination-class*

6. (Optional) Configure the condition to match packets based on IP options.

[edit policies group junos list bodVpn rule pr traffic-condition ctc traffic-match-condition]
user@host# **set allow-ip-options** *allow-ip-options*

7. (Optional) Verify the JUNOS filter condition configuration.

```
[edit policies group junos list bodVpn rule pr traffic-condition ctc
traffic-match-condition]
user@host# show
forwarding-class fc_expedited;
interface-group 42;
source-class gold-class;
destination-class gold-class;
allow-ip-options strict-source-route;
```

Configuring Application Protocol Conditions

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.

Use the following configuration statements to add application protocol conditions to a classify-traffic condition:

policies group *name* list *name* rule *name* traffic-condition *name*
application-protocol-condition *name* {
    protocol *protocol*;
    application-protocol *application-protocol*;
    idle-timeout *idle-timeout*;
    dce-rpc-uuid *dce-rpc-uuid*;
    rpc-program-number *rpc-program-number*;
    snmp-command s*nmp-command*;
    ttl-threshold *ttl-threshold*;
}

policies group *name* list *name* rule *name* traffic-condition *name*
application-protocol-condition *name* proto-attr {
    icmp-type *icmp-type*;
    icmp-code *icmp-code*;
}

policies group *name* list *name* rule *name* traffic-condition *name*
application-protocol-condition *name* proto-attr destination-port port {
from-port *from-port*;
}

policies group *name* list *name* rule *name* traffic-condition *name*
application-protocol-condition *name* proto-attr source-port port {
    from-port *from-port*;
}

To add application protocol conditions to a classify-traffic condition:

1. From configuration mode, enter the application protocol configuration. In this procedure, apc is the name of the application protocol condition. For example:

   user@host# **edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc**

2. (Optional) Configure the network protocol to match.

   [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc]
   user@host# **set protocol** *protocol*

3. (Optional) Configure the application protocol to match.

   [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc]
   user@host# **set application-protocol** *application-protocol*

4. (Optional) Configure the length of time the application is inactive before it times out.

   [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc]
   user@host# **set idle-timeout** *idle-timeout*

5. (Optional) For the DCE RPC application protocol, configure the universal unique identifier (UUID).

   [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc]
   user@host# **set dce-rpc-uuid** *dce-rpc-uuid*

6. (Optional) For the remote procedure call (RPC) application protocol, configure an RPC program number.

   [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc]
   user@host# **set rpc-program-number** *rpc-program-number*

7. (Optional) Configure the SNMP command for packet matching.

   [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc]
   user@host# **set snmp-command** *snmp-command*

8. (Optional) For the traceroute application protocol, configure the traceroute time-to-live (TTL) threshold value. This value sets the acceptable level of network penetration for trace routing.

   [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc]
   user@host# **set ttl-threshold** *ttl-threshold*

9. (Optional) Enter configuration mode for the protocol attribute.

   [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc]
   user@host# **edit proto-attr**

10. (Optional) For the ICMP protocol, configure the ICMP packet type.

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr]
    user@host# **set icmp-type** *icmp-type*

11. (Optional) For the ICMP protocol, configure the ICMP code.

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr]
    user@host# **set icmp-code** *icmp-code*

12. (Optional) Enter the destination port configuration.

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr]
    user@host# **edit destination-port port**

13. (Optional) Configure the TCP or UDP destination port.

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr destination-port port]
    user@host# **set from-port** *from-port*

14. (Optional) Enter the source port configuration.

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr destination-port port]
    user@host# **up**

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr]
    user@host# **edit source-port port**

15. (Optional) Configure the TCP or UDP source port.

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr source-port port]
    user@host# **set from-port** *from-port*

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr source-port port]
    user@host# **up**

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr source-port]
    user@host# **up**

    [edit policies group junos list staticnat rule nat traffic-condition ctc application-protocol-condition apc proto-attr]
    user@host# **up**

```
[edit policies group junos list staticnat rule nat traffic-condition ctc
application-protocol-condition apc proto-attr]
user@host# up
```

16. (Optional) Verify the application protocol condition configuration.

```
[edit policies group junos list staticnat rule nat traffic-condition ctc
application-protocol-condition apc]
user@host# show
protocol ip;
application-protocol dce_rpc;
idle-timeout 900;
dce-rpc-uuid dce_rpc;
snmp-command get;
ttl-threshold 25;
proto-attr {
  icmp-type icmpType;
  icmp-code icmpCode;
  destination-port {
    port {
      from-port 11..655;
    }
  }
  source-port {
    port {
      from-port service_port;
    }
  }
}
```

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 option—the application-protocol option. 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 option. "

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

You can also create a local parameter, add a map expression as the default value of the parameter, and then enter the local parameter in the application-protocol option.

Configuring QoS Conditions

You can create QoS conditions within JUNOS scheduler policy rules. Use the following configuration statements to configure a QoS condition:

```
policies group name list name rule name qos-condition name {
    forwarding-class forwarding-class;
    description description;
}
```

To create a QoS condition:

1. From configuration mode, enter the QoS condition configuration. For example:

   ```
   user@host# edit policies group junos list qos rule pr qos-condition qc
   ```

2. (Optional) Configure the forwarding class to match.

   ```
   [edit policies group junos list qos rule pr qos-condition qc]
   user@host# set forwarding-class forwarding-class
   ```

3. (Optional) Enter a description of the QoS condition.

   ```
   [edit policies group junos list qos rule pr qos-condition qc]
   user@host# set description description
   ```

4. (Optional) Verify the QoS condition configuration.

   ```
   [edit policies group junos list qos rule pr qos-condition qc]
   user@host# show
   forwarding-class assured-forwarding;
   description "QoS condition for QoS scheduling";
   ```

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.

Configure the action as described in the following sections:

Configuring DOCSIS Actions

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

Use the following configuration statements to configure DOCSIS actions. Use the configuration statement for the service flow scheduling type that you want to use for the DOCSIS action. The types are best effort, downstream, non-real-time polling service, real-time polling service, unsolicited grant service, unsolicited grant service with activity detection, or parameter.

```
policies group name list name rule name docsis-best-effort name {
    traffic-priority traffic-priority;
    request-transmission-policy request-transmission-policy;
    maximum-sustained-rate maximum-sustained-rate;
    maximum-traffic-burst maximum-traffic-burst;
    minimum-reserved-rate minimum-reserved-rate;
    assumed-minimum-res-packet-size assumed-minimum-res-packet-size;
    description description;
}

policies group name list name rule name docsis-down-stream name {
    traffic-priority traffic-priority;
    maximum-latency maximum-latency;
    maximum-sustained-rate maximum-sustained-rate;
    maximum-traffic-burst maximum-traffic-burst;
    minimum-reserved-rate minimum-reserved-rate;
    assumed-minimum-res-packet-size assumed-minimum-res-packet-size;
    description description;
}

policies group name list name rule name docsis-non-real-time name {
    traffic-priority traffic-priority;
    request-transmission-policy request-transmission-policy;
    maximum-sustained-rate maximum-sustained-rate;
    maximum-traffic-burst maximum-traffic-burst;
    minimum-reserved-rate minimum-reserved-rate;
    assumed-minimum-res-packet-size assumed-minimum-res-packet-size;
    nominal-polling-interval nominal-polling-interval;
    description description;
}

policies group name list name rule name docsis-real-time name {
    request-transmission-policy request-transmission-policy;
    maximum-sustained-rate maximum-sustained-rate;
    maximum-traffic-burst maximum-traffic-burst;
    minimum-reserved-rate minimum-reserved-rate;
    assumed-minimum-res-packet-size assumed-minimum-res-packet-size;
    nominal-polling-interval nominal-polling-interval;
    tolerated-poll-jitter tolerated-poll-jitter;
    description description;
}
```

```
policies group name list name rule name docsis-unsolicited-grant name {
    request-transmission-policy request-transmission-policy;
    grant-size grant-size;
    grants-per-interval grants-per-interval;
    tolerated-grant-jitter tolerated-grant-jitter;
    nominal-grant-interval nominal-grant-interval;
    description description;
}

policies group name list name rule name docsis-unsolicited-grant-ad name {
    request-transmission-policy request-transmission-policy;
    nominal-polling-interval nominal-polling-interval;
    grant-size grant-size;
    grants-per-interval grants-per-interval;
    tolerated-grant-jitter tolerated-grant-jitter;
    nominal-grant-interval nominal-grant-interval;
    description description;
}

policies group name list name rule name docsis-param name {
    service-flow-type service-flow-type;
    traffic-priority traffic-priority;
    request-transmission-policy request-transmission-policy;
    maximum-sustained-rate maximum-sustained-rate;
    maximum-traffic-burst maximum-traffic-burst;
    minimum-reserved-rate minimum-reserved-rate;
    assumed-minimum-res-packet-size assumed-minimum-res-packet-size;
    maximum-latency maximum-latency;
    nominal-polling-interval nominal-polling-interval;
    tolerated-poll-jitter tolerated-poll-jitter;
    grant-size grant-size;
    grants-per-interval grants-per-interval;
    tolerated-grant-jitter tolerated-grant-jitter;
    nominal-grant-interval nominal-grant-interval;
    description description;
}
```

To configure a DOCSIS action:

1. From configuration mode, enter the DOCSIS action configuration. For example, in this procedure, DOCSISParameter is the name of the DOCSIS action.

   ```
   user@host# edit policies group pcmm list DocsisParameter rule in docsis-param
   DOCSISParameter
   ```

2. Assign a parameter as the service flow scheduling type.

   Before you assign a parameter, you must create a parameter of type trafficProfileType and commit the parameter configuration.

   ```
   [edit policies group pcmm list DocsisParameter rule in docsis-param
   DOCSISParameter]
   user@host# set service-flow-type service-flow-type
   ```

3. (Optional) Configure a 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.

   [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
   user@host# **set traffic-priority** *traffic-priority*

4. (Optional) Configure the request transmission policy, which is the interval usage code that the cable modem uses for upstream transmission requests and packet transmissions for this service flow. It also specifies whether requests can be piggybacked with data.

   - For data packets transmitted on this service flow, this option also specifies whether packets can be concatenated, fragmented, or have their payload headers suppressed.

   - For UGS service flows, this option also specifies how to treat packets that do not fit into the UGS grant.

   [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
   user@host# **set request-transmission-policy** *request-transmission-policy*

5. (Optional) Configure the maximum sustained rate at which traffic can operate over the service flow.

   [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
   user@host# **set maximum-sustained-rate** *maximum-sustained-rate*

6. (Optional) Configure the maximum burst size for the service flow. This option has no effect unless you configure a nonzero value for the maximum sustained rate.

   [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
   user@host# **set maximum-traffic-burst** *maximum-traffic-burst*

7. (Optional) Configure the guaranteed minimum rate that is reserved for the service flow.

   [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
   user@host# **set minimum-reserved-rate** *minimum-reserved-rate*

8. (Optional) Configure the 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 option.

   [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
   user@host# **set assumed-minimum-res-packet-size** *assumed-minimum-res-packet-size*

9. (Optional) Configure the 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.

   [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
   user@host# **set maximum-latency** *maximum-latency*

10. (Optional) Configure the nominal interval between successive unicast request opportunities for this service flow.

    [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
    user@host# **set nominal-polling-interval** *nominal-polling-interval*

11. (Optional) Configure the maximum amount of time that unicast request intervals can be delayed beyond the nominal polling interval.

    [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
    user@host# **set tolerated-poll-jitter** *tolerated-poll-jitter*

12. (Optional) Configure the size of the individual data grants provided to the service flow.

    [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
    user@host# **set grant-size** *grant-size*

13. (Optional) Configure the actual number of data grants given to the service flow during each nominal grant interval.

    [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
    user@host# **set grants-per-interval** *grants-per-interval*

14. (Optional) Configure the maximum amount of time that the transmission opportunities can be delayed beyond the nominal grant interval.

    [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
    user@host# **set tolerated-grant-jitter** *tolerated-grant-jitter*

15. (Optional) Configure the nominal interval between successive unsolicited data grant opportunities for this service flow.

    [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
    user@host# **set nominal-grant-interval** *nominal-grant-interval*

16. (Optional) Enter a description for the filter action.

    [edit policies group pcmm list DocsisParameter rule in docsis-param DOCSISParameter]
    user@host# **set description** *description*

17. (Optional) Verify the DOCSIS action configuration.

```
[edit policies group pcmm list DocsisParameter rule in docsis-param
DOCSISParameter]
user@host# show
service-flow-type action;
traffic-priority 1;
request-transmission-policy 1;
maximum-sustained-rate 1500;
maximum-traffic-burst 3044;
minimum-reserved-rate 1240;
assumed-minimum-res-packet-size 124;
description "DOCSIS parameter action with a parameter service flow
scheduling type";
```

Configuring Filter Actions

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

Use the following configuration statement to configure a filter action:

policies group *name* list *name* rule *name* filter *name* {
    description *description*;
}

To configure a filter action:

1. From configuration mode, enter the filter action configuration. For example, in this procedure, fa is the name of the filter action.

   user@host# **edit policies group junos_filter list in rule pr filter fa**

2. (Optional) Enter a description for the filter action.

   [edit policies group junos_filter list in rule pr filter fa]
   user@host# **set description** *description*

3. (Optional) Verify the filter action configuration.

```
[edit policies group junos_filter list in rule pr filter fa]
user@host# show
description "Filter action for JUNOS policies";
```

Configuring FlowSpec Actions

A FlowSpec is made up of two parts, a traffic specification (TSpec) and a service request specification (RSpec). The TSpec describes the traffic requirements for the flow, and the RSpec specifies resource requirements for the desired service. You can configure FlowSpec actions for PCMM policy rules.

Use the following configuration statements to configure FlowSpec actions:

```
policies group name list name rule name flow-spec name {
    service-type service-type;
    token-bucket-rate token-bucket-rate;
    token-bucket-size token-bucket-size;
    peak-data-rate peak-data-rate;
    minimum-policed-unit minimum-policed-unit;
    maximum-packet-size maximum-packet-size;
    rate rate;
    slack-term slack-term;
    description description;
}
```

To configure a FlowSpec action:

1. From configuration mode, enter the FlowSpec action configuration. For example in this procedure, fsa is the name of the FlowSpec action.

   user@host# **edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa**

2. (Optional) Configure the type of FlowSpec service as either controlled_load_service or guaranteed_service. The FlowSpec options available for configuration change depending on the type of service that you select:

   - Controlled load services can contain only TSpec parameters.
   - Guaranteed services can contain both TSpec and RSpec parameters.

   [edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
   user@host# **set service-type** *service-type*

3. (Optional TSpec parameter) Configure the guaranteed minimum rate that is reserved for the service flow.

   [edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
   user@host# **set token-bucket-rate** *token-bucket-rate*

4. (Optional TSpec parameter) Configure the maximum burst size for the service flow.

   [edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
   user@host# **set token-bucket-size** *token-bucket-size*

5. (Optional TSpec parameter) Configure the amount of bandwidth over the committed rate that is allocated to accommodate excess traffic flow over the committed rate.

   [edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
   user@host# **set peak-data-rate** *peak-data-rate*

6. (Optional TSpec parameter) Configure the 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 option.

   [edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
   user@host# **set minimum-policed-unit** *minimum-policed-unit*

7. (Optional TSpec parameter) Configure the maximum packet size for the FlowSpec.

   [edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
   user@host# **set maximum-packet-size** *maximum-packet-size*

8. (Optional RSpec parameter) Configure the average rate.

   [edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
   user@host# **set rate** *rate*

9. (Optional RSpec parameter) Configure the amount of slack in the bandwidth reservation that can be used without redefining the reservation.

   [edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
   user@host# **set slack-term** *slack-term*

10. (Optional) Configure a description for the FlowSpec action.

    [edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
    user@host# **set description** *description*

11. (Optional) Verify the FlowSpec action configuration.

```
[edit policies group pcmm list TrafficProfileFlowSpec rule pr flow-spec fsa]
user@host# show
service-number guaranteed_service;
token-bucket-rate bucketRate;
token-bucket-size bucketDepth;
peak-data-rate peakRate;
minimum-policed-unit minPolicedUnit;
rate reservedRate;
slack-term slackTerm;
description "FlowSpec guaranteed service";
```

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.

Use the following configuration statement to configure forward actions:

```
policies group name list name rule name forward name {
    description description;
}
```

To configure a forward action:

1. From configuration mode, enter the forward action configuration. For example, in this procedure, fwdAction is the name of the forward action.

   ```
   user@host# edit policies group junose list forward rule pr forward fwdAction
   ```

2. (Optional) Enter a description for the forward action.

   ```
   [edit policies group junose list forward rule pr forward fwdAction]
   user@host# set description description
   ```

3. (Optional) Verify the forward action configuration.

   ```
   [edit policies group junose list forward rule pr forward fwdAction]
   user@host# show
   description "JUNOS Forward Action";
   ```

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.

Use the following configuration statements to configure a forwarding class action:

```
policies group name list name rule name forwarding-class name {
    forwarding-class forwarding-class;
    description description;
}
```

To configure a forwarding class action:

1. From configuration mode, enter the forwarding class action configuration. For example, in this procedure, fca is the name of the forwarding class action.

   ```
   user@host# edit policies group bod list input rule pr forwarding-class fca
   ```

2. (Optional) Configure the name of the forwarding class assigned to packets.

   ```
   [edit policies group bod list input rule pr forwarding-class fca]
   user@host# set forwarding-class forwarding-class
   ```

3. (Optional) Enter a description for the forwarding class action.

   [edit policies group bod list input rule pr forwarding-class fca]
   user@host# **set description** *description*

4. (Optional) Verify the forwarding class action configuration.

```
[edit policies group bod list input rule pr forwarding-class fca]
user@host# show
forwarding-class fc_expedited;
description "Expedited forwarding class";
```

Configuring GateSpec Actions

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

Use the following configuration statements to configure GateSpec actions:

policies group *name* list *name* rule *name* gate-spec *name* {
    session-class-id-priority *session-class-id-priority*;
    session-class-id-preemption *session-class-id-preemption*;
    session-class-id-configurable *session-class-id-configurable*;
    description *description*;
}

To configure a GateSpec action:

1. From configuration mode, enter the GateSpec action configuration. For example, in this procedure, gsa is the name of the GateSpec action.

   user@host# **edit policies group pcmm list GateSpec rule pr gate-spec gsa**

2. (Optional) Configure the priority bits in the session class ID. The priority describes the relative importance of the session as compared with other sessions generated by the same policy decision point.

   [edit policies group pcmm list GateSpec rule pr gate-spec gsa]
   user@host# **set session-class-id-priority** *session-class-id-priority*

3. (Optional) Configure the preemption bit in the session class ID. Use the preemption bit to allocate bandwidth to lower-priority sessions.

   [edit policies group pcmm list GateSpec rule pr gate-spec gsa]
   user@host# **set session-class-id-preemption** *session-class-id-preemption*

4. (Optional) Configure the configurable bit in the session class ID.

   [edit policies group pcmm list GateSpec rule pr gate-spec gsa]
   user@host# **set session-class-id-configurable** *session-class-id-configurable*

5. (Optional) Enter a description for the GateSpec action.

   [edit policies group pcmm list GateSpec rule pr gate-spec gsa]
   user@host# **set description** *description*

6. (Optional) Verify the GateSpec action configuration.

```
[edit policies group pcmm list GateSpec rule pr gate-spec gsa]
user@host# show
session-class-id-priority 5;
session-class-id-preemption 0;
session-class-id-configurable 5
```

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.

Use the following configuration statements to configure loss priority actions:

policies group *name* list *name* rule *name* loss-priority *name* {
    loss-priority *loss-priority*;
    description *description*;
}

To configure a loss priority action:

1. From configuration mode, enter the loss priority action configuration. For example, in this procedure, lpa is the name of the loss priority action.

   user@host# **edit policies group junos list lossPriority rule pr loss-priority lpa**

2. (Optional) Configure the packet loss priority.

   [edit policies group junos list lossPriority rule pr loss-priority lpa]
   user@host# **set loss-priority** *loss-priority*

3. (Optional) Enter a description for the loss priority action.

   [edit policies group junos list lossPriority rule pr loss-priority lpa]
   user@host# **set description** *description*

4. (Optional) Verify the loss priority action configuration.

```
[edit policies group junos list lossPriority rule pr loss-priority lpa]
user@host# show
loss-priority high_priority;
description "Loss Priority set to high";
```

Configuring Mark Actions

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

Use the following configuration statements to configure a mark action:

```
policies group name list name rule name mark name {
    description description;
}

policies group name list name rule name mark name info {
    value value;
    mask mask;
}
```

To configure a mark action:

1. From configuration mode, enter the mark action configuration. For example, in this procedure, markAction is the name of the mark action.

   ```
   user@host# edit policies group junose list mark rule pr mark markAction
   ```

2. (Optional) Enter a description for the mark action.

   ```
   [edit policies group junose list mark rule pr mark markAction]
   user@host# set description description
   ```

3. (Optional) Configure the mark value.

   ```
   [edit policies group junose list mark rule pr mark markAction]
   user@host# set info value value
   ```

4. (Optional) Configure the mark mask.

   ```
   [edit policies group junose list mark rule pr mark markAction]
   user@host# set info mask mask
   ```

5. (Optional) Verify the mark action configuration.

   ```
   [edit policies group junose list mark rule pr mark markAction]
   user@host# show
   info {
     mark-value 10;
     mask 255;
   }
   description "Mark action";
   ```

Configuring NAT Actions

You can configure NAT actions for JUNOS ASP policy rules.

Use the following configuration statements to configure NAT actions:

```
policies group name list name rule name nat name {
    translation-type translation-type;
    description description;
}

policies group name list name rule name nat name port {
    from-port from-port;
}

policies group name list name rule name nat name ip-network group-network {
    network-specifier network-specifier;
}
```

To configure a NAT action:

1. From configuration mode, enter the NAT action configuration. For example, in this procedure, natAction is the name of the NAT action.

   user@host# **edit policies group junos list nat rule pr nat natAction**

2. (Optional) Configure the type of network address translation that is used.

   [edit policies group junos list nat rule pr nat natAction]
   user@host# **set translation-type** *translation-type*

3. (Optional) Enter a description for the NAT action.

   [edit policies group junos list nat rule pr nat natAction]
   user@host# **set description** *description*

4. (Optional) Configure the port range to restrict port translation when the NAT translation type is configured in dynamic-source mode.

   [edit policies group junos list nat rule pr nat natAction]
   user@host# **set port from-port** *from-port*

5. (Optional) Configure the IP address ranges.

   [edit policies group junos list nat rule pr nat natAction]
   user@host# **set ip-network group-network network-specifier** *network-specifier*

6. (Optional) Verify the NAT action configuration.

```
[edit policies group junos list nat rule pr nat natAction]
user@host# show
translation-type "source dynamic";
ip-network {
  group-network {
    network-specifier 192.168.1.100/32;
  }
}
port {
  from-port 2010..2020;
}
```

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.

Using the Next-Hop Action with the Captive Portal

The captive portal feature is used to intercept HTTP requests from a subscriber to an unauthorized Web resource and redirect the requests to a dedicated Web page, the captive portal page. See *Redirecting Traffic to a Captive Portal Web Page* in *SRC-PE Subscribers and Subscriptions Guide, Chapter 18, Developing a Residential Portal*.

In a captive portal environment, you would typically set up a next-hop action on a subscriber's interface that forwards traffic to the redirect engine. In this case, you would set the next-hop address to the address of the redirect server.

When you set up redirect server redundancy, both the active and redundant redirect servers share a virtual IP address so that subscribers can always reach the active redirect server. Subscribers send requests to the virtual IP address, and the router automatically sends the request to the active redirect server by means of a static route. In this case, you would set the next-hop address to the virtual IP address.

Configuring Next-Hop Action

Use the following configuration statements to configure the next-hop action.

```
policies group name list name rule name next-hop name {
    next-hop-address next-hop-address;
    description description;
}
```

To configure a next-hop action:

1. From configuration mode, enter the next-hop action configuration. For example, in this procedure, nha is the name of the next-hop action.

   user@host# **edit policies group junose list nexthop-to-ssp rule to-ssp next-hop nha**

2. (Optional) Configure the next IP address where the classified packets should go.

   [edit policies group junose list nexthop-to-ssp rule to-ssp next-hop nha]
   user@host# **set next-hop-address** *next-hop-address*

3. (Optional) Enter a description for the next-hop action.

   [edit policies group junose list nexthop-to-ssp rule to-ssp next-hop nha]
   user@host# **set description** *description*

4. (Optional) Verify the next-hop action configuration.

   ```
   [edit policies group junose list nexthop-to-ssp rule to-ssp next-hop nha]
   user@host# show
   next-hop-address virtual_ipAddress;
   description "Next hop action";
   ```

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.

Use the following configuration statements to configure next-interface actions:

```
policies group name list name rule name next-interface name {
    interface-specifier interface-specifier;
    next-hop-address next-hop-address;
    description description;
}
```

To configure a next-interface action:

1. From configuration mode, enter the next-interface action configuration. For example, in this procedure, nextInterface is the name of the next-interface action.

   user@host# **edit policies group redirect list input rule redirect next-interface nextInterface**

2. (Optional) Configure the IP interface to be used as the next interface for packets.

   [edit policies group redirect list input rule redirect next-interface nextInterface]
   user@host# **set interface-specifier** *interface-specifier*

3. (Optional) Configure the next IP address where the classified packets should go. This option is available only in JUNOSe policy rules.

   [edit policies group redirect list input rule redirect next-interface nextInterface]
   user@host# **set next-hop-address** *next-hop-address*

4. (Optional) Enter a description for the next-interface action.

   [edit policies group redirect list input rule redirect next-interface nextInterface]
   user@host# **set description** *description*

5. (Optional) Verify the next-interface action configuration.

```
[edit policies group redirect list input rule redirect next-interface
nextInterface]
user@host# show
interfaceSpec "name='fastethernet3/0'";
next-hop-address 10.10.227.3;
description "Next-interface action for redirect policy";
```

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.

Use the following configuration statement to configure next-rule actions.

policies group *name* list *name* rule *name* next-rule *name* {
    description *description*;
}

To configure a next-rule action:

1. From configuration mode, enter the next-rule action configuration. For example, in this procedure, nra is the name of the next-rule action.

   user@host# **edit policies group junos list filter rule next next-rule nra**

2. (Optional) Enter a description for the next-rule action.

   [edit policies group junos list filter rule next next-rule nra]
   user@host# **set description** *description*

3. (Optional) Verify the next-rule action configuration.

```
[edit policies group junos list filter rule next next-rule nra]
user@host# show configuration policies group junos list filter rule next
next-rule nra
description "Next-rule action";
```

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.

Use the following configuration statements to configure policer actions:

```
policies group name list name rule name policer name {
    bandwidth-limit bandwidth-limit;
    bandwidth-limit-unit bandwidth-limit-unit;
    burst burst;
    description description;
}
```

To configure a policer action:

1. From configuration mode, enter the policer action configuration. For example, in this procedure, pa is the name of the policer action.

   ```
   user@host# edit policies group junos list firewallFilterPolicer rule pr policer pa
   ```

2. (Optional) Configure the traffic rate that, if exceeded, causes the router to take the indicated packet action.

   ```
   [edit policies group junos list firewallFilterPolicer rule pr policer pa]
   user@host# set bandwidth-limit bandwidth-limit
   ```

3. (Optional) Configure the type of value entered for bandwidth limit.

   ```
   [edit policies group junos list firewallFilterPolicer rule pr policer pa]
   user@host# set bandwidth-limit-unit bandwidth-limit-unit
   ```

4. (Optional) Configure the maximum burst size. The minimum recommended value is the maximum transmission unit (MTU) of the IP packets being policed.

   ```
   [edit policies group junos list firewallFilterPolicer rule pr policer pa]
   user@host# set burst burst
   ```

5. (Optional) Enter a description for the policer action.

   ```
   [edit policies group junos list firewallFilterPolicer rule pr policer pa]
   user@host# set description description
   ```

6. (Optional) Verify the policer action configuration.

   ```
   [edit policies group junos list firewallFilterPolicer rule pr policer pa]
   user@host# show
   bandwidth-limit 1048576;
   bandwidth-limit-unit bps;
   burst 15000;
   ```

Configuring the Packet Action for the Policer Action

The packet action specifies the action taken on a packet that exceeds its rate limits. You configure packet actions within policer actions.

Use the following configuration statements to configure a packet action:

policies group *name* list *name* rule *name* policer *name* packet-action *name* ...

```
policies group name list name rule name policer name packet-action name
forwarding-class {
    forwarding-class forwarding-class;
}
```

```
policies group name list name rule name policer name packet-action name loss-priority
{
    loss-priority loss-priority;
}
```

```
policies group name list name rule name policer name packet-action name parameter {
    action action;
}
```

To configure a packet action:

1. From configuration mode, enter the packet action configuration. For example, in this procedure, pktAction is the name of the packet action.

   user@host# **edit policies group junos list firewallFilterPolicer rule pr policer pa packet-action pktAction**

2. (Optional) Configure the action to take on packets that exceed the bandwidth limit configured in the policer action.

   - Filter—Packets are discarded.

     [edit policies group junos list firewallFilterPolicer rule pr policer pa packet-action pktAction]
     user@host# **set filter**

   - Forwarding class—Packets are assigned to the forwarding class that you specify.

     [edit policies group junos list firewallFilterPolicer rule pr policer pa packet-action pktAction]
     user@host# **set forwarding-class** *forwarding-class*

   - Loss priority—Packets are assigned the loss priority that you specify.

     [edit policies group junos list firewallFilterPolicer rule pr policer pa packet-action pktAction]
     user@host# **set loss-priority** *loss-priority*

   - Parameter—The action specified by the parameter is applied. Before you assign a parameter, you must create a parameter of type packetOperation and commit the parameter configuration.

[edit policies group junos list firewallFilterPolicer rule pr policer pa packet-action pktAction]
user@host# **edit parameter**

[edit policies group junos list firewallFilterPolicer rule pr policer pa packet-action pktAction parameter]
user@host# **set action paramAction**

3. (Optional) Verify the policer action configuration.

```
[edit policies group junos list firewallFilterPolicer rule pr policer pa
packet-action pktAction parameter]
user@host# show
packet-action pktAction {
  parameter {
    action PolicyParameterAction;
  }
}
bandwidth-limit 1048576;
bandwidth-limit-unit bps;
burst 15000;
```

Configuring QoS Profile Attachment Actions

Use this action to specify the name of the QoS profile to attach to the router interface when this action is taken. 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*.

Use the following configuration statements to configure QoS profile attachment actions:

policies group *name* list *name* rule *name* qos-attach *name* {
    qos-profile *qos-profile*;
    description *description*;
}

To configure a QoS profile attachment action:

1. From configuration mode, enter the QoS profile attachment action configuration. For example, in this procedure, qos_vod is the name of the QoS profile attachment action.

   user@host# **edit policies group junose list qos rule input qos-attach qos_vod**

2. (Optional) Configure the name of the QoS profile to attach to the JUNOSe interface when this action is taken.

   [edit policies group junose list qos rule input qos-attach qos_vod]
   user@host# **set qos-profile** *qos-profile*

3. (Optional) Enter a description for the QoS profile attachment action.

```
[edit policies group junose list qos rule input qos-attach qos_vod]
user@host# set description description
```

4. (Optional) Verify the QoS profile attachment action configuration.

```
[edit policies group junose list qos rule input qos-attach qos_vod]
user@host# show
qos-profile qp-vod-1024;
description "Action for QoS video-on-demand";
```

Configuring Rate-Limit Actions

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

Use the following configuration statements to configure rate-limit actions:

```
policies group name list name rule name rate-limit name {
    type type;
    committed-rate committed-rate;
    committed-burst committed-burst;
    peak-rate peak-rate;
    peak-burst peak-burst;
    excess-burst excess-burst;
    description description;
}

policies group name list name rule name rate-limit name committed-action mark
mark-info {
    value value;
    mask mask;
}

policies group name list name rule name rate-limit name committed-action parameter {
    action action;
}

policies group name list name rule name rate-limit name conformed-action mark
mark-info {
    value value;
    mask mask;
}

policies group name list name rule name rate-limit name conformed-action parameter {
    action action;
}

policies group name list name rule name rate-limit name exceed-action mark mark-info
{
    value value;
    mask mask;
}
```

```
policies group name list name rule name rate-limit name exceed-action parameter {
    action action;
}
```

To configure a rate-limit action:

1. From configuration mode, enter the rate-limit action configuration. For example, in this procedure, rla is the name of the rate-limit action.

   user@host# **edit policies group junose list rate-limiter rule pr rate-limit rla**

2. (Optional) Specify that the rate-limit profile is either one rate or two rate. The rate-limit type determines the options that you can configure for a rate-limit action.

   [edit policies group junose list rate-limiter rule pr rate-limit rla]
   user@host# **set type** *type*

3. (Optional) Configure the target rate for the traffic that the policy covers.

   [edit policies group junose list rate-limiter rule pr rate-limit rla]
   user@host# **set committed-rate** *committed-rate*

4. (Optional) Configure the amount of bandwidth allocated to burst traffic in bytes.

   [edit policies group junose list rate-limiter rule pr rate-limit rla]
   user@host# **set committed-burst** *committed-burst*

5. (Optional) For two-rate rate-limit profiles, specify the amount of bandwidth allocated to excess traffic flow over the committed rate.

   [edit policies group junose list rate-limiter rule pr rate-limit rla]
   user@host# **set peak-rate** *peak-rate*

6. (Optional) For two-rate rate-limit profiles, specify the amount of bandwidth allocated to burst traffic in excess of the peak rate.

   [edit policies group junose list rate-limiter rule pr rate-limit rla]
   user@host# **set peak-burst** *peak-burst*

7. (Optional) For one-rate rate-limit profiles, specify the amount of bandwidth allocated to accommodate burst traffic.

   [edit policies group junose list rate-limiter rule pr rate-limit rla]
   user@host# **set excess-burst** *excess-burst*

8. (Optional) Enter a description for the rate-limit action.

   [edit policies group junose list rate-limiter rule pr rate-limit rla]
   user@host# **set description** *description*

9. (Optional) Configure the rate-limit action for traffic flows that do not exceed the committed rate to one of the following:

   - Filter.

     [edit policies group junose list rate-limiter rule pr rate-limit rla]
     user@host# **set committed-action filter**

   - Forward.

     [edit policies group junose list rate-limiter rule pr rate-limit rla]
     user@host# **set committed-action forward**

   - Mark. If you select mark, enter the mark values.

     [edit policies group junose list rate-limiter rule pr rate-limit rla]
     user@host# **edit committed-action mark mark-info**

     [edit policies group junose list rate-limiter rule pr rate-limit rla
     committed-action mark mark-info]
     user@host# **set value** *value*

     [edit policies group junose list rate-limiter rule pr rate-limit rla
     committed-action mark mark-info]
     user@host# **set mask** *mask*

   - Parameter. Before you assign a parameter, you must create a parameter of type packetOperation and commit the parameter configuration.

     [edit policies group junose list rate-limiter rule pr rate-limit rla
     committed-action mark mark-info]
     user@host# **set committed-action parameter action** *action*

10. (Optional) Configure the rate-limit action for traffic flows that exceed the committed rate but remain below the peak rate to one of the following:

    - Filter.

      [edit policies group junose list rate-limiter rule pr rate-limit rla]
      user@host# **set conformed-action filter**

    - Forward.

      [edit policies group junose list rate-limiter rule pr rate-limit rla]
      user@host# **set conformed-action forward**

    - Mark. If you select mark, enter the mark values.

      [edit policies group junose list rate-limiter rule pr rate-limit rla]
      user@host# **edit conformed-action mark mark-info**

[edit policies group junose list rate-limiter rule pr rate-limit rla conformed-action mark mark-info]
user@host# **set value** *value*

[edit policies group junose list rate-limiter rule pr rate-limit rla conformed-action mark mark-info]
user@host# **set mask** *mask*

- Parameter. Before you assign a parameter, you must create a parameter of type packetOperation and commit the parameter configuration.

  [edit policies group junose list rate-limiter rule pr rate-limit rla conformed-action mark mark-info]
  user@host# **set conformed-action parameter action** *action*

11. (Optional) Configure the rate-limit action for traffic flows exceed the peak rate to one of the following:

    - Filter.

      [edit policies group junose list rate-limiter rule pr rate-limit rla]
      user@host# **set exceed-action filter**

    - Forward.

      [edit policies group junose list rate-limiter rule pr rate-limit rla]
      user@host# **set exceed-action forward**

    - Mark. If you select mark, enter the mark values.

      [edit policies group junose list rate-limiter rule pr rate-limit rla]
      user@host# **edit exceed-action mark mark-info**

      [edit policies group junose list rate-limiter rule pr rate-limit rla exceed-action mark mark-info]
      user@host# **set value** *value*

      [edit policies group junose list rate-limiter rule pr rate-limit rla exceed-action mark mark-info]
      user@host# **set mask** *mask*

    - Parameter. Before you assign a parameter, you must create a parameter of type packetOperation and commit the parameter configuration.

      [edit policies group junose list rate-limiter rule pr rate-limit rla exceed-action mark mark-info]
      user@host# **set exceed-action parameter action** *action*

12. (Optional) Return to the rate-limit action configuration, and verify the configuration.

```
[edit policies group junose list rate-limiter rule pr rate-limit rla]
user@host# show
committed-action {
  forward {
  }
}
conformed-action {
  forward {
  }
}
exceed-action {
  filter {
  }
}
type 1;
committed-rate 1000000;
committed-burst 125000;
excess-burst 312500;
```

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.

Use the following configuration statements to configure reject actions:

policies group *name* list *name* rule *name* reject *name* {
    message-type *message-type*;
    description *description*;
}

To configure a reject action:

1. From configuration mode, enter the reject action configuration. For example, in this procedure, rejectAction is the name of the reject action.

   user@host# **edit policies group junos list filter rule rejectRule reject rejectAction**

2. (Optional) Configure the type of ICMP destination unreachable message sent to the client.

   [edit policies group junos list filter rule rejectRule reject rejectAction]
   user@host# **set message-type** *message-type*

3. (Optional) Enter a description for the reject action.

   [edit policies group junos list filter rule rejectRule reject rejectAction]
   user@host# **set description** *description*

4. (Optional) Verify the reject action configuration.

```
[edit policies group junos list filter rule rejectRule reject rejectAction]
user@host# show
message-type network-prohibited;
description "Reject action in JUNOS filter policy";
```

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.

Use the following configuration statements to configure routing instance actions:

policies group *name* list *name* rule *name* routing-inst *name* {
    routing-instance *routing-instance*;
    description *description*;
}

To configure a routing instance action:

1. From configuration mode, enter the routing instance action configuration. For example, in this procedure, ria is the name of the routing instance action.

   user@host# **edit policies group junos list bodVpn rule pr routing-inst ria**

2. (Optional) Configure the routing instance to which packets are forwarded. The routing instance must be configured on the router.

   [edit policies group junos list bodVpn rule pr routing-inst ria]
   user@host# **set routing-instance** *routing-instance*

3. (Optional) Enter a description for the reject action.

   [edit policies group junos list bodVpn rule pr routing-inst ria]
   user@host# **set description** *description*

4. (Optional) Verify the routing instance action configuration.

```
[edit policies group junos list bodVpn rule pr routing-inst ria]
user@host# show
routing-instance isp2-route-table;
description "Routing Instance Action";
```

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.

Use the following configuration statements to configure scheduler actions:

```
policies group name list name rule name scheduler-action name {
    buffer-size buffer-size;
    buffer-size-unit buffer-size-unit;
    priority priority;
    transmit-rate transmit-rate;
    transmit-rate-unit transmit-rate-unit;
    exact exact;
    description description;
}
```

To configure a scheduler action:

1. From configuration mode, enter the scheduler action configuration. For example, in this procedure, sa is the name of the scheduler action.

   user@host# **edit policies group junos list qos rule pr scheduler-action sa**

2. (Optional) Configure the queue transmission buffer size.

   [edit policies group junos list qos rule pr scheduler-action sa]
   user@host# **set buffer-size** *buffer-size*

3. (Optional) Configure the type of value that you entered for buffer size.

   [edit policies group junos list qos rule pr scheduler-action sa]
   user@host# **set buffer-size-unit** *buffer-size-unit*

4. (Optional) Configure the packet-scheduling priority. The priority determines the order in which an output interface transmits traffic from the queues.

   [edit policies group junos list qos rule pr scheduler-action sa]
   user@host# **set priority** *priority*

5. (Optional) Configure the transmit rate.

   [edit policies group junos list qos rule pr scheduler-action sa]
   user@host# **set transmit-rate** *transmit-rate*

6. (Optional) Configure the type of value entered for transmit rate.

   [edit policies group junos list qos rule pr scheduler-action sa]
   user@host# **set transmit-rate-unit** *transmit-rate-unit*

7. (Optional) Specify 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.

   [edit policies group junos list qos rule pr scheduler-action sa]
   user@host# **set exact** *exact*

8. (Optional) Enter a description for the scheduler action.

   [edit policies group junos list qos rule pr scheduler-action sa]
   user@host# **set description** *description*

9. (Optional) Verify the scheduler action configuration.

```
[edit policies group junos list qos rule pr scheduler-action sa]
user@host# show
buffer-size 85;
buffer-size-unit buffer_size_percentage;
priority low;
transmit-rate 10485760;
transmit-rate-unit rate_in_bps;
description "Scheduler action for logical interface scheduling";
```

Configuring Drop Profiles

You configure drop profiles within scheduler actions. Drop profiles support the RED process by defining the drop probabilities across the range of delay-buffer occupancy. 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.

In drop profiles you configure the queue threshold 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.

Use the following configuration statements to configure drop profiles:

policies group *name* list *name* rule *name* scheduler-action *name* drop-profile *name* {
    loss-priority *loss-priority*;
    protocol *protocol*;
    drop-probability *drop-probability*;
    drop-profile-type *drop-profile-type*;
    queue-threshold *queue-threshold*;
}

To configure drop profiles:

1. From configuration mode, enter the drop profile configuration. For example, in this procedure, drop1 is the name of the drop profile.

   user@host# **edit policies group junos list qosWithDropProfile rule pr scheduler-action sa drop-profile drop1**

2. Configure the loss priority.

   [edit policies group junos list qosWithDropProfile rule pr scheduler-action sa drop-profile drop1]
   user@host# **set loss-priority** *loss-priority*

3. Configure the protocol type.

   [edit policies group junos list qosWithDropProfile rule pr scheduler-action sa drop-profile drop1]
   user@host# **set protocol** *protocol*

4. Configure the relationship between the fill level and drop probability.

   [edit policies group junos list qosWithDropProfile rule pr scheduler-action sa drop-profile drop1]
   user@host# **set drop-profile-type** *drop-profile-type*

5. Configure the probability that a packet will be dropped.

   [edit policies group junos list qosWithDropProfile rule pr scheduler-action sa drop-profile drop1]
   user@host# **set drop-probability** *drop-probability*

6. Configure the fill level of the queue.

   [edit policies group junos list qosWithDropProfile rule pr scheduler-action sa drop-profile drop1]
   user@host# **set queue-threshold** *queue-threshold*

7. (Optional) Verify the drop profile configuration.

```
[edit policies group junos list qosWithDropProfile rule pr scheduler-action
sa drop-profile drop1]
user@host# show
loss-priority high_priority;
protocol any_protocol;
drop-probability "[75, 100]";
drop-profile-type interpolated;
queue-threshold "[50, 80]";
```

Configuring Service Class Name Actions

You can configure service class name actions for PCMM policy rules. Use the following configuration statements to configure service class name actions:

```
policies group name list name rule name service-class-name name {
    service-class-name service-class-name;
    description description;
}
```

To configure a service class name action:

1. From configuration mode, enter the service class name action configuration. For example, in this procedure, scna is the name of the service class name action.

   ```
   user@host# edit policies group pcmm list serviceClass rule pr
   service-class-name scna
   ```

2. (Optional) Configure the name of a service class on the CMTS device that specifies QoS parameters for a service flow.

   ```
   [edit policies group pcmm list serviceClass rule pr service-class-name scna]
   user@host# set service-class-name service-class-name
   ```

3. (Optional) Enter a description for the service class name action.

   ```
   [edit policies group pcmm list serviceClass rule pr service-class-name scna]
   user@host# set description description
   ```

4. (Optional) Verify the service class name action configuration.

   ```
   [edit policies group pcmm list serviceClass rule pr service-class-name scna]
   user@host# show configuration policies group pcmm list serviceClass rule pr
   service-class-name scna
   service-class-name scn_up;
   description "Service class name action for pcmm service class policy.";
   ```

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.

Use the following configuration statements to configure stateful firewall actions:

```
policies group name list name rule name stateful-firewall name {
    description description;
}

policies group name list name rule name stateful-firewall name packet-action reject {
    message-type message-type;
}

policies group name list name rule name stateful-firewall name packet-action
parameter {
    action action;
}
```

To configure a stateful firewall action:

1. From configuration mode, enter the stateful firewall action configuration. For example, in this procedure, sfa is the name of the stateful firewall action.

   user@host# **edit policies group junos list sfw rule pr stateful-firewall sfa**

2. (Optional) Set the action to take on a packet to one of the following:

   - Filter.

     [edit policies group junos list sfw rule pr stateful-firewall sfa]
     user@host# **set packet-action filter**

   - Forward.

     [edit policies group junos list sfw rule pr stateful-firewall sfa]
     user@host# **set packet-action forward**

   - Reject. If you set the action to reject, configure the type of ICMP destination unreachable message sent to the client.

     [edit policies group junos list sfw rule pr stateful-firewall sfa]
     user@host# **set packet-action reject message-type** *message-type*

   - Parameter. Before you assign a parameter, you must create a parameter of type packetOperation and commit the parameter configuration.

     [edit policies group junos list sfw rule pr stateful-firewall sfa]
     user@host# **set packet-action parameter action** *action*

3. (Optional) Enter a description for the stateful firewall action.

   [edit policies group junos list sfw rule pr stateful-firewall sfa]
   user@host# **set description** *description*

4. (Optional) Verify the stateful firewall action configuration.

```
[edit policies group junos list sfw rule pr stateful-firewall sfa]
user@host# show
packet-action {
  reject {
    message-type administratively-prohibited;
  }
}
description "Stateful firewall action";
```

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.

Use the following configuration statement to configure traffic-class actions:

policies group *name* list *name* rule *name* traffic-class *name* {
    traffic-class *traffic-class*;
    description *description*;
}

To configure a traffic-class action:

1. From configuration mode, enter the traffic-class configuration. For example, in this procedure, tca is the name of the traffic-class action.

   user@host# **edit policies group junose list class rule pr traffic-class tca**

2. (Optional) Configure the name of the traffic-class profile that is applied to a packet when it passes through the router.

   [edit policies group junose list class rule pr traffic-class tca]
   user@host# **set traffic-class** *traffic-class*

3. (Optional) Enter a description for the traffic-class action.

   [edit policies group junose list class rule pr traffic-class tca]
   user@host# **set description** *description*

4. (Optional) Verify the traffic-class action configuration.

```
[edit policies group junose list class rule pr traffic-class tca]
user@host# show
traffic-class TCent;
description "Traffic class action";
```

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 for JUNOS filter 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.

Use the following configuration statement to configure a traffic-mirror action:

```
policies group name list name rule name traffic-mirror name {
    description description;
}
```

To configure a traffic-mirror action:

1. From configuration mode, enter the traffic-mirror configuration. For example, in this procedure, fromSubnets is the name of the traffic-mirror action.

   ```
   user@host# edit policies group junos list mirror rule pr traffic-mirror fromSubnets
   ```

2. (Optional) Enter a description for the traffic-mirror action.

   ```
   [edit policies group junos list mirror rule pr traffic-mirror fromSubnets]
   user@host# set description description
   ```

3. (Optional) Verify the traffic-mirror action configuration.

   ```
   [edit policies group junos list mirror rule pr traffic-mirror fromSubnets]
   user@host# show
   description "Traffic mirroring action for subnet.";
   ```

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.

Use the following configuration statements to configure traffic-shape actions:

```
policies group name list name rule name traffic-shape name {
    rate rate;
    description description;
}
```

To configure a traffic-shape action:

1. From configuration mode, enter the traffic-shape configuration. For example, in this procedure, tsa is the name of the traffic-shape action.

   user@host# **edit policies group junos list trafficShaping rule shaping traffic-shape tsa**

2. (Optional) Configure the maximum transmission rate.

   [edit policies group junos list trafficShaping rule shaping traffic-shape tsa]
   user@host# **set rate** *rate*

3. (Optional) Enter a description for the traffic-shape action.

   [edit policies group junos list trafficShaping rule shaping traffic-shape tsa]
   user@host# **set description** *description*

4. (Optional) Verify the traffic-shape action configuration.

```
[edit policies group junos list trafficShaping rule shaping traffic-shape
tsa]
user@host# show
rate 10200000;
description "Traffic-shaping action";
```