Chapter 4

Creating Classifier Groups and Policy Rules

This chapter provides information for configuring policy-based routing management on E-series routers. The chapter discusses the following topics:

Classifier Groups and Policy Rules Overview

Classifier groups contain the policy rules that make up a policy list. A policy rule is an association between a policy action and an optional CLACL. The CLACL defines the packet flow on which the policy action is taken.

A policy list might contain multiple classifier groups—you can specify the precedence in which classifier groups are evaluated. Classifier groups are evaluated starting with the lowest precedence value. Classifier groups with equal precedence are evaluated in the order of creation.

NOTE: For IP policies, the **forward** command supports the **order** keyword, which enables you to order multiple forward rules within a single classifier group. (See *Using Policy Rules to Provide Routing Solutions* on page 35.)

From Policy Configuration mode, you can assign a precedence value to a CLACL by using the **precedence** keyword when you create a classifier group. The default precedence value is 100. For example:

```
host1(config-policy-list)#classifier-group ipCLACL25 precedence 21
host1(config-policy-list-classifier-group)#
```

The **classifier-group** command puts you in Classifier Group Configuration mode. In this mode you configure the policy rules that make up the policy list. For example:

```
host1(config-policy-list-classifier-group)#forward next-hop 172.18.20.54
```

To stop and start a policy rule without losing statistics, you can suspend the rule. Suspending a rule maintains the policy rule with its current statistics, but the rule no longer affects packets in the forwarding path.

From Classifier Group Configuration mode, you can suspend a rule by using the **suspend** version of that policy rule command. The **no suspend** version reactivates a suspended rule. For example:

```
host1(config-policy-list-classifier-group)#suspend forward next-hop 172.18.20.54
host1(config-policy-list-classifier-group)#no suspend forward next-hop 172.18.20.54
```

You can add, remove, or suspend policy rules while the policy is attached to one or more interfaces. The modified policy takes effect once you exit Policy Configuration mode.

Policy Rule Precedence

Because of the flexibility in creating policy lists and classifier groups, you can configure a classifier group that has multiple policy rules.

If a classifier group has multiple rules, the router uses the rules according to their precedence—not in the order in which you created the rules. The first rule listed (the forward rule) for a policy list type has the highest precedence and the last rule has the lowest. The precedence is based on the order in which the router performs rules. Rules are performed in order from lower to higher precedence. In the event of a conflict, a higher precedence rule overrides the lower precedent rule.

The precedence of rules is important if you want a specific rule to be applied. For example, if an IP policy list has both a rate-limit-profile rule (which specifies a color) and a color rule in the same classifier-group, the color specified by the color rule is always used rather than the color implied in the rate-limit-profile rule (the color rule has a higher precedence).

Table 5 lists the policy rule commands that you can use for each type of policy list. The table lists the rules in their order of precedence.

NOTE: The ES2 10G Uplink LM and the ES2 10G LM support only IP, MPLS, and VLAN interfaces.

Table 5: Policy Rule Commands and Precedence

ATM	Frame Relay	GRE	IP	IPv6	L2TP	MPLS	VLAN
forward	forward	forward	forward	forward	forward	forward	forward
color	color	color	forward interface (input, secondary input, and output policies only)	color	color	color	color
–	–	–	exception for input and secondary input policies only (not supported on ES2 10G Uplink LM or ES2 10G LM)	–	–	–	–
mark-clp (See **mark-clp command** for platform support information.)	mark-de	mark	forward next-hop for input policies only	rate-limit-profile	rate-limit-profile	rate-limit-profile	mark-user-priority
filter	filter	filter	color	user-packet-class	filter	mark-exp	filter
user-packet-class	user-packet-class	user-packet-class	rate-limit-profile	traffic-class	user-packet-class	filter	user-packet-class
traffic-class	traffic-class	traffic-class	user-packet-class	mark	traffic-class	user-packet-class	traffic-class
–	–	–	traffic-class	filter	–	traffic-class	–
–	–	–	mark	–	–	–	–
–	–	–	filter	–	–	–	–
–	–	–	log (not supported on ES2 10G Uplink LM or ES2 10G LM)	–	–	–	–

NOTE: The commands listed in this section replace the Policy List Configuration mode versions of the commands. For example, the **color** command replaces the Policy List Configuration mode version of the **color** command. The original command may be removed completely in a future release.

Related Topics

- Classifier Groups and Policy Rules Overview on page 32
- *Chapter 9, Monitoring Policy Management*
- **color** command
- **color-mark-profile** command
- **filter** command
- **green-mark** command
- **log** command
- **mark** command
- **mark-clp** command
- **mark-de** command
- **mark-exp** command
- **mark-user-priority** command
- **next-hop** command
- **next-interface** command
- **rate-limit-profile** command
- **red-mark** command
- **reference-rate** command
- **traffic-class** command
- **user-packet-class** command
- **yellow-mark** command

Using Policy Rules to Provide Routing Solutions

The next-interface, next-hop, filter, and forward rules provide routing solutions for traffic matching a classifier. A classifier can have only one action that provides a routing solution.

If you configure two routing solution rules, such as filter and forward, in the same classifier group, the router displays a warning message, and the rule configured last replaces the previous rule.

For IP policy lists, policy rules are available to enable you to make a forwarding decision that includes the next interface and next hop:

- Forward next interface—Causes an interface to forward all packets that satisfy the classification associated with that rule to the next interface specified
- Forward next hop—Causes an interface to forward all packets that satisfy the classification associated with that rule to the next-hop address specified

For example, you can route packets arriving at IP interface ATM 0/0.0 so that they area handled as indicated:

- Packets from source 1.1.1.1 are forwarded out of interface ATM 0/0.1.
- Packets from source 2.2.2.2 are forwarded out of interface ATM 2/1.1.
- All other packets are dropped.

To configure this routing policy, issue the following commands:

```
host1(config)#ip classifier-list clacIA ip host 1.1.1.1 any
host1(config)#ip classifier-list clacIB ip host 2.2.2.2 any
host1(config)#ip policy-list IpPolicy100
host1(config-policy-list)#classifier-group clacIA
host1(config-policy-list-classifier-group)#forward interface atm 0/0.1
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group clacIB
host1(config-policy-list-classifier-group)#forward interface atm 2/1.1
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group *
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#exit

host1(config)#interface atm 0/0.0
host1(config-subif)#ip policy input IpPolicy100 statistics enabled
```

Configuring Policies to Provide Network Security

You can configure policy management to provide a level of network security by using policy rules that selectively forward or filter packet flows:

- Forward—Causes the packet flows that satisfy the classification associated with the rule to be routed by the virtual router
- Filter—Causes the interface to drop all packets of the packet flow that satisfy the classification associated with the rule

To stop a denial-of-service attack, you can use a policy with a filter rule. You need to construct the classifier list associated with the filter rule so that it isolates the attacker's traffic into a flow. To determine the criteria for this classifier list, you need to analyze the traffic received on an interface. *Chapter 9, Monitoring Policy Management*, describes how to capture packets into a log.

For example, you can route packets entering an IP interface (ATM 0/0.0) so that they are handled as indicated:

- Packets from source 1.1.1.1 are routed.
- TCP packets from source 2.2.2.2 with the IP fragmentation offset set to one are dropped.
- All other TCP packets are routed.
- All other packets are dropped.

To configure this policy, issue the following commands:

```
host1(config)#ip classifier-list clacIA ip host 1.1.1.1 any
host1(config)#ip classifier-list clacIB tcp host 2.2.2.2 any ip-frag-offset eq 1
host1(config)#ip classifier-list clacIC tcp any any
host1(config)#ip policy-list IpPolicy100
host1(config-policy-list)#classifier-group clacIA
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group clacIB
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group clacIC
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group *
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#exit

host1(config)#interface atm 0/0.0
host1(config-subif)#ip policy input IpPolicy100 statistics enabled
```

Creating an Exception Rule within a Policy Classifier Group

To create the exception rule within an IP policy classifier group to specify the client application for the destination of packets rather than forwarding them by the forwarding controller (FC), use the **exception http-redirect** command.Doing this allows the application to then perform an application-dependent action on the content of the packet. The exception rule applies to input and secondary-input policies.

NOTE: The exception http-redirect command is not supported for the ES2 10G LM or the ES2 10G Uplink LM.

An exception rule in the input policy only takes effect if neither the input policy nor the secondary policy drops the packet. Packets dropped by input or secondary policies are not exceptioned to the SRP module. HTTP redirect is the only application that is available as a destination of the **exception** rule.

Because classifier groups can contain multiple actions, the following list describes how each rule interacts with the exception rule:

- **color**—Packets are colored and the exception rule is applied.
- **filter**—Packets are filtered and the exception rule is *not* applied. When the filter rule is present, other rules are not applied.
- **forward**—Forward rule is ignored and the exception rule is applied to packets.
- **log**—Packets are logged and the exception rule is applied.
- **mark**—Packets are marked and the exception rule is applied.
- **next-hop**—Next-hop rule is ignored and the exception rule is applied to packets.
- **next-interface**—Next-interface rule is ignored and the exception rule is applied to packets.
- **rate-limit-profile**—Rate limit is applied and the exception rule is applied to packets.
- **traffic-class**—Traffic class is set and the exception rule is applied to packets.
- **user-packet-class**—User packet class is set and the exception rule is applied to packets.
- **exception**—Exception rule is applied to packets.

Related Topics

- **exception http-redirect** command

Defining Policy Rules for Forwarding

The **forward next-hop** command defines a rule that creates the forwarding solution for packets matching the current CLACL.The **forward** command can be used while the policy list is referenced by interfaces. The **suspend** version suspends the forward rule within the classifier group.

For IP policy lists only:

- You can use the **forward interface** command to specify multiple interfaces and the **forward next-hop** command to specify next-hop addresses as possible forwarding solutions. If you define multiple forwarding solutions for a single CLACL, use the **order** keyword to specify the order in which the router chooses the solutions. The router uses the first reachable solution in the list, starting with the solution with the lowest order value. The default order value is 100.

NOTE: The forward interface and **forward next-hop** commands replace the **nest-interface** and **next-hop** commands.

The switch route processor (SRP) module Fast Ethernet port cannot be the destination of the **forward next-hop** and **forward next-interface** commands.

- If you specify a next-hop address as the forwarding solution, you can specify that the default route is not used as a routing solution for the next-hop address when selecting a reachable forward rule entry.
- IP interfaces referenced with this command can be tracked if they move. Policies attached to an interface also move if the interface moves. However, statistics are not maintained across the move.
- You can no longer use an interface specifier of **tunnel:mpls** with the **forward interface** command, because that usage requires IP interfaces on top of RSVP-TE tunnels. Such interfaces are no longer present in the redesigned MPLS architecture. However, you can configure a static route for an address that is not otherwise used to point to a tunnel, and then use the **forward next-hop** command in the policy:

  host1(config)#**ip route 10.10.10.10/32 tunnel mpls:foo**
  host1(config)#**ip policy-list bar**
  host1(config-policy-list-classifier-group)#**forward next-hop 10.10.10.10**

Related Topics

- **forward** command
- **forward interface** command
- **forward next-hop** command

Assigning Values to the ATM CLP Bit

The **mark-clp** command assigns a value of 0 or 1 to the ATM CLP bit for packets conforming to the current classifier control list.

Modules on E-series routers support classifying and marking of the ATM CLP bit according to the following rules:

- Modules on E120 and E320 routers support classifying of the ATM CLP bit only for frame-based interfaces (ATM Adaptation Layer 5 [AAL5] encapsulation), but not for individual ATM cells (ATM Adaptation Layer 0 [AAL0] encapsulation). In this case, if the CLP bit in any cell in the frame has a value of 1, the router treats the reassembled AAL5 frame as if it also had a CLP value of 1.
- Modules on E120 and E320 routers support marking of the ATM CLP bit on frame-based interfaces. In this case, every cell of the segmented frame leaves the router with the same CLP value.
- Modules on ERX-7xx models, ERX-14xx models, and the ERX-310 router support classifying and marking of the ATM CLP bit for individual ATM cells (AAL0 encapsulation), but not for frame-based interfaces (AAL5 encapsulation).

Related Topics

- **mark-clp** command

Enabling ATM Cell Mode

When you configure a rate limit profile to account for ATM cell tax, the forwarding code calculates this information to determine the size of a frame instead of using only the frame size.

- Issue the **atm-cell-mode** command to account for the ATM cell tax in statistics and rate calculations:

  ```
  host1(config-policy-list)#atm-cell-mode
  ```

Use the **show rate-limit-profile** command to display the state of the mode.

Related Topics

- *Chapter 9, Monitoring Policy Management*
- **atm-cell-mode** command
- **show rate-limit-profile** command

Enabling IP Options Filtering

You can filter packets with IP options on an interface:

- Issue the **ip filter-options** all command.

  host1(config-if)#**ip filter-options all**

When a packet arrives on an interface, the router checks to see if the packet contains IP options. If it does and if IP options filtering is enabled, that packet is dropped. IP options filtering is disabled by default.

Related Topics

- Classifier Groups and Policy Rules Overview on page 32
- **ip filter-options all**

Packet Tagging Overview

You can use the traffic-class rule in policies to tag a packet flow so that the QoS application can provide traffic-class queuing. Policies can perform both in-band and out-of-band packet tagging:

- Policies perform in-band tagging by using their respective mark rule to modify a packet header field. For example, IP policies use the **mark** rule to modify an IP packet heard ToS field, and Frame Relay policies use the **mark-de** rule to modify the DE bit.

- Policies perform out-of-band tagging by using the traffic class or color rule. Explicit packet coloring lets you configure prioritized packet flows without having to configure a rate-limit profile. The router uses the color to queue packets for egress queue threshold dropping as described in *Chapter 5, Creating Rate-Limit Profiles*.

For example, an Internet service provider (ISP) provides a Broadband Remote Access Server (B-RAS) service that has both video and data components, and the ISP wants to guarantee that the video traffic gets priority treatment relative to the data traffic. The ISP's users have a 1.5 Mbps virtual circuit (VC) terminating on a digital subscriber line access multiplexer (DSLAM). The ISP wants to allocate 800 Kbps of this link for video, if there is a video stream.

The ISP creates a classifier list to define a video packet flow, creates a policy to color the packets, and applies the policy to the interface:

host1(config)#**ip classifier-list video ip any any dsfield 16**
host1(config)#**ip classifier-list data ip any any dsfield 32**
host1(config)#**ip policy-list colorVideoGreen**
host1(config-policy-list)#**classifier-group video**
host1(config-policy-list-classifier-group)#**color green**
host1(config-policy-list-classifier-group)#**exit**
host1(config-policy-list)#**classifier-group data**
host1(config-policy-list-classifier-group)#**color yellow**

```
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit

host1(config)#interface atm 12/1.1
host1(config-if)#ip policy input colorVideoGreen statistics enabled
```

Creating Multiple Forwarding Solutions with IP Policy Lists

By default, the router uses a single route table lookup to determine the forwarding solution for packets. For IP policy lists only, the **forward** command enables you to configure one or more unique forwarding solutions (interfaces or next-hop addresses) that override the route table lookup. By creating a group of forwarding solutions, you can ensure that there is a reachable solution for the packets.

You can use the **order** keyword to specify the order of the group of forwarding solutions within a single forward rule. If no order value is specified, then the default order of 100 is assigned to a solution. The router evaluates the forwarding solutions in the group, starting at the solution with the lowest order value, and then uses the first reachable solution. To be considered a reachable solution, a solution must be a reachable interface or a next-hop address that has a route in the routing table. If no solutions are reachable, the traffic is dropped.

The following guidelines apply when you create a group of forwarding solutions in an IP policy list:

- You can specify a maximum of 20 forwarding solutions for a classifier.
- The interface and next-hop elements of a forwarding solution must exist within a single virtual router:
  - Next-interface elements are associated with the virtual router where that interface exists.
  - You can include an optional parameter to specify the virtual router when you define next-hop elements.
  - If only next-hop elements exist and you do not use the virtual router option, then the policy assumes the virtual router context of the command-line interface (CLI), making the policy specific to that VR. The policy can be attached only to interfaces that belong to that VR. However, the policy can still be displayed and modified from any VR. The output of the **show configuration** command displays the policy in the section of output related to that VR rather than in the section for the default VR. This behavior ensures that when you use that output for a configuration script, the policy is specific to the correct VR, and the original configuration is re-created.
- If you specify both an interface element and a next-hop address element, then they both must be reachable to be used. Also, the interface must be the correct interface for the next-hop address.
- If you specify a next-hop address, then you can optionally specify that the default route be ignored.

- If you delete the target (interface or next-hop address) referenced in a rule, that solution is replaced by the null interface but retains the same order number in the policy list. The null interface is always considered unreachable.
- When a forwarding solution with a lower order value than the currently active solution becomes reachable, the router switches to the lower-ordered solution.
- If two rules that have the same order value are reachable, then the rule that was created first is used.

NOTE: The **forward interface** and **forward next-hop** commands are replacing the **next-interface** and **next-hop** commands, which do not support multiple forwarding solutions in a single forward rule.

In the following sample classifier group of a policy list, the forwarding solution of ATM interface 0/0.1 has the lowest order value in the group, and would therefore be selected as the solution for the policy list. However, if this interface is not reachable, the router then attempts to use the solution with the next higher order; which would be ATM interface 12/0.1. If none of the solutions in the group is reachable, the traffic is dropped.

host1(config-policy-list)#**classifier-group westfordClacl precedence 200**
host1(config-policy-list-classifier-group)#**forward interface atm 0/0.1 order 10**
host1(config-policy-list-classifier-group)#**forward interface atm 12/0.1 order 50**
host1(config-policy-list-classifier-group)#**forward interface atm 3/0.25 order 300**

NOTE: You can use the **suspend** version of the command to suspend an individual entry in a group of forwarding solutions. The forward rule remains active as long as there is a reachable or active entry in the group of forwarding solutions. If you suspend all entries in the group, the status of the forward rule is changed to suspended.

Creating a Classifier Group for a Policy List

To create a classifier group for a policy list and assigns precedence to the specific CLACL that is referenced in the group:

1. Create a classifier group.

   host1(config-policy-list)#**classifier-group C1 parent-group IPG1**

2. Assign a precedence to the CLACL.

   host1(config-policy-list)#**classifier-group westfordClacl precedence 150**

3. Create a hierarchical policy parameter list.

   host1(config)#**policy-parameter A hierarchical**
   host1(config)#**parent-group EPG1**
   host1(config-parent-group)#**exit**
   host1(config)#**ip policy-list POL**

```
host1(config-policy-list)#classifier-group C1 external parent-group EPG1
parameter A
host1(config-policy-list)#exit
```

The **no** version removes the classifier group and its rules from a policy list. The **precedence** keyword specifies the order in which a classifier group is evaluated compared to other classifier groups. Classifier groups are evaluated from lowest to highest precedence value (for example, a classifier group with a precedence of 1 is used before a classifier group with a precedence of 2). Classifier groups with equal precedence are evaluated in the order of creation, with the group created first having precedence. A default value of 100 is used if no precedence is specified.

The **parent-group** keyword creates a parent group in a rate-limit hierarchy for IP, IPv6, L2TP, and MPLS. The **external parent-group** keyword creates an external parent group in a rate-limit hierarchy for IP, IPv6, L2TP, and MPLS. All packets matching the classifier are sent to the parent group for further processing, except for packets dropped by the classifier using the filter rule.

More than one classifier group can have the same parent group, which enables you to create hierarchies.

NOTE: Empty classifier groups have no effect on the router's classification of packets and are ignored by the router. You might inadvertently create empty classifier groups in a policy if you use both the newer CLI style and the older CLI style, which used the Policy List Configuration mode version of the classifier list commands.

Related Topics

- Classifier Groups and Policy Rules Overview on page 32
- *Chapter 5, Creating Rate-Limit Profiles* for examples of using this command to rate limit traffic flows
- *Chapter 9, Monitoring Policy Management*
- **aggregation-node** command
- **classifier-group** command
- **ip policy-parameter hierarchical** command
- **ip policy-parameter reference-rate** command
- **ipv6 policy-parameter hierarchical** command
- **ipv6 policy-parameter reference-rate** command
- **l2tp policy-parameter hierarchical** command
- **l2tp policy-parameter reference-rate** command
- **mpls policy-parameter hierarchical** command

- **mpls policy-parameter reference-rate** command
- **next-parent** command
- **parent-group** command
- **policy-parameter hierarchical** command