Chapter 6

Policy Management Overview

This chapter provides an overview of the policy management feature. Topics include:

Overview of Policy Management

The SRC software works with Juniper Networks routers and PacketCable Multimedia Specification (PCMM)–compliant cable modem termination system (CMTS) platforms to provide differentiated quality of service (QoS). The SRC software uses policies to define how the router or the CMTS device treats subscriber traffic. Policy management is responsible for defining policies and deploying the policies on a router or CMTS device.

Router Policy Features Supported

This section describes the features that the SRC policy management software supports on JUNOS routing platforms and on JUNOSe routers. For information about features supported on CMTS devices, see *Delivering QoS Services in a Cable Environment* on page 157.

JUNOS Routing Platform Features

The SRC software supports the following features on JUNOS routing platforms:

- JUNOS class-of-service (CoS)

  Allows you to provide differentiated services. You can assign forwarding classes to different applications, set a loss priority, define which packets are placed into each output queue, schedule the transmission service level for each queue, and manage congestion using a random early detection (RED) algorithm. You can also configure a shaping rate for interfaces.

  For complete information about how this feature works on the router, see the *JUNOS Network Interfaces and Class of Service Configuration Guide*.

- Firewall filter

  Allows you to control packets transiting the router to a network destination and packets destined for and sent by the router.

  For complete information about how this feature works on the router, see the *JUNOS Policy Framework Configuration Guide*.

- Policing, or rate limiting

  Enables you to limit the amount of traffic that passes into or out of an interface. Policing is designed to thwart denial-of-service (DoS) attacks. It applies two types of rate limits on the traffic:

  - Bandwidth—Number of bits per second permitted, on average.
  - Maximum burst size—Maximum size permitted for bursts of data that exceed the bandwidth limit.

  For complete information about how this feature works on the router, see the *JUNOS Policy Framework Configuration Guide*.

- Adaptive Services PIC (ASP)

  Supports stateful firewall and network address translation (NAT) services:

  - Stateful firewall—Type of firewall filter that considers state information derived from previous communications and other applications when evaluating traffic.
  - NAT—Security procedure for concealing host addresses on a private network behind a pool of public addresses.

  For complete information about how this feature works on the router, see the *JUNOS Services Interfaces Configuration Guide*.

- Port mirroring

  Allows you to control traffic on the router by mirroring traffic with a preconfigured mirroring port and filtering with a specific policy.

  For complete information about how this feature works on the router, see the *JUNOS Policy Framework Configuration Guide*.

JUNOSe Router Features

The SRC software supports the following policy management features on JUNOSe routers:

- Policy routing

  Allows the router to classify a packet on ingress and make a forwarding decision based on that classification, without performing the normal routing table processing.

- Rate limiting

  Provides bandwidth management by enforcing line rates below the physical line rate of the port and setting limits on packet flows.

- QoS classification and marking

  Marks packets in a packet flow so that the QoS application can provide traffic-class queuing.

- Packet forwarding

  Forwards packets in a packet flow.

- Packet filtering

  Drops packets in a packet flow.

For complete information about how these features work on the router, see the *JUNOSe Policy Management Configuration Guide*.

For more information about using the SRC software to manage QoS services on JUNOSe routers, see *SRC-PE Solutions Guide, Chapter 1, Managing Tiered and Premium Services with QoS on JUNOSe Routers with the SRC CLI*.

Default Policies and Service Policies

The policy management feature provides two types of policies that make it possible for you to control when the policies are deployed; this feature provides dynamic deployment of policies. The two types of policies are:

- Default policies—Are attached to a router interface when the SAE begins to manage the interface, before subscribers activate services. Default policies define the subscriber's initial network access. Typically, they block access to value-added services, restrict a subscriber's bandwidth, or restrict network access altogether.

  If you are using the captive portal in a PCMM environment, you do not need default policies.

- Service policies—Are attached to an interface when a subscriber activates a service; they take priority over the default policy. Service policies allow access to value-added services or provide higher bandwidth. (When you create a service policy, you assign a lower precedence number to the policy rule so that it is preferred over the default policy.)

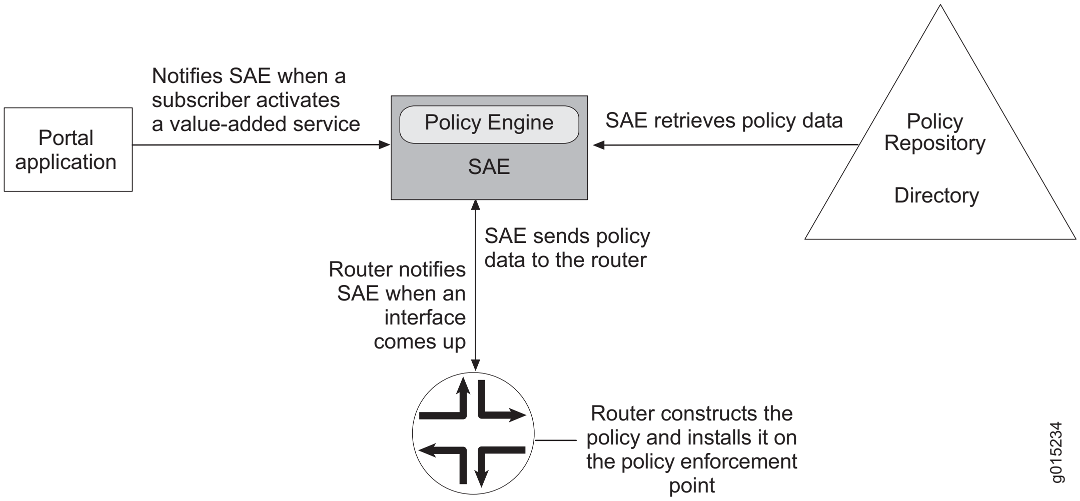
Where you reference the policies determines whether it is a default policy or a service policy. Default policies are referenced in interface classification scripts. Service policies are referenced in value-added service definitions.

How Policies Are Installed on the Router

The policy engine in the SAE makes decisions about the deployment of policies on the router. When the SAE needs to install a policy on the router, it retrieves the policy data from the directory, processes the data, and sends the data to the router. The router uses the data to construct the policy, and then it applies the policy as instructed by the SAE.

Figure 9 gives an overview of how policies are installed on the router.

Figure 9: Installing Policies on the Router


Notifies SAE when a subscriber activates a value-added service
Portal application
Policy Engine
SAE
SAE retrieves policy data
Policy Repository
Directory
SAE sends policy data to the router
Router notifies SAE when an interface comes up
Router constructs the policy and installs it on the policy enforcement point
g015234

Installing Default Policies

When an interface comes up on the router, the SAE runs the interface classification script to determine whether it manages the interface. If the interface is managed—that is, controlled by—the SAE, the SAE sends the default policy referenced in the interface classification script to the router.

Installing and Removing Service Policies

When a subscriber activates a service (for example, video-gold), the portal application notifies the SAE to activate that service. The SAE obtains the policy data associated with the service and sends the data to the router. The router constructs and installs the appropriate policies.

When the subscriber deactivates the service, the portal application passes the request to the SAE, and the SAE notifies the router to remove the policies for the service.

Reloading Default Policies

The SAE reapplies default policies when:

- The definition of a default policy changes.
- The interface classification criteria change.

When the SAE is triggered to reload default policies, it generates default policies for each interface that was previously reported as up. If the default policies have changed compared with the previously applied policies, the current default policies (if any) are removed and the new policies are applied.

NOTE: This behavior means that the SAE also must keep track of unmanaged interfaces to handle changes in the interface classification script.

Policy List Sharing

Policy list sharing is supported on JUNOS routing platforms and on JUNOSe routers that are managed using the COPS-PR router driver. Policy sharing allows the same policy list to be attached to multiple interfaces. Before the SAE modifies policies that are attached to an interface, installs policies on an interface, or removes policies from an interface, it checks whether the requested combination of policy rules already exists on the router.

- If the combination exists, the SAE changes the policy attachment of the interface to use the existing policy. Using an existing policy increases router performance because the router does not have to construct a new policy.

  The router maintains policy counters when it changes policy attachments. To generate accounting data, the SAE reads the policy counters before it deactivates a policy.

- If the combination does not exist, the SAE sends the policy data to the router. The router either creates a new list (if the interface is not managed yet) or modifies the policy list currently attached to the interface.

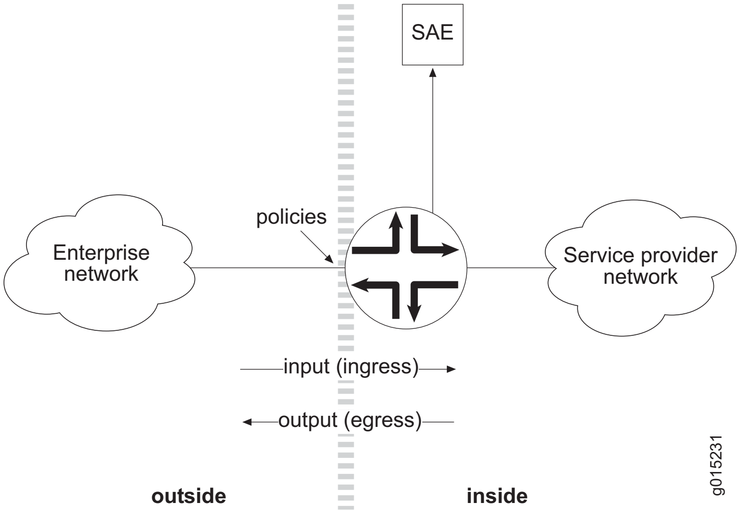
If a policy list is no longer referenced by a session, the SAE removes it from the interface.

Network Perspective for Creating Policies

When you create a policy, you indicate where the policy is applied on the router. You can apply policies to the ingress (input) side of the interface, to the egress (output) side of the interface, to both the ingress and egress sides of the interface, or, in the case of JUNOS scheduler policy rules, you can attach the policy to the interface without indicating direction. Typically, policies are applied to subscriber-facing interfaces.

Figure 10 shows a sample network diagram with an enterprise network and a service provider network. Ingress traffic flows from the enterprise network to the service provider's network. Egress traffic flows from the service provider's network to the enterprise network.

Figure 10: Network Perspective for Creating Policies



Collecting Accounting Statistics

You can specify whether accounting data is collected for the actions specified in a policy rule. If you specify that accounting data is collected, the SAE begins collecting accounting information when a service that uses the policy rule is activated. When the service is deactivated, the SAE sends the accounting records to the RADIUS accounting server or to a plug-in.

When you specify multiple actions for accounting, the SAE adds the accounting data for individual actions together to obtain a summary accounting record for that interface direction.

Accounting is not available for all actions. For example, the NAT action does not provide accounting.

Policy Components

The policy management architecture is fully compliant with Internet Engineering Task Force (IETF) policy management standards. The SRC policy management system uses a distributed architecture with the following components:

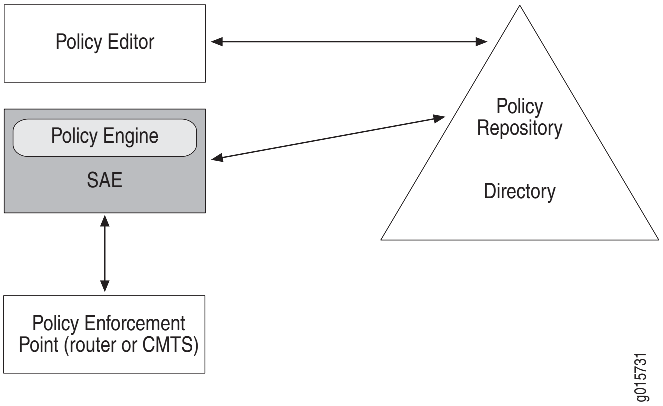
- Policy Editor—Defines and deploys policies
- Policy engine—Resides on the SAE and makes policy decisions (policy decision point)

- Policy enforcement point—Resides on the router or policy server and performs policy management on the router
- Policy repository—Resides in the directory and stores and distributes policies

Figure 11 shows the components of the policy management system. As shown:

1. Policy Editor is used to create policies and maintain policy data in the policy repository.
2. The policy repository distributes policy data to policy engines that are located on SAEs throughout the network.
3. The policy engine uses the policy data to instruct the policy enforcement points to apply appropriate policies to subscriber traffic in the network.

Figure 11: Policy Management Components



Policy Editor

Policy Editor is one of the applications that you use to define policies. It dynamically changes the panes that it provides to you, based on your input. It can show or hide policy object attributes as you interact with it. For example, when you choose the TCP or UDP protocols, the source and destination ports are shown; otherwise, they are not shown.

Policy Editor also allows you to store policy data in a directory server or in files. By storing data in files, you can create a backup of the repository or transfer policies from one repository to another.

See *Chapter 7, Using Policy Editor*.

Policy Engine

The policy engine acts as a policy decision point (PDP) and is responsible for making decisions about the deployment of policies on the router or the CMTS device. The policy engine runs as part of the SAE.

Policy Repository

The policy repository is a directory that stores policies and distributes policies to policy engines.

Policy Enforcement Point

The policy enforcement point is the policy management component of the router that is responsible for enforcing the deployed policies. In cable networks, the policy enforcement point is the CMTS device.

Policy Information Model

Policies are made up of conditions and actions that cause the router to handle packets in a certain way.

- Condition—Defines values or fields that a packet must contain before an action is triggered; for example, packet direction, network protocol, source and destination ports, application protocol, source and destination networks, packet length, forwarding class, source and destination class
- Action—Specifies the action that the router takes on packets that match the condition; for example, filter (drop), forward, send to next interface, apply rate and burst size limits, assign a forwarding class

Here are two examples of policies with conditions and actions:

- A stateful firewall:
  - Condition—Matches input packets to a specific destination network
  - Action—Forwards matching packets
- Controlled access policy that defines the sites that a subscriber can view:
  - Condition—Traffic to and from the restricted site
  - Action—Access to the site is stopped if the site has a restricted rating

The SRC policy information model is designed to consolidate information models from various devices to provide a standard way to configure policies. This way, similar operations on different devices are represented as a single policy action or condition which is translated to device-specific operations. For example, the SRC policy information model provides an action that forwards traffic. This action is translated into actions such as forward, accept, or simple handoff on various routers. For instances in which policy conditions or actions are significantly different, the model provides support for each type of condition or action. For example, because rate-limiting on JUNOSe routers is significantly different than policing on JUNOS routing platforms the SRC provides a rate-limit action for JUNOSe routers and policer action for JUNOS routing platforms.

For JUNOSe routers, SRC policies are translated at the COPS-PR or COPS-XDR level. and at the router level. For JUNOS routing platforms, policies are translated at the JUNOS XML on BEEP level and at the router level.

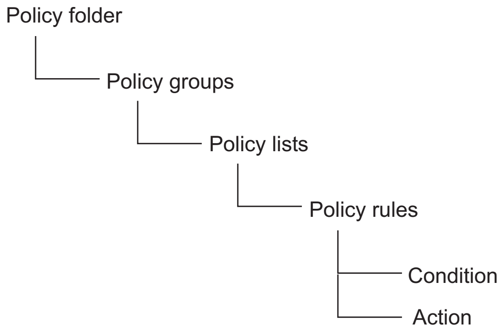
The SRC policy model also lets you simplify policy configuration for policy conditions that classify traffic. For JUNOSe and PCMM policies, you can combine different conditions that classify traffic and configure these conditions to use a single action. In addition for JUNOSe policies, you can create a condition which actually represents a number of classifiers. The SAE expands the classifier to multiple classifiers before installing them on the router.

For more information about multiple classifiers and expanded classifiers, see *Policy Conditions* on page 152.

Policy Objects

The SRC policy model is made up of objects that are organized as shown in Figure 12.

Figure 12: Policy Object Organization



The following is a description of these objects:

- Policy folders—Used to organize policy groups.
- Policy groups—Hold policy lists. You associate policy groups with a service or with an interface. The SAE sends the information in a policy group to the router, and the router uses the information to create policies that it attaches to router interfaces.
- Policy lists—Used to organize policy rules. You can create policy lists for JUNOS routing platforms, for JUNOSe routers, or for PCMM devices. Whether you create a JUNOS policy list, a JUNOSe policy list, or a PCMM policy list determines the types of policy rules that you can add to the policy list.
- Policy rules—Used to organize the conditions and actions that make up the policy rule. Policy rules consist of conditions that you use to match traffic and actions that specify the action to take if traffic matches the condition. In JUNOS terminology, a policy rule is the same as a *term*.
- Conditions—Define match conditions or classifiers that a packet or packet flow must contain; for example, packet direction, network protocol, application protocol, source and destination networks, packet length, forwarding class, and source and destination class
- Actions—Define the action that the router or CMTS device takes on packets that match conditions

Policy Rules

JUNOSe routers and PCMM devices support one type of policy rule. JUNOS routing platforms support five types of policy rules:

- JUNOS Adaptive Services PIC (ASP)

  Supports stateful firewall and Network Address Translation (NAT) services.

- JUNOS scheduler

  Supports transmission scheduling and rate control parameters on interfaces that support the per-unit scheduler. Schedulers define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles to be applied to a particular class of traffic.

- JUNOS shaping

  Supports setting a shaping rate on PICS that support shaping rate and on interfaces that support the per-unit scheduler.

- JUNOS filter

  Supports JUNOS firewall filters.

- JUNOS policer

  Supports policing, or rate limiting, by enabling you to limit the amount of traffic that passes into or out of an interface. It is an essential component of firewall filters that is designed to thwart denial-of-service attacks.

  Policing applies two types of rate limits on the traffic:

  - Bandwidth—Number of bps permitted, on average.
  - Maximum burst size—Maximum size permitted for bursts of data that exceed the bandwidth limit.

Supported Conditions and Actions

The types of conditions and actions that are available for a policy rule depend on the type of rule. Figure 13 shows the types of conditions and actions that are available for JUNOS policy rules. Figure 14 shows the types of conditions and actions that are available for JUNOSe policy rules. The color and user packet class actions are available for JUNOSe policy rules on IPv6 routers. Figure 15 shows the types of conditions and actions that are available for PCMM policy rules.

Figure 13: JUNOS Policy Rules with Supported Conditions and Actions

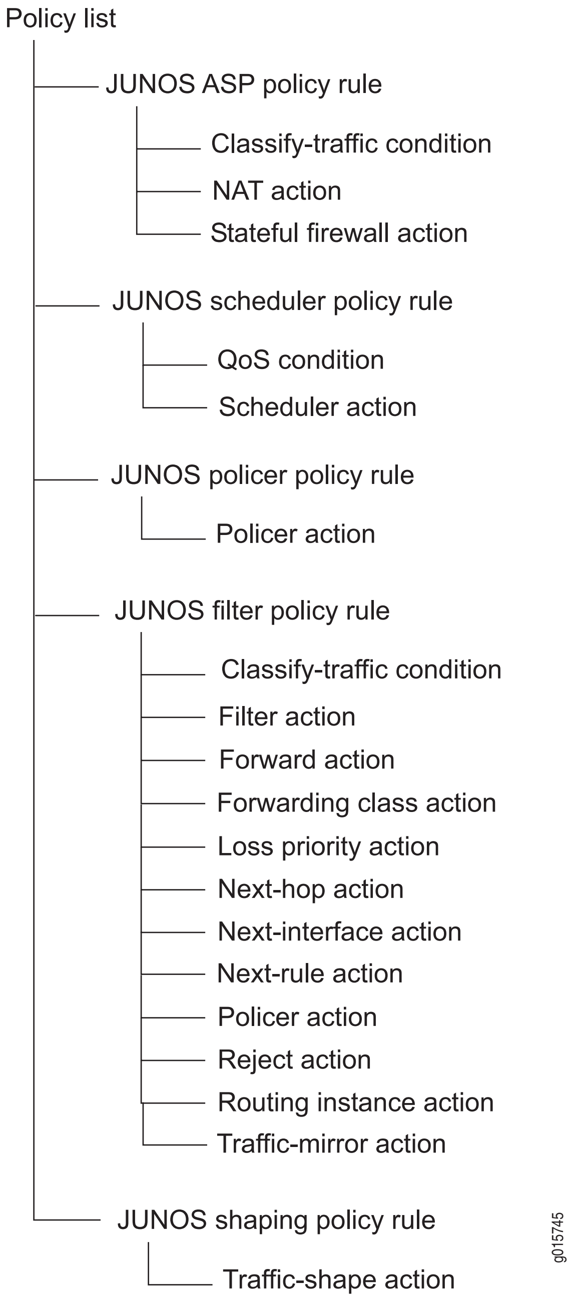


Figure 14: JUNOSe Policy Rules with Supported Conditions and Actions

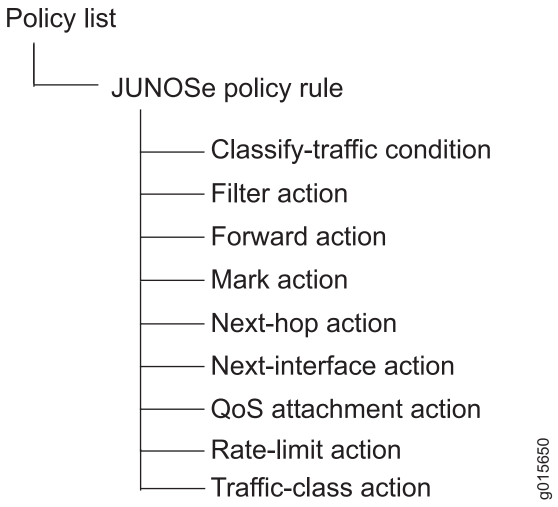
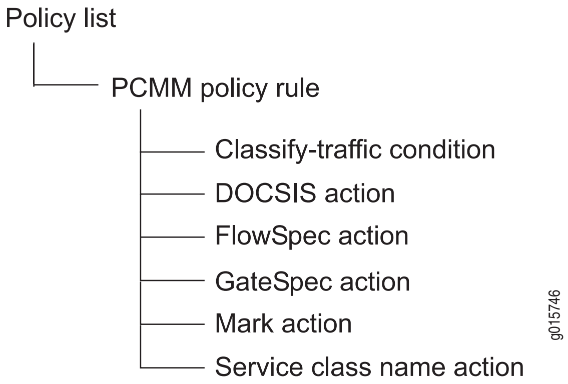


Figure 15: PCMM Policy Rules with Supported Conditions and Actions



Policy Conditions

Policy conditions are values or fields that a packet must contain. If a policy rule does not contain a match condition, all packets are considered to match. There are two types of conditions:

- Classify-traffic condition—Matches can include source and destination addresses or networks; ports, packet types, IP options, TCP flags, network protocol, application protocol
- QoS condition—Matches the forwarding class of the packet

See also *PCMM Classifiers* on page 160.

Multiple Classifiers

JUNOSe and PCMM policy rules can contain multiple classify-traffic conditions. Having multiple classifiers in a policy rule gives you more flexibility for defining services and allows you to use fewer policy rules for some applications.

If multiple policy rules have the same action, but different classify conditions, you can combine the policy rules into one policy rule. You can also set up one policy rule that has multiple classifiers, each for a different subnet or range of addresses.

If you want to collect accounting data on internal versus external traffic, you can configure one policy rule with a set of classifiers for internal traffic and one policy rule with a set of classifiers for external traffic.

Rate-Limiting with Multiple Classifiers

Multiple classifiers give you more flexibility for rate-limiting policies. Without multiple classifiers, you can rate-limit only individual traffic flows. With multiple classifiers, you can rate-limit the aggregate of traffic flows from all sources.

The following example uses multiple classifiers to rate-limit traffic to 1 Mbps for traffic going to two different subnets.

```
Policy List je-in
Policy Rule rate-limiter
ClassifyTrafficCondition CTC1
        SourceNetwork:
          any
        DestinationNetwork:
          ipAddress=172.60.40.0/0.0.0.255
ClassifyTrafficCondition CTC2
        SourceNetwork:
          any
        DestinationNetwork:
          ipAddress=172.60.20.0/0.0.0.255
Rate limit action that limits to 1 Mbps

Policy List je-out
Policy Rule forward
ClassifyTrafficCondition
        DestinationNetwork:
          any
        SourceNetwork:
          any
Forward action
```

Expanded Classifiers

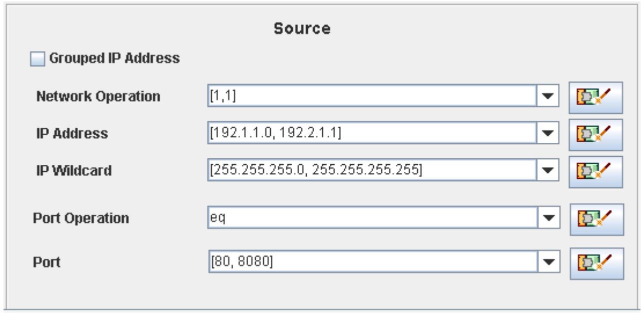
For JUNOSe policies, you can create classify-traffic conditions that the SAE expands into multiple classifiers before it installs the policy on the router. If you enter a comma-separated list of values in the source and destination network (IP address, mask, and IP operation) or port fields (for port-related protocols), the software creates a classifier for each possible combination of address and port. Note that the software does not expand classifiers for values that are entered as a range.

You would use this feature in policies that are used in IP multimedia subsystem (IMS) environments. You can also use it to simplify the configuration of JUNOSe policies.

For example, the source configuration in the classify-traffic condition in Figure 16 would cause the condition to be expanded into four classifiers that have the following combination of source addresses and source ports:

192.1.1.0/255.255.255.0 eq 80
192.1.1.0/255.255.255.0 eq 8080
192.2.1.1/255.255.255.0 eq 80
192.2.1.1/255.255.255.0 eq 8080

Figure 16: Classify-Traffic Condition Example for Expanded Classifiers



Source

☐ Grouped IP Address

Network Operation: [1,1]

IP Address: [192.1.1.0, 192.2.1.1]

IP Wildcard: [255.255.255.0, 255.255.255.255]

Port Operation: eq

Port: [80, 8080]

Policy Actions

JUNOS policy rules and PCMM policy rules can have multiple actions. JUNOSe policy rules can have only one action. The types of actions available for a policy rule depend on the type of rule. See *Supported Conditions and Actions* on page 150. The following table is a description of all actions.

Table 11: Policy Actions

Action	Type of Rule	Description
Color	JUNOSe	Specifies the color attribute that is applied to the packet when it passes through the router that is running IPv6.
DOCSIS	PCMM	Explicitly specifies the Data over Cable Service Interface Specifications (DOCSIS) parameters of the DOCSIS service flow. It supports all DOCSIS service flow scheduling types.
Filter	JUNOS filter JUNOSe	Discards all packets that match the classify-traffic condition.
FlowSpec	PCMM	Specifies a traffic profile by using a Resource Reservation Protocol (RSVP)-style FlowSpec.
Forward	JUNOS filter JUNOSe	Forwards packets that match the classify-traffic condition; forwards packets to a particular interface and/or a next-hop address.
Forwarding class	JUNOS filter	Assigns a forwarding class to packets that match the classify-traffic condition.
GateSpec	PCMM	Specifies the session class ID in the gate. The session class ID provides a way to group gates into different classes with different authorization characteristics.
Loss priority	JUNOS filter	Assigns a packet loss priority to packets that match the classify-traffic condition.

Table 11: Policy Actions (continued)

Action	Type of Rule	Description
Mark	PCMM JUNOSe	Sets the ToS field in the IP header for IPv4 packets, or sets the traffic-class field in the header for IPv6 packets to a specified value.
NAT	JUNOS ASP	Specifies the type of network address translation (source dynamic, destination static), IP address ranges, and a port range to restrict port translation when NAT is configured in dynamic-source mode.
Next hop	JUNOS filter JUNOSe	Specifies the IP address of the next hop; used to create a static route on the router; used for captive portal behavior; JUNOS filters support multiple next hops for load balancing.
Next interface	JUNOS filter JUNOSe	Defines an output interface and/or a next-hop address for a policy list; used to create a static route on the router; used for captive portal behavior.
Next rule	JUNOS filter	Causes the router to skip to and evaluate the next rule in the policy list.
Policer	JUNOS policer JUNOS filter	Specifies rate and burst size limits and the action taken if a packet exceeds those limits.
QoS attachment	JUNOSe	Specifies the QoS profile that is applied to the packet when it passes through the router.
Rate limit	JUNOSe	Specifies bandwidth attributes (committed, peak, and excess rates and burst sizes) and the action taken relative to the bandwidth (filter, forward, or mark).
Reject	JUNOS filter	Discards the packet and sends an ICMP destination unreachable message to the client; can set the type of ICMP message to send.
Routing instance	JUNOS filter	Also called filter-based forwarding; directs traffic to a routing instance that is configured on the router.
Scheduler	JUNOS scheduler	Specifies transmission-scheduling and rate-control parameters. Schedulers define the priority, bandwidth, delay buffer size, rate-control status, and RED drop profiles to be applied to a particular class of traffic.
Service class name	PCMM	Specifies that traffic is controlled by a service class that is configured on the CMTS device.
Stateful firewall	JUNOS ASP	Specifies whether to filter, forward, or reject a packet. If a packet is rejected, a rejection message is returned.
Traffic class	JUNOSe	Specifies the traffic-class profile that is applied to the packet when it passes through the router.
Traffic shape	JUNOS shaping	Specifies the maximum rate of traffic transmitted on an interface.
Traffic mirror	JUNOS filter	Mirrors traffic from a destination to a source or from a source to a destination.
User packet class	JUNOSe	Specifies the user packet class that is applied to the packet when it passes through the router that is running IPv6.

Combining Actions

JUNOS policy rules and PCMM policy rules support multiple actions. For example, in PCMM policies, you can combine a mark action with a DOCSIS parameter action, a service schedule action, or a FlowSpec action. In JUNOS policy rules you can combine the forwarding class action, routing instance action, and loss priority action. The result is that packets that match the condition are assigned to a forwarding class, directed to a routing instance on the router, and assigned a packet loss priority.

Only one of the following actions can exist in a policy rule: next-hop action, next-interface action, forward action, filter action, and reject action.

For example, if you add the next-rule action to a policy rule, do not add a next-hop action, next-interface action, forward action, filter action, or reject action to the same policy rule.

Although you can have only one action in a JUNOSe policy rule, you can set up a policy list to take two corresponding actions on a packet. To do so, you create a JUNOSe policy list that has more than one policy rule with the same precedence. For example, you might 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 action and a policy rule that forwards the packet to the next hop.

Policy LDAP Schema Model

The policy information model is based on the Policy Core Information Model (PCIM) that is mapped to the Policy Framework LDAP core schema by the IETF. SRC software extends this model in such a way to be very close to the policy model used by the router. A policy folder might be the base of the policy subtree (*o = policies, o = umc*) or an organizationalUnit object, underneath the policy base. Such a policy folder contains group objects consisting of one or many policy lists that contain one or many policy rules. A policy rule consists of policy actions and policy conditions.

The objects policy group, policy list, and policy rule are mapped to structural object classes. Each of those classes is derived from the object class policy. This abstract policy object class is inherited from dlm1ManagedElement, which is the top class of the CIM. The policy actions and policy conditions are mapped to auxiliary classes that are attached to the object policyRule. The classes policyActionAuxClass and policyConditionAuxClass are the top classes for any policy action and policy condition. SSP service objects point through the DN pointer to one policy group.

For detailed information about the SRC LDAP schema, see the documentation in the SRC software distribution in the folder */SDK/doc/ldap* or on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/management/sdx

Delivering QoS Services in a Cable Environment

This section describes how SRC policies provide quality of service in the cable network environment.

Service Flow Scheduling Types

The DOCSIS protocol is used to support quality of service for traffic between the cable modem and the CMTS device. To support QoS, the DOCSIS protocol uses the concept of service flows for traffic that is transmitted between cable modems and CMTS devices. A service flow is a unidirectional flow of packets that provides a particular quality of service. Traffic is classified into a service flow, and each service flow has its own set of QoS parameters. Table 12 describes the service flow scheduling types and the QoS parameters that you can set for each type.

The SRC software is compliant with the service flow scheduling types as defined in the PacketCable Multimedia Specification PKT-SP-MM-I03-051221. See the specification for detailed information about each scheduling type.

Table 12: DOCSIS Service Flow Scheduling Types

Type	Description	Suitable Traffic Type(s)	QoS Parameters
Best effort	For upstream service flows. The CMTS scheduler grants transmit opportunities on a first-come first-served basis. You can supplement best effort with QoS parameters.	Standard Internet traffic such as Web browsing, e-mail, or instant messaging	Traffic priority Request transmission policy Maximum sustained traffic rate Maximum traffic burst Minimum reserved traffic rate Assumed minimum reserved-traffic-rate packet size
Non-real-time polling service (NRTPS)	For upstream service flows. The CMTS scheduler sends unicast polls to cable modems on a fixed interval to determine whether data is queued for transmission on a particular service flow. If data is queued, the scheduler provides a transmission grant for the service flow.	Standard Internet traffic that requires high throughput, and traffic that requires variable-sized data grants on a regular basis, such as high-bandwidth FTP.	Traffic priority Request transmission policy Maximum sustained traffic rate Maximum traffic burst Minimum reserved traffic rate Assumed minimum reserved-traffic-rate packet size Nominal polling interval
Real-time polling service (RTPS)	For upstream service flows. Analogous to NRTPS, except that the fixed polling interval is typically very short. Offers request opportunities that meet the service flows' real-time needs and allows the cable modem to specify the size of the desired grant.	Real-time traffic that generates variable-sized data packets on a periodic basis and has inflexible latency and throughput requirements. Applications include Moving Pictures Experts Group (MPEG) video.	Request transmission policy Maximum sustained traffic rate Maximum traffic burst Minimum reserved traffic rate Assumed minimum reserved-traffic-rate packet size Nominal polling interval Tolerated poll jitter

Table 12: DOCSIS Service Flow Scheduling Types (continued)

Type	Description	Suitable Traffic Type(s)	QoS Parameters
Unsolicited grant service (UGS)	For upstream service flows. The CMTS device provides a fixed-size grant to a service flow at fixed intervals without additional polling or interaction. UGS eliminates much of the overhead associated with the polling flow types.	Real-time traffic that generates fixed-size data packets on a periodic basis. Applications include voice over IP (VoIP)	Request transmission policy Unsolicited grant size Grants per interval Nominal grant interval Tolerated grant jitter
Unsolicited grant service with activity detection (UGS-AD)	For upstream service flows. A hybrid of the UGS and RTPS scheduling types. ■ When there is activity, the CMTS device sends unsolicited fixed grants at fixed intervals to the cable modem. ■ When there is no activity, the CMTS device sends unicast poll requests to the cable modem to conserve unused bandwidth.	Applications include voice activity detection, also known as silence suppression	Request transmission policy Nominal polling interval Tolerated poll jitter Unsolicited grant size Grants per interval Nominal grant interval Tolerated grant jitter
Downstream	For downstream service flows. Downstream service flows are defined through a similar set of QoS parameters that are associated with the best-effort scheduling type on upstream service flows.	All downstream traffic	Traffic priority Maximum sustained traffic rate Maximum traffic burst Minimum reserved traffic rate Assumed minimum reserved-traffic-rate packet size Maximum latency

Client Type 1 Support

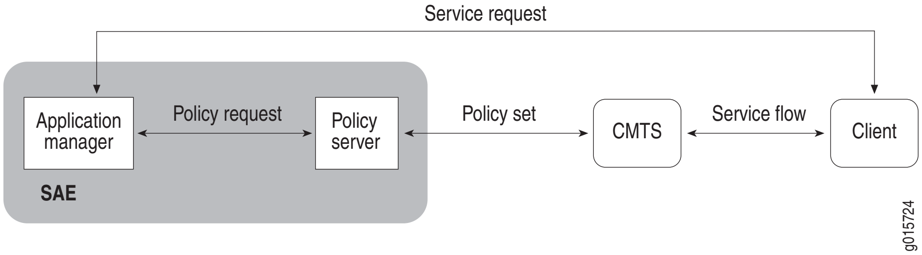
The PCMM specification defines three types of clients, and defines a client as a logical entity that can send or receive data. The SRC software supports client type 1, which represents endpoints such as PC applications or gaming consoles that lack specific QoS awareness or signaling capabilities. Client type 1 entities communicate with an application manager to request service, and the CMTS device manages the QoS signaling.

Client type 1 entities support the proxied QoS with policy push scenario of service delivery defined in the PacketCable Multimedia Architecture Framework Technical Report (PKT-TR-MM-ARCH). In this scenario, the application manager requests QoS resources on behalf of the client, and the policy server pushes the request to the CMTS device. The CMTS device sets up and manages the DOCSIS service flow that the application requires.

Proxied QoS with Policy Push

In the proxied QoS with policy push scenario of service delivery, the client requests a service by sending a service request to the application manager. The application manager determines the QoS needs of the request and sends a policy request to the policy server. The policy server validates the policy request and if, the decision is affirmative, sends a policy set message to the CMTS device. The CMTS device performs admission control on the requested QoS envelope, installs the policy decision, and establishes the service flow to the client with the requested QoS levels.

Figure 17: Authorization Framework for Proxied QoS with Policy Push



PCMM Gate

A PCMM gate is a logical representation of a policy decision that has been installed on the CMTS device. The gate performs traffic classification and enforces QoS policies on media streams.

The set of service flow characteristics that provide enhanced QoS is the envelope. A CMTS gate contains up to three envelopes that indicate authorized, reserved, and committed resources for the service flow that corresponds to the gate. A gate defines a resource authorization envelope that consists of IP-level QoS parameters as well as classifiers that define the scope of service flows that can be established against the gate.

Three elements of a gate discussed here are session class ID, classifiers, and traffic profiles.

Session Class ID

The session class ID provides a way for the application manager and the policy server to group gates into classes with different authorization characteristics. A CMTS device can perform authorization based not only on the requested QoS and the gate's authorized flow specification (FlowSpec), but also on the session class ID specified in the GateSpec. For example, you could use the session class ID to represent a prioritization scheme that allows either the policy server or the CMTS device to preempt a preauthorized gate in favor of allowing a new gate with a higher priority to be authorized.

Use the GateSpec action to specify the session class ID for a gate.

PCMM Classifiers

The classifier identifies the IP flow that will be mapped to the DOCSIS service flow associated with the gate. In Policy Editor, you define the classifier by using a classify-traffic condition.

PCMM Classifiers and Extended Classifiers

Classify-traffic conditions comply with the classifiers specified in PacketCable Multimedia Specification PKT-SP-MM-I02-040930 (referred to as PCMM I02) as well as the extended classifiers in PacketCable Multimedia Specification PKT-SP-MM-I03-051221 (referred to as PCMM I03).

To specify which version of the PCMM classifiers that you are using, see one of the following:

- *Specifying the PCMM Classifier Type* on page 218 in *Chapter 10, Configuring and Managing Policies with the SRC CLI*.
- *Specifying the PCMM Classifier Type* on page 296 in *Chapter 11, Configuring and Managing Policies with Policy Editor*.
- *SRC-PE C-Web Interface Configuration Guide, Chapter 21, Configuring and Managing Policies with the C-Web Interface*, *Specifying the PCMM Classifier Type*.

PCMM I02 classifiers do not support IP masks or a range of port numbers. PCMM I03 classifiers do support IP masks and a range of port numbers.

Using Policy Editor, you define classifiers for PCMM irrespective of whether the policy is meant for I02 or I03. At service activation time, depending on whether the SAE is configured to use I02 or I03 policies, the policy engine does the appropriate translations. For example, if I02 policies are to be used, source and destination IP masks and ranges of port numbers are ignored.

You can configure all fields for extended PCMM classifiers (PCMM I03), except for classifierID, activation state, and action. At service activation, the policy engine sets these fields as follows:

- ClassifierID = A system-generated number
- Activation state = Active
- Action = Add

Guidelines for Configuring Classifiers

When you configure classify-traffic conditions for PCMM policies, keep in mind the following:

- Do not leave the IP address field empty.
- For PCMM classify-traffic conditions, there are two special protocol values:
  - 256 matches traffic that has any IP protocol value
  - 257 matches both TCP and UDP traffic

- PCMM I02 classifiers do not support IP masks or a range of port numbers.
- PCMM I03 classifiers to support IP masks and a range of port numbers.

Traffic Profiles

There are three ways to express the traffic profile for a gate:

- DOCSIS parameters—Specifies the traffic profile through DOCSIS-specific parameters.
- Service class name—Name of a service class that is configured on the CMTS device.
- FlowSpec—Defines the traffic profile through an RSVP-like parameterization scheme.

You can also mark the ToS byte of a packet as it gets to the gate.

DOCSIS Parameters

You use DOCSIS parameters in a network that uses version 1.1 of the DOCSIS protocol. To define DOCSIS parameters for a traffic profile, use the DOCSIS action. This action supports all of the service flow scheduling types and QoS parameters described in Table 12 on page 157. See one of the following:

- *Configuring DOCSIS Actions* on page 247 in *Chapter 10, Configuring and Managing Policies with the SRC CLI*.
- *Configuring DOCSIS Actions* on page 153 in *SRC-PE C-Web Interface Configuration Guide, Chapter 21, Configuring and Managing Policies with the C-Web Interface*
- *Configuring Color Actions* on page 320 in *Chapter 11, Configuring and Managing Policies with Policy Editor*.

Service Class Name

To use a service class name for a traffic profile, use the service class name action. Instead of setting QoS parameters, you specify the name of a service class that is configured on the CMTS device. See one of the following:

- *Configuring Service Class Name Actions* on page 274 in *Chapter 10, Configuring and Managing Policies with the SRC CLI*.
- *Configuring Service Class Name Actions* on page 165 in *SRC-PE C-Web Interface Configuration Guide, Chapter 21, Configuring and Managing Policies with the C-Web Interface*.
- *Configuring Service Class Name Actions* on page 358 in *Chapter 11, Configuring and Managing Policies with Policy Editor*.

FlowSpec Parameters

You can use an RSVP-style FlowSpec to specify a traffic profile. 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.

TSpec parameters defined in the FlowSpec are:

- Bucket rate
- Bucket depth
- Peak rate
- Minimum policed unit
- Maximum packet size

RSpec parameters defined in the FlowSpec are:

- Reserved rate
- Slack term

Types of FlowSpec Services

FlowSpecs support two types of services—controlled load and guaranteed.

- Controlled-load service can be used to provide minimum bandwidth guarantees, and is suitable for applications that are not latency sensitive. Controlled-load service allows applications to have low delay and high throughput even during times of congestion. Controlled-load service can be closely approximated to the best-effort service flow scheduling type. Controlled-load services support TSpec parameters only.

- Guaranteed service allows applications to reserve bandwidth, and is suitable for latency and jitter-sensitive applications such as voice, MPEG video, or gaming. The CMTS device uses the traffic profile parameters specified in the FlowSpec to select one of the two types of DOCSIS scheduling types that can provide guaranteed services—RTPS and UGS. Guaranteed services support both TSpec and RSpec parameters.

Table 13 shows how the FlowSpec service types map to the DOCSIS service scheduling types.

Table 13: Mapping FlowSpec Types

FlowSpec Service Type	DOCSIS Scheduling Type	Application Example
Guaranteed	Unsolicited Grant Service (UGS)	Voice over IP
Guaranteed	Real-Time Polling Service (RTPS)	Guaranteed VPN
Controlled load	Best effort	Standard Internet service

FlowSpec Parameters

Table 14 shows the parameters that you can set for each service type.

Table 14: Parameters Available for Each Type of Service

Controlled Load	Guaranteed Service
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
	Slack term

Marking Packets

You can also mark packets and then install policies on the router that handle the marked packets in a certain way. The mark action causes the ToS byte to be set in the IP header of IPv4 traffic or the traffic-class field to be set in the IP header of IPv6 traffic. For example, to offer videoconferencing, you could:

1. Create a classify-traffic condition that causes the CMTS device to classify the traffic.

2. Create a mark action that causes the CMTS device to mark the ToS byte or traffic-class field in the classified traffic.

3. Create a policy on the router that classifies the traffic according to the marked ToS byte.