

Chapter 2

Configuring Policy Management

This chapter describes how to configure policy-based routing management on an E-series device by using the NMC-RX application.

Topic	Page
Overview	13
References	14
Configuring Classifier Control Lists	14
Configuring Traffic Classes	19
Configuring Rate Limit Profiles	20
Creating a Policy List	23
Adding Rules to a Policy List	24
Removing a Rule	31
Modifying Policy Lists	32
Associating a Policy List with an IP Interface	33
Associating a Policy List with a Profile	34

Overview

Policy management allows you to implement packet forwarding and routing specifically tailored to customers' requirements. You can create and implement policies, and assign those policies to profiles or IP interfaces. In this way, specified tasks will be performed on packets based on the criteria you define in the policy list.

Policy management uses policy routing to predefine packet flow to a destination port without performing a routing table lookup. Packets are sorted according to protocol or precedence into packet flows at ingress or egress by classifier control lists. Policy lists initiate actions specified by rules that can include classifier control lists.

Terminology

See Table 6 for a list of common policy management terms.

Table 6: Policy management terminology

Term	Definition
Policy lists	A policy list is a set of rules; each rule initiates a policy action. A rule is a policy action optionally combined with a classification. You can apply policy lists to packets that arrive at or leave an interface.
Classifier control lists	Classifier control lists specify the criteria according to which a packet flow is defined. The criteria include packet fields such as source IP address, destination IP address, source port address, destination port address, ToS byte, TCP flags, IP flags, and IP fragmentation offset.
Rate limit profiles	Rate limiting is the process of limiting either a classified packet flow or source interface at a configured rate that is less than the physical rate on the port. A rate limit profile is a set of bandwidth attributes and associated actions. The NMC-RX application supports one-rate rate limit profiles and two-rate rate limit profiles.
Traffic classes	A traffic class is a systemwide collection of resources configured to provide a defined level of service to packets assigned to the traffic class. The resources consist of buffers, queues, and bandwidth. The NMC-RX application allows you to create traffic classes and assign them to traffic class rules, which are a part of policy lists.

References

See the *E-series Policy Management and QoS Configuration Guide* for more information.

Configuring Classifier Control Lists

This section describes how you create classifier control lists and classifier control list entries.

The NMC-RX application allows you to configure up to 512 classifier control list entries per classifier control list. Each classifier control list entry is automatically numbered when created.

Creating a Classifier Control List

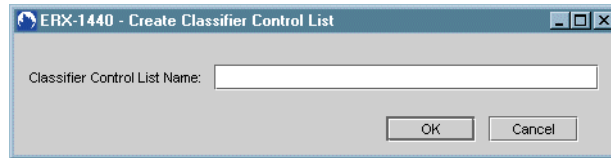
You can create and list classifier control lists from the Device-wide Explorer. Double-click Classifier Control List in the Device-wide Explorer to list all classifier control lists defined on the current device.

You can also create and list classifier control lists from the System folder in the Instance Explorer and the Device-wide Explorer.

To create a classifier control list:

1. From the Device-wide Explorer, select Classifier Control Lists.
2. Right click, select Create, and click Classifier Control List.

The Create Classifier Control List dialog box appears.



3. Type the Classifier Control List Name with 1 to 40 characters.
4. Click OK.

A Creation complete message appears.

5. Click OK.

Creating a Classifier Control List Entry

Once you have created a classifier control list, you can configure a classifier control list entry.

From the Classifier Control List Entry dialog box, you can specify a protocol or set the IP flag or TCP flag by clicking the appropriate button. Clicking this button displays additional related dialog boxes. Many parameters are available only when a particular protocol is selected. See Table 7 for complete descriptions.

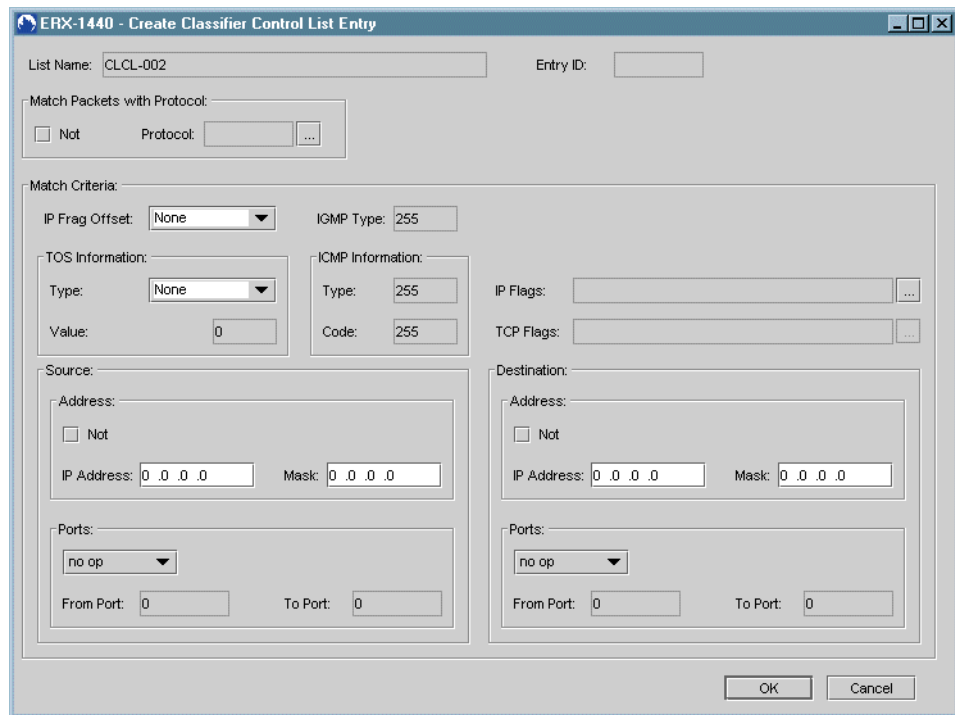
To create a classifier control list entry:

1. From the Device-wide Explorer, in the Policy Management folder, double-click Classifier Control Lists.

All classifier control lists defined on the current device appear in the list area of the Device Workshop.

2. Select a classifier control list from the list.
3. Right-click, select Create, and click Classifier Control List Entry.

The Create Classifier Control List Entry dialog box appears.



4. Set the parameters. See Table 7.

Table 7: Classifier control list entry parameters




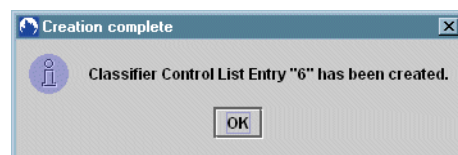
Parameter	Description
List Name	Identifier of the classifier control list of which this entry is a part; not editable
Entry ID	Identifier of this entry; value populated from device; not editable
Match Packets with Protocol	
Not	Indicates that packets matched are not equal to the protocol specified
Protocol	Protocol matched (or not) by this classifier list entry; not editable; range 0–255 Click  to select a protocol from the Select Protocol dialog box. See <i>Related Dialog Boxes</i> .
Match Criteria	
IP Frag Offset	IP fragmentation offset; options: Equal to 0, Equal to 1, Greater than 1, or None
IGMP Type	IGMP message type value; editable only when IGMP is the specified protocol; range 1–255
IP Flags	IP header flags for classification Click  to select an IP header flag from the Configure IP Flag dialog box. See <i>Related Dialog Boxes</i> .

Table 7: Classifier control list entry parameters (continued)

Parameter	Description
TCP Flags	TCP header flags for classification. Active only when TCP is selected. Click  to select a TCP flag from the ConfigureTCP Flag dialog box. See <i>Related Dialog Boxes</i> .
ToS Information	
Type	Specifies how the ToS information is set; options: ToS Value, Precedence, DS Field, or None
Value	Value set based on type selected. ToS Value – range 0–255; default 255 Precedence – range 0–7; default 7 DS Field – range 0–63; default 63
ICMP Information	
Type	ICMP message type value; editable only when ICMP is the specified protocol; range 0–255
Code	ICMP message code value; editable only when ICMP is the specified protocol; range 0– 255
Source/Destination Address	
Not	When checked, indicates that the packets matched have a source or destination address not equal to the specified address
IP Address	Source or destination IP address matched (or not) by this classifier list entry; 0.0.0.0 is the wildcard; must be a valid IP address; default 0.0.0.0
Mask	Mask to apply to the source or destination address; default 0.0.0.0
Source/Destination Ports	
Options	Operation used to match ports to the specified From Port and To Port fields (if appropriate); editable only when TCP or UDP is the specified protocol Options: no op, less than, greater than, equal to, not equal to, range; default: no op
From Port	Source or destination port number used in port comparisons; invalid only for no op; range 1–65535
To Port	End source or destination port number used in port range comparisons; valid only for range; range 1–65535

- Click OK.

The Creation complete message appears. Note that the classifier control list entry is automatically numbered.

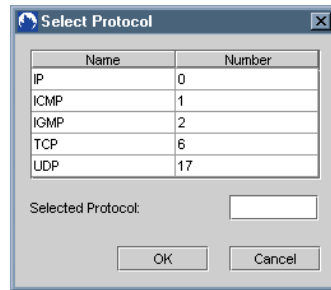


- Click OK.

Related Dialog Boxes

This section presents the procedures for setting the classifier control list parameters in the Create Classifier Control List Entry dialog box.

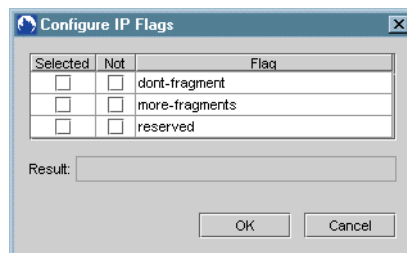
Select Protocol The Select Protocol dialog box appears when you click  next to the Protocol field.



1. Either click a protocol in the list, or manually specify a different protocol by typing the protocol number in the Select Protocol box. The range is 0–255.
2. Click OK.

The protocol you selected appears in the Protocol field in the Create Classifier Control List Entry dialog box.

Configure IP Flags The Configure IP Flags dialog box appears when you click  next to the IP Flags field. Use it to select an IP flag.




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

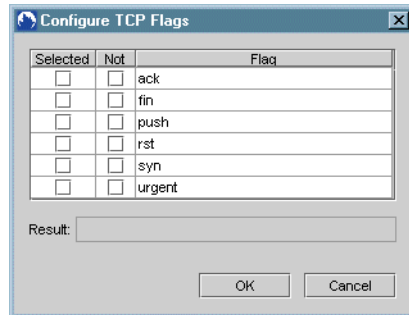


NOTE: The check box in the Not column cannot be checked unless the check box in the corresponding Selected column is checked first.

3. Click OK.

The IP flags you selected appear to the right of the IP Flags field in the Classifier Control List Entry dialog box.

Configure TCP Flags The Configure TCP Flags dialog box appears when you click  next to the TCP Flags field. Use it to select a TCP flag.



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



NOTE: The check box in the Not column cannot be checked unless the check box in the corresponding Selected column is checked first.

3. Click OK.

The TCP flag you selected appears to the right of the TCP Flags field in the Classifier Control List Entry dialog box.

Configuring Traffic Classes

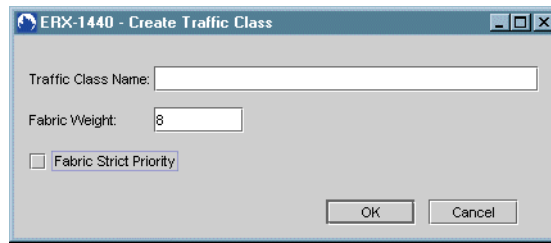
You can create and list traffic classes from the Device-wide Explorer. Traffic classes can also be created and listed from the System folder in the Instance Explorer and Device-wide Explorer.

The NMC-RX application allows you to create a maximum of eight traffic classes on an E-series router.

To configure a traffic class:

1. From the Device-wide Explorer, under Policy Management, click Traffic Classes.
2. Right-click, select Create, and click Traffic Class.

The Create Traffic Class dialog box appears.



3. Set the parameters. See Table 8.

Table 8: Create traffic class parameters

Parameters	Description
Traffic Class Name	Identification of traffic class; can be set only when created; range 1–31
Fabric Weight	Relative weight for fabric queue in this traffic class; range 1–63; default 8
Fabric Strict Priority	When checked, allows packets in this class to be dequeued out of the fabric ahead of other traffic classes

4. Click OK.

A pop-up message appears.

5. Click OK.

Configuring Rate Limit Profiles

You can configure a one-rate or two-rate rate limit profile type on an E-series device. Both profile types have common and type-specific parameters.

You can double-click the rate limit profile entry to list all rate limit profiles defined on the current device. You can also create and list rate limit profiles from the System folder in the Instance Explorer and Device-wide Explorer.

Configuring a One-Rate Rate Limit Profile

To configure a one-rate rate limit profile:

1. From the Device-wide Explorer, under Policy Management, click Rate Limit Profiles.
2. Right-click, select Create, and click Rate Limit Profile (one rate).

The Create Rate Limit Profile (one rate) dialog box appears.

3. Set the parameters. See Table 9.

Table 9: Rate limit profile (one-rate) parameters

Parameter	Description
Name	Identification of the rate limit profile; name can be set only when created; range 1–40 characters
Committed Rate (bps)	Committed access rate value; range 0–4294967295; default 0
Committed Burst (bytes)	Committed access rate burst size; range 8192–4294967295; default 8192
Excess Burst (bytes)	Excess burst size; range 0–4294967295; default 0; if the value is not 0, then it must be greater than the committed burst value
Committed Action	Action to be assigned in packets within the committed access rate Options: transmit, drop, or mark; default: transmit
Committed Mark Value	Mark value to be assigned to packets; editable when committed action is <i>mark</i> ; range 0–255; default: blank
Conformed Action	Action to be applied to packets that exceed the committed access rate; options: transmit, drop, or mark; default: transmit
Conformed Mark Value	Mark value to be assigned to packets; editable when conformed action is <i>mark</i> ; range 0–255; default is blank
Exceeded Action	Action to be applied to packets that exceed the peak access rate; options: transmit, drop, or mark; default: drop
Exceeded Mark Value	Mark value to be assigned to packets; field is editable when exceeded action is <i>mark</i> ; range 0–255; default: blank
Mark Mask	Mask to be applied with mark values; range 1–255; default 255

4. Click OK.

A pop-up message appears.

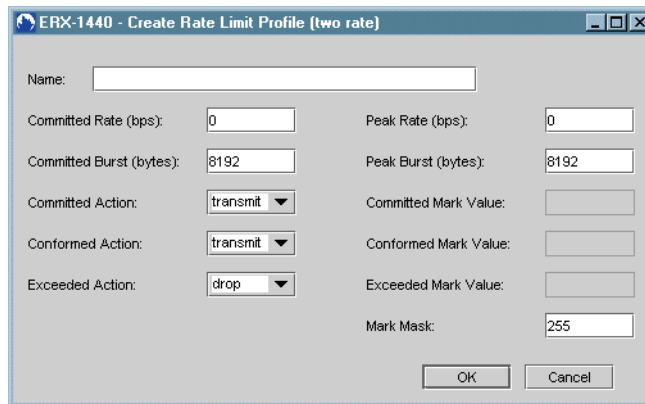
5. Click OK.

Configuring a Two-Rate Rate Limit Profile

To configure a two-rate rate limit profile:

1. From the Device-wide Explorer, under Policy Management, click Rate Limit Profiles.
2. Right-click, select Create, and click Rate Limit Profile (two rate).

The Create Rate Limit Profile (two rate) dialog box appears.



3. Set the parameters. See Table 10.

Table 10: Rate limit profile (two rate) parameters

Parameter	Description
Name	Identification of the rate limit profile; name can be set only when created; range 1–40 characters.
Committed Rate (bps)	Committed access rate value; range 0–4294967295; default 0
Committed Burst (bytes)	Committed access rate burst size; range 8192–4294967295; default 8192
Peak Rate (bps)	Peak access rate; range 0–4294967295; default 0; if the value is not 0, then it must be greater than the committed rate value
Peak Burst (bytes)	Peak burst size; range 8192–4294967295; default 8192
Committed Action	Action to be assigned in packets within the committed access rate Options: transmit, drop, or mark; default: transmit
Committed Mark Value	Mark value to be assigned to packets; editable when committed action is <i>mark</i> ; range 0–255; default: blank
Conformed Action	Action to be applied to packets that exceed the committed access rate; options: transmit, drop, or mark; default: transmit
Conformed Mark Value	Mark value to be assigned to packets; editable when conformed action is <i>mark</i> ; range 0–255; default: blank
Exceeded Action	Action to be applied to packets that exceed the peak access rate; options: transmit, drop, or mark; default: drop
Exceeded Mark Value	Mark value to be assigned to packets; field is editable when exceeded action is <i>mark</i> ; range 0–255; default: blank

Table 10: Rate limit profile (two rate) parameters (continued)

Parameter	Description
Mark Mask	Mask to be applied with mark values; range 1–255; default: 255

4. Click OK.

A pop-up message appears.

5. Click OK.

Creating a Policy List

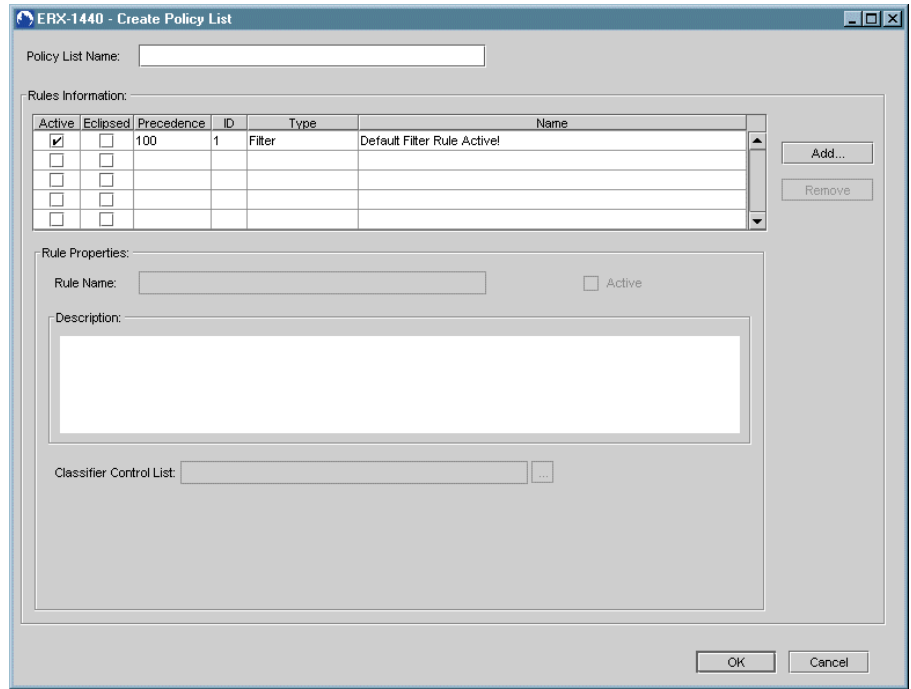
Policy lists allow you to create, modify, and delete policy rules. Policy list names can be set only during creation. You can modify parameters after rules are added.

If a policy list is created without rules, the Default Filter Rule is automatically created on the policy list. Once you add a second rule, the Default Filter Rule is removed from the table. If you remove the last rule in the policy list, an entry is added for the Default Filter Rule. You cannot edit the fields in the Default Filter Rule, nor can you remove the Default Filter Rule from the policy list.

To create a policy list:


1. From the Device-wide Explorer, under Policy Management, click Policy Lists.
2. Right-click, select Create, and click Policy List.

The Create Policy List dialog box appears.



3. Name the policy list. See Table 11.

Table 11: Policy list parameters

Parameters	Description
Policy List Name	Identification of the policy list; 1–40 characters; name can be set only when a policy list is first created
Rule Name	Name of the policy rule
Active	When checked, indicates that the rule is active
Classifier Control List	Classifier control list associated with the selected rule; 1–40 characters Click  to display the dialog box. See <i>Creating a Classifier Control List</i> on page 14.

4. To create a policy list without rules, click OK.
5. To add one or more rules, follow the steps in the next section, *Adding Rules to a Policy List*.

Adding Rules to a Policy List

A policy list can comprise nine different types of rules: color, filter, forward, log, mark, next hop, next interface, rate limit profile, and traffic class. Once you select a rule type, specific attributes for that rule type appear.

Policy List Limits

Consider the following limitations when creating policy lists. The NMC-RX application allows you to configure:

- One classifier control list per rule
- A maximum of 512 classifier control list entries per policy list
- An unlimited number of rules per policy list
- Any combination of rule types per policy list

Creating a Rule

Each rule has six common rule parameters. One of the common parameters is an association with a classifier control list, which specifies the criteria used to determine whether a rule is applied.

Most rules contain one or more type-specific parameters, some of which are associations with other objects, such as an IP interface, rate limit profile, or traffic class.



NOTE: You can create a rule from either the Create Policy List dialog box or from the Policy List configuration area.

To add a rule:

1. From the Create Policy List dialog box, click the Add button.

The Add Policy Rule dialog box appears.

2. In the Rule Type drop-down list, select one of the nine rule types.

Depending on the rule type you select, parameters appear below the Classifier Control List entry.

Table 12: Rule types

Type	Description
Color	Specifies which color to explicitly assign to a packet
Filter	Drops all packets conforming to the classifier control list that you specify
Forward	Forwards all packets conforming to a specified classifier control list
Log	Logs all packets conforming to the specified classifier control list
Mark	Sets the ToS byte in the IP header to a specified value
Next Hop Rule	Defines the IP address of the next hop for a policy list
Next Interface	Defines an output interface for a policy list
Rate Limit Profile	Specifies a rate limit profile in a policy list
Traffic Class	Specifies a traffic class in a policy list. When applied to a packet, the packet is placed into the specified traffic class when passing through the router.

3. Set the common parameters. See Table 13.

Table 13: Policy rule common parameters for the nine rule types

Parameters	Description
Rule Name	Logical identification of rule; 1–32 characters
Precedence	Priority of rule; can be set only at time rule is created; range 1–32768; default 100
Rule ID	Identifier given to the rule by the device; not editable
Active	When checked, indicates that the rule is active; when not checked, indicates that the rule is not active
Eclipsed	When checked, indicates that the rule will be eclipsed by another rule; not editable
Description	Logical description of rule; 1–255 characters
Classifier Control List	Classifier control list associated with the selected rule; 1–40 characters. See step 5 on page 30.

4. Set the rule-specific parameter(s).

Information for each rule type is presented in the following sections. When you finish setting the parameters for the rule types, go to step 5 below.



NOTE: There are no additional rule-specific parameters for Filter, Forward, and Log rules.

Color Rule From the Color drop-down list, select a color. See Table 14.

Table 14: Type-specific parameters for Color rule

Parameter	Description
Color	Red – exceeded peak access rate Yellow – exceeded the committed access rate Green – within the committed access rate


Mark Rule Set the mark parameters. See Table 15.

Table 15: Type-specific parameters for Mark rule

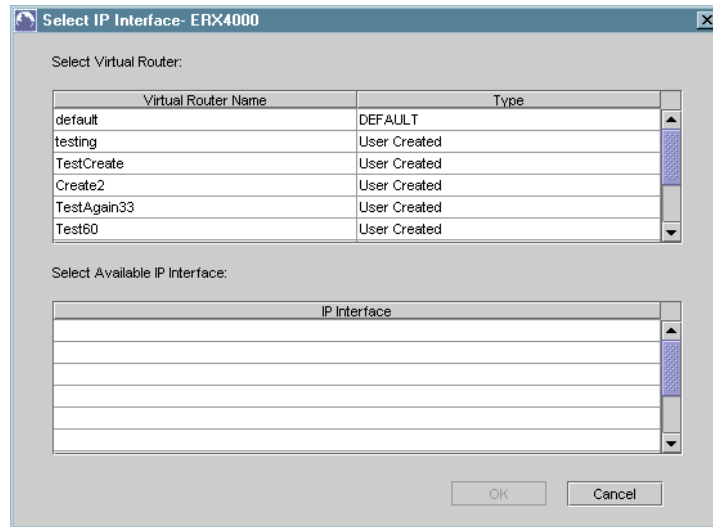
Parameters	Description
Type	Specifies how the ToS information is set. Options: ToS Value, Precedence, DS Field, and Byte Value/Mask. See Value below.
Value	Based on the type selected. The mask range field is editable only for the Byte Value/Mask type. Value set based on type selected. ToS Value – range 0–255; default 255; mask 255 Precedence – range 0–7; default 7; mask 224 DS Field – range/length 0–63; default 63; mask 252 Byte Value/Mask – range 0-255; default 255; mask range 1– 255; mask default 255
Mask	Mask to be applied to value. See Value above. Editable only for Byte Value/Mask type.

Next Hop Rule Enter a valid IP address for the next hop.

Next Interface Rule Follow these steps:

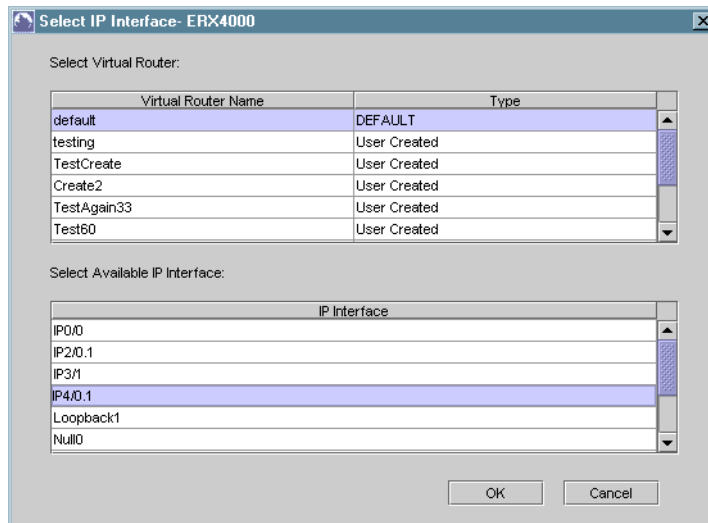
- a. Click  to the right of the IP Interface text box.

The Select IP Interface dialog box appears.



- b. Click a virtual router name from the Select Virtual Router list.

All IP interfaces on the selected virtual router appear in the IP Interface area.



- c. Click an IP interface from the Select Available IP Interface list.
- d. Click OK.


The IP description name appears in the text box to the right of IP Interface label.

- e. In the Add Policy Rule dialog box, set the Next Hop parameter by entering a valid IP address for the next hop.

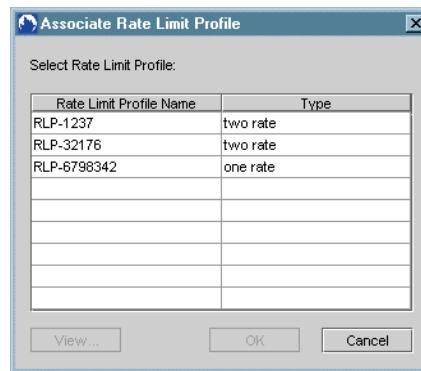


NOTE: The next hop is optional for nonshared interfaces.

Rate Limit Profile Rule Follow these steps:

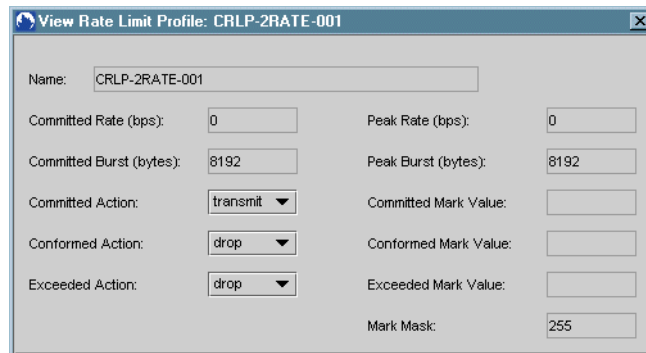
- a. Click  to the right of the Rate Limit Profile text box.

The Associate Rate Limit Profile dialog box appears.




- b. Click a rate limit profile name in the list.
- c. (Optional) View the rate limit profile attributes by clicking the View... button.

The View Rate Limit Profile dialog box appears.




These attributes cannot be edited.

Close the dialog box by clicking .

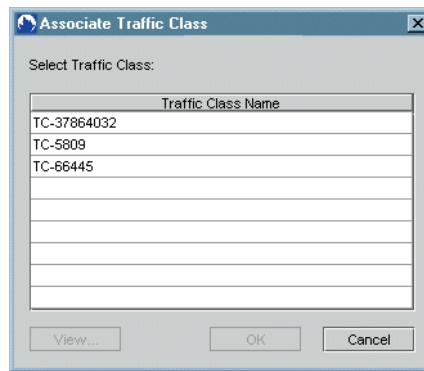
- d. Click OK.

The rate limit profile name appears in the text box to the right of the Rate Limit Profile label.

Traffic Class Rule Follow these steps:

- a. Click  to the right of the Traffic Class text box.

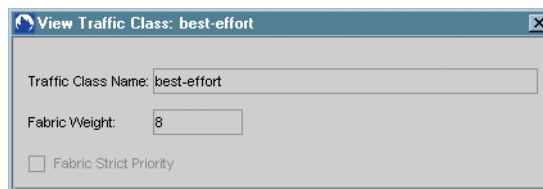
The Associate Traffic Class dialog box appears.




NOTE: A maximum of eight traffic classes are allowed on an E-series router.

- b. Click a traffic class name in the list.
- c. (Optional) View the traffic class attributes by clicking the View... button.

The View Traffic Class dialog box appears.

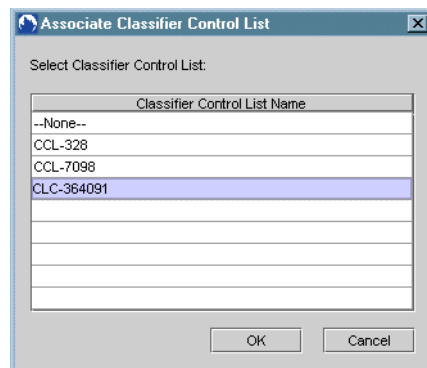


These attributes cannot be edited.

Close the dialog box by clicking .

5. In the Add Policy Rule dialog box, click  to the right of the Classifier Control List box.

The Associate Classifier Control List dialog box appears.



6. Click a classifier control list name.
7. Click OK.

The classifier control list name appears in the text box to the right of Classifier Control List in the Add Policy Rule dialog box.

8. Click OK in the Add Policy Rule dialog box.

The newly created rule name(s) appear(s) in the Rules Information area of the Create Policy List dialog box.

Removing a Rule

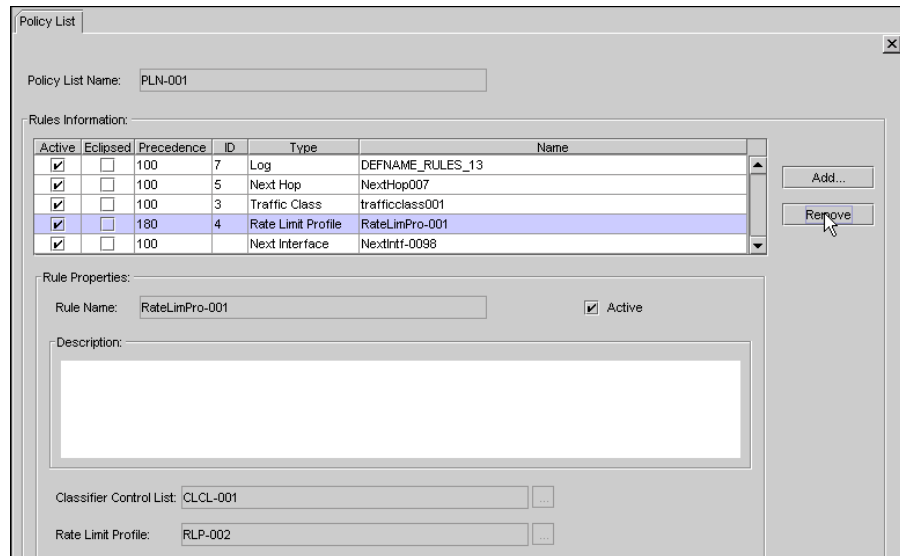
You can remove a rule from the list of available rules. You can remove a rule from either the Create Policy List dialog box or from the Policy List configuration tab.

To remove a rule from the Policy List configuration tab:

1. On the Policy List tab, click the rule type you want to delete.

The common and type-specific parameters appear on the Policy List tab.

2. Click the Remove button.



The rule is permanently deleted from the Rules Information list.

Modifying Policy Lists

You can modify any existing policy list by first listing all policy lists and then selecting Configure. You can modify only the Active parameter for existing rules. You can modify all parameters for new rules you add to the policy list.

To modify the Active parameter for existing rules in a policy list:

1. From the Rules Information area, click the rule you want to edit.
Only the Active check box becomes active.
2. Select or deselect the Active check box.
3. Click Save.

To modify parameters for new rules you are adding to a policy list:

1. From the Rules Information area, click the rule you want to edit.
All parameters for the rule you selected become active.
2. Modify the parameters.
3. Click Save.



NOTE: Once you save a policy list, you cannot edit existing rules contained in the policy list, with the exception of the Active parameter.

Associating a Policy List with an IP Interface

For a policy list to become active, it must be associated with either an IP interface or a profile. You can associate up to three policy lists with an IP interface at a time by specifying Input, Output, or Local Input. You can make this association when you configure an IP interface.

To associate a policy list with an IP interface:

1. From the Device-wide Explorer, under the IP folder, double-click IP Interfaces.

All IP interfaces configured on this device are listed in the list area.

2. Select an IP interface from the list, right-click, and click Configure.


The IP Intf Configuration tab appears in the work area.

The screenshot shows the 'IP Intf Configuration' dialog box with the following fields and sections:

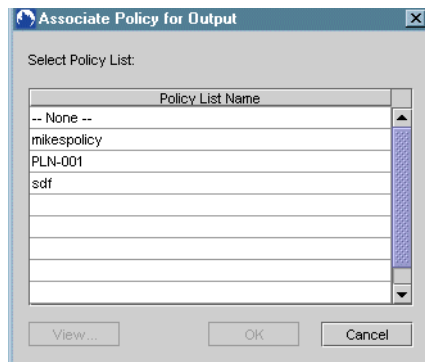
- Location:**
 - Physical: Module: SRP-1 port, Slot: 0, Port: 0
 - Logical: (empty)
- Name:** IP0/0
- Alias:** (empty)
- Intf Index:** 3
- Status:**
 - Operational: Up
 - Administrative: Up
- Category:** pointToPoint
- Virtual Router:** default
- Interface Number:** (empty)
- Policy Information:**

Type	Policy Name	Statistics Enabled
Input	-- None --	<input type="checkbox"/>
Output	-- None --	<input type="checkbox"/>
Local Input	-- None --	<input type="checkbox"/>
- IP Addresses:**

Slot	IP Address	Intf Index
0	10.6.129.203	3

3. In the Policy Information group box, in the row where you want to specify the policy list, click  to the right of the Policy Name column.

For example, if you select Output, the Associate Policy for Output dialog box appears.



4. Click a policy list name.
5. (Optional) View the policy list attributes by clicking the View button.
6. Click OK.

The policy name appears in the text box to the right of the Type (Input, Output, or Local Input) on the IP Intf Configuration tab.

7. (Optional) Repeat steps 4–7 for the two remaining types.
8. (Optional) Enable statistics by selecting the Statistics Enabled box to the right of each policy name.



NOTE: To view policy list statistics, see Viewing Policy List Statistics on IP Interfaces in *Chapter 6, Configuring IP*.

9. Click Save.

The policy list(s) are associated with the IP interface you selected.

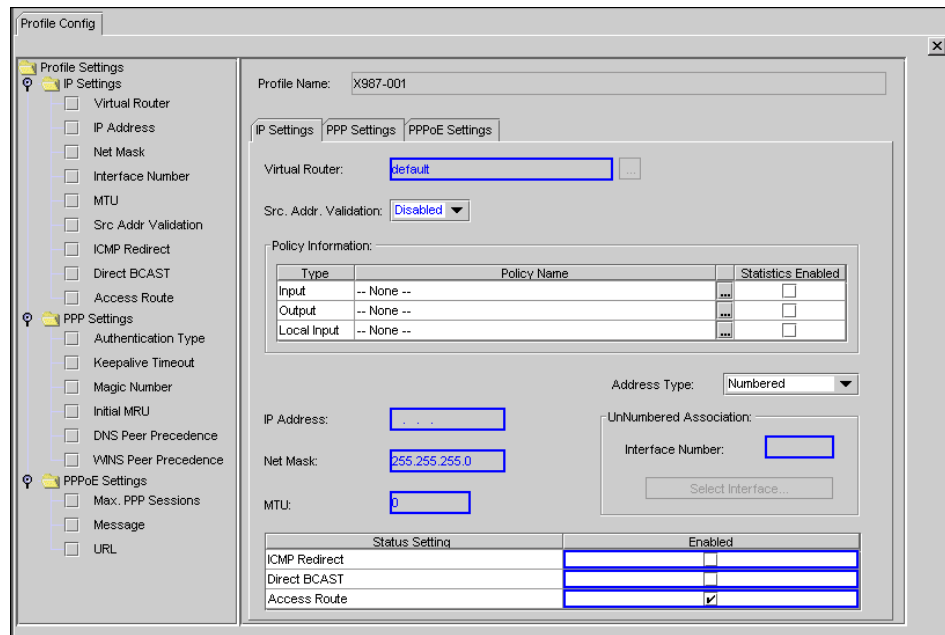
Associating a Policy List with a Profile


Profiles can have different policy lists associated with each device. Unlike policy lists, which are device-wide objects, profiles are network-wide objects. For this reason, you must associate a policy list with a profile from the Device Workshop. Each profile can have three policy lists associated with it for each device.

To associate a policy list with a profile:

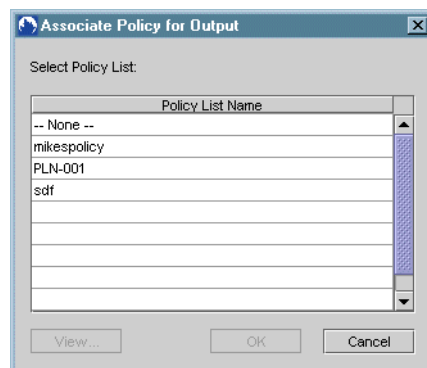
1. From the Device-wide Explorer, double-click Profiles.
All available profiles are listed in the list area.
2. Click a profile name from the list, right-click, and click Configure.

The Profile Config tab appears in the work area.



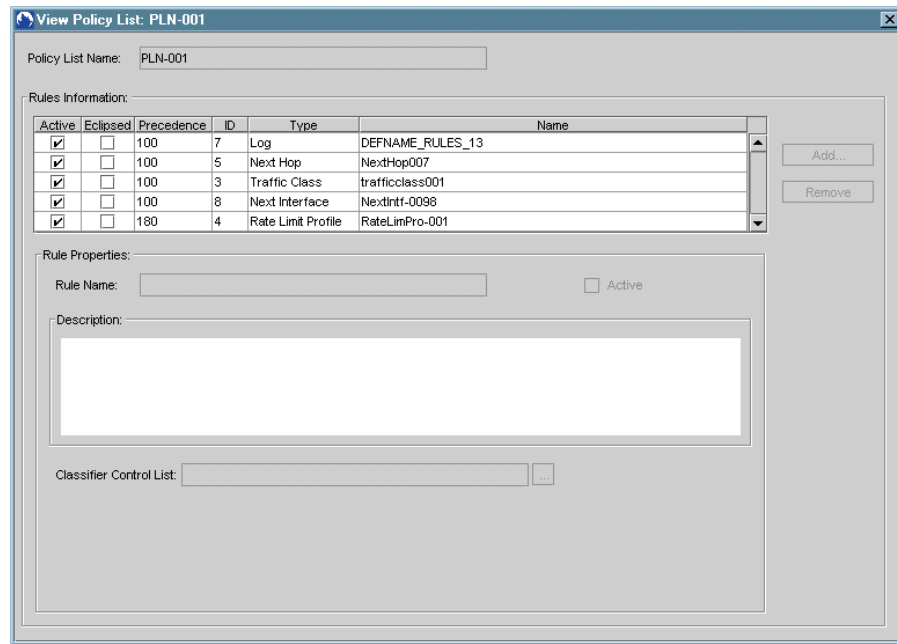
- In the Policy Information group box, in the row where you want to specify the policy list, click  to the right of the Policy Name column.


For example, if you select Output, the Associate Policy for Output dialog box appears.



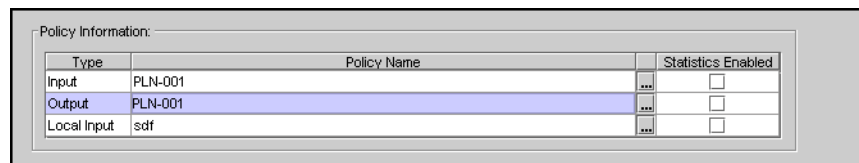
- Select a policy list name in the list.
- (Optional) View the policy list attributes by clicking the View button.

The View Policy List dialog box appears.



- a. Click any rule in the Rules Information list to view the attributes associated with that rule. Attributes cannot be edited from this dialog box.
 - b. Close the dialog box by clicking .
6. Click OK.
 7. (Optional) Repeat steps 3–6 for the two remaining types.
 8. (Optional) Enable statistics by selecting the Statistics Enabled box to the right of each policy name.

The policy name appears in the text box to the right of the type (input, output, or local input) on the Policy Configuration tab.



9. Click Save.

The policy list(s) are associated with the profile you selected.