Configuring Route Policies with CLI

This section provides information to configure route policies using the command line interface.

Topics in this section include:

Route Policy Configuration Overview

Route policies allow you to configure routing according to specifically defined policies. You can create policies and entries to allow or deny paths based on various parameters such as destination address, protocol, packet size, and community list.

Policies can be as simple or complex as required. A simple policy can block routes for a specific location or IP address. More complex policies can be configured using numerous policy statement entries containing matching conditions to specify whether to accept or reject the route, control how a series of policies are evaluated, and manipulate the characteristics associated with a route.

When to Create Routing Policies

Route policies are created in the **config>router** context. There are no default route policies. Each route policy must be explicitly created and applied. Applying route policies can introduce more efficiency as well as more complexity to routers' .

A route policy impacts the flow of routing information or packets within and through the router. A routing policy can be specified to prevent a particular customer's routes to be placed in the route table which causes those routes to not forward traffic to various destinations and the routes are not advertised by the routing protocol to neighbors.

Route policies can be created to control:

- A protocol to export all the active routes learned by that protocol.
- Route characteristics to control which route is selected to act as the active route to reach a destination and advertise the route to neighbors.
- Protocol to import all routes into the routing table. A routing table must learn about particular routes to be able to forward packets and redistribute to other routing protocols.
- Damping.

Before a route policy is applied, analyze the policy's purpose and be aware of the results (and consequences) when packets match the specified criteria and the associated actions and default actions, if specified, are executed. Membership reports can be filtered based on a specific source address.

Default Route Policy Actions

Each routing protocol has default behaviors for the import and export of routing information. Table 24 shows the default behavior for each routing protocol.

Table 24: Default Route Policy Actions

Protocol	Import	Export
OSPF	Not applicable. All OSPF routes are accepted from OSPF neighbors and cannot be controlled via route policies.	• Internal routes: All OSPF routes are automatically advertised to all neighbors. • External routes: By default all non-OSPF learned routes are not advertised to OSPF neighbors
IS-IS	Not applicable. All IS-IS routes are accepted from IS-IS neighbors and can not be controlled via route policies	• Internal routes: All IS-IS routes are automatically advertised to all neighbors. • External routes: By default all non-IS-IS learned routes are not advertised to IS-IS peers.
RIP	By default, all RIP-learned routes are accepted.	• External routes: By default all non-RIP learned routes are not advertised to RIP peers.
BGP	By default, all routes from BGP peers are accepted and passed to the BGP route selection process.	• Internal routes: By default all active BGP routes are advertised to BGP peers • External routes: By default all non-BGP learned routes are not advertised to BGP peers.

Policy Evaluation

Routing policy statements can consist of as few as one or several entries. The entries specify the matching criteria. A route is compared to the first entry in the policy statement. If it matches, the specified entry action is taken, either accepted or rejected. If the action is to accept or reject the route, that action is taken and the evaluation of the route ends.

If the route does not match the first entry, the route is compared to the next entry (if more than one is configured) in the policy statement. If there is a match with the second entry, the specified action is taken. If the action is to accept or reject the route, that action is taken and the evaluation of the route ends, and so on.

Each route policy statement can have a default-action clause defined. If a default-action is defined for one or more of the configured route policies, then the default actions should be handled in the following ways:

- The process stops when the first complete match is found and executes the action defined in the entry.
- If the packet does not match any of the entries, the system executes the default action specified in the policy statement.

Figure 38 depicts an example of the route policy process.

Route policies can also match a given route policy entry and continue to search for other entries within either the same route policy or the next route policy by specifying the *next-entry* or *next-policy* option in the entry's **action** command. Policies can be constructed to support multiple states to the evaluation and setting of various route attributes.

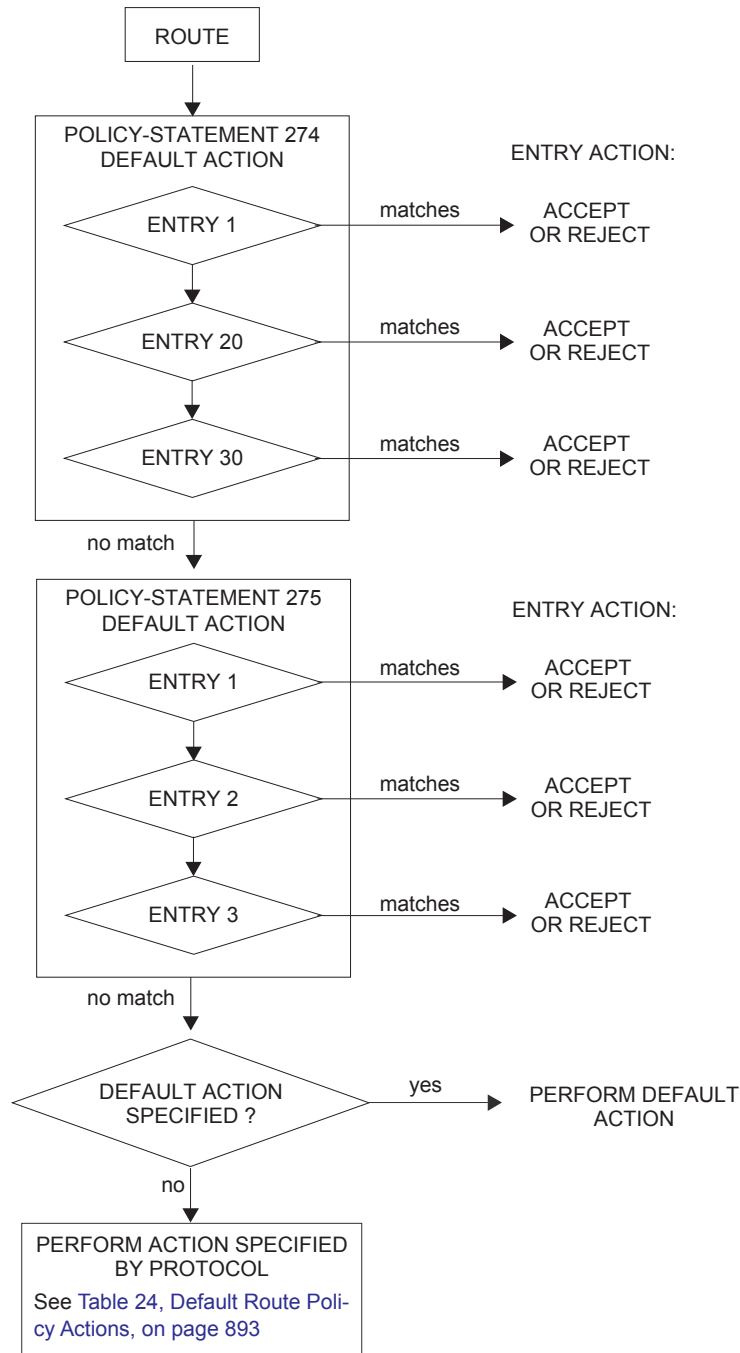Figure 39 depicts the next-policy and next-entry route processes.

```
                        ┌─────────────┐
                        │    ROUTE    │
                        └──────┬──────┘
                               │
                               ▼
        ┌────────────────────────────────────┐
        │ POLICY-STATEMENT 274                │        ENTRY ACTION:
        │ DEFAULT ACTION                      │
        │          ◇ ENTRY 1 ◇  ── matches ──▶│        ACCEPT
        │               │                     │        OR REJECT
        │               ▼                     │
        │          ◇ ENTRY 20 ◇ ── matches ──▶│        ACCEPT
        │               │                     │        OR REJECT
        │               ▼                     │
        │          ◇ ENTRY 30 ◇ ── matches ──▶│        ACCEPT
        │                                     │        OR REJECT
        └──────────────┬─────────────────────┘
              no match  │
                        ▼
        ┌────────────────────────────────────┐
        │ POLICY-STATEMENT 275                │        ENTRY ACTION:
        │ DEFAULT ACTION                      │
        │          ◇ ENTRY 1 ◇  ── matches ──▶│        ACCEPT
        │               │                     │        OR REJECT
        │               ▼                     │
        │          ◇ ENTRY 2 ◇  ── matches ──▶│        ACCEPT
        │               │                     │        OR REJECT
        │               ▼                     │
        │          ◇ ENTRY 3 ◇  ── matches ──▶│        ACCEPT
        │                                     │        OR REJECT
        └──────────────┬─────────────────────┘
              no match  │
                        ▼
             ◇ DEFAULT ACTION ◇  ── yes ──▶   PERFORM DEFAULT
             ◇ SPECIFIED ?   ◇               ACTION
                        │
                    no  │
                        ▼
        ┌────────────────────────────────────┐
        │ PERFORM ACTION SPECIFIED            │
        │ BY PROTOCOL                         │
        │ See Table 24, Default Route Poli-   │
        │ cy Actions, on page 893             │
        └────────────────────────────────────┘
```
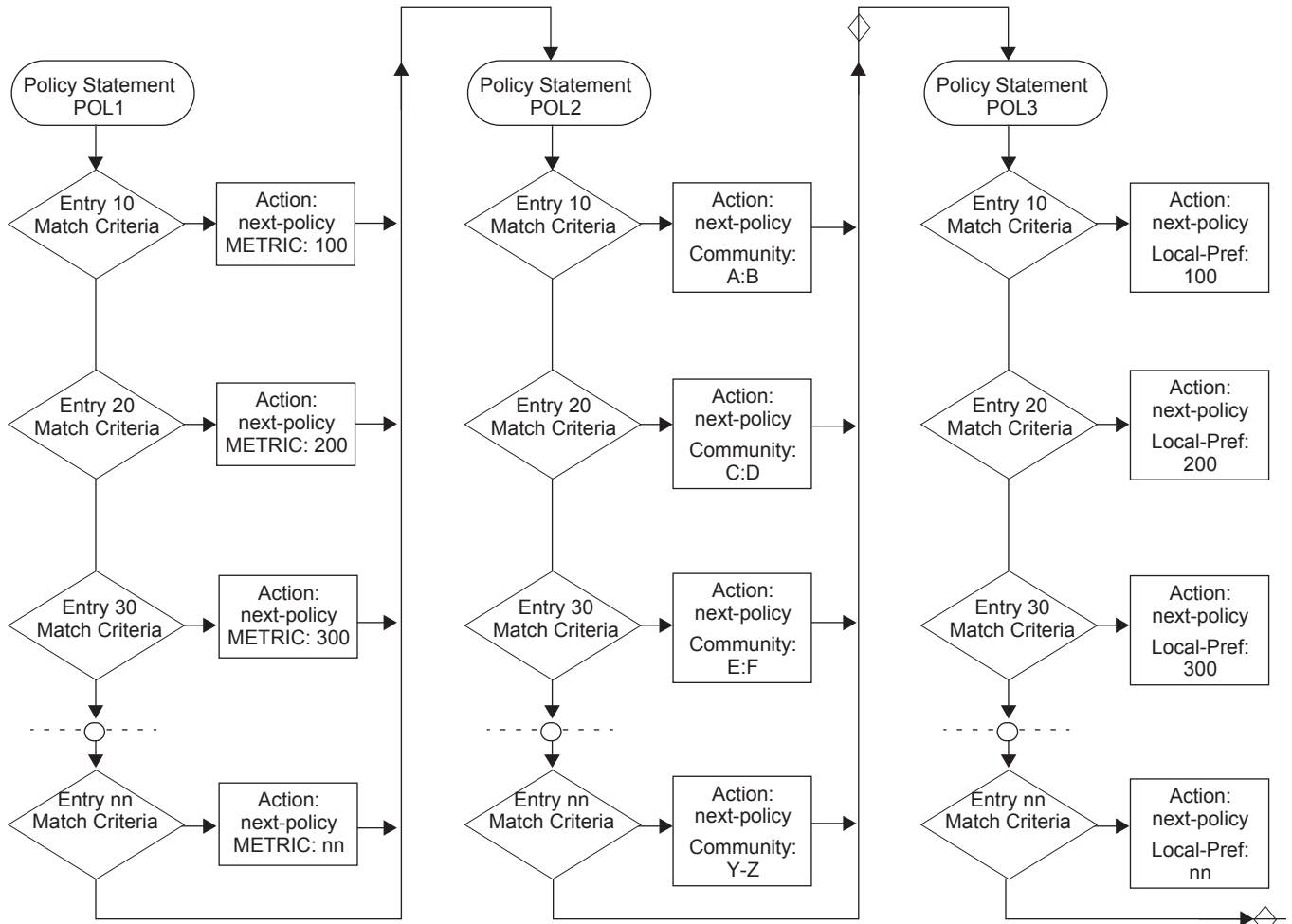
Figure 38: Route Policy Process Example

Figure 39: Next Policy Logic Example

Damping

Damping initiates controls when routes flap. Route flapping can occur when an advertised route between nodes alternates (flaps) back and forth between two paths due to network problems which cause intermittent route failures. It is necessary to reduce the amount of routing state change updates propagated in order to limit processing requirements. Thus, when a route flaps beyond a configured value (the suppress value), then that route is removed from the routing tables and routing protocols until the value falls below the reuse value.

A route can be suppressed according to the Figure of Merit (FoM) value. The FoM is a value that is added to a route each time it flaps. A new route begins with an FoM value of 0.

Damping is optional. If damping is configured, the following parameter values must be explicitly specified as there are no default values:

- suppress
- half-life
- reuse
- max-suppress

When a route's FoM value exceeds the suppress value, then the route is removed from the routing table. The route is considered to be stable when the FoM drops below the `reuse` value by means of the specified half life parameter. The route is returned to the routing tables. When routes have higher FoM and half life values, they are suppressed for longer periods of time. Figure 40 depicts an example of a flapping route, the suppress threshold, the half life decay (time), and reuse threshold. The peaks represent route flaps, the slopes represent half life decay.
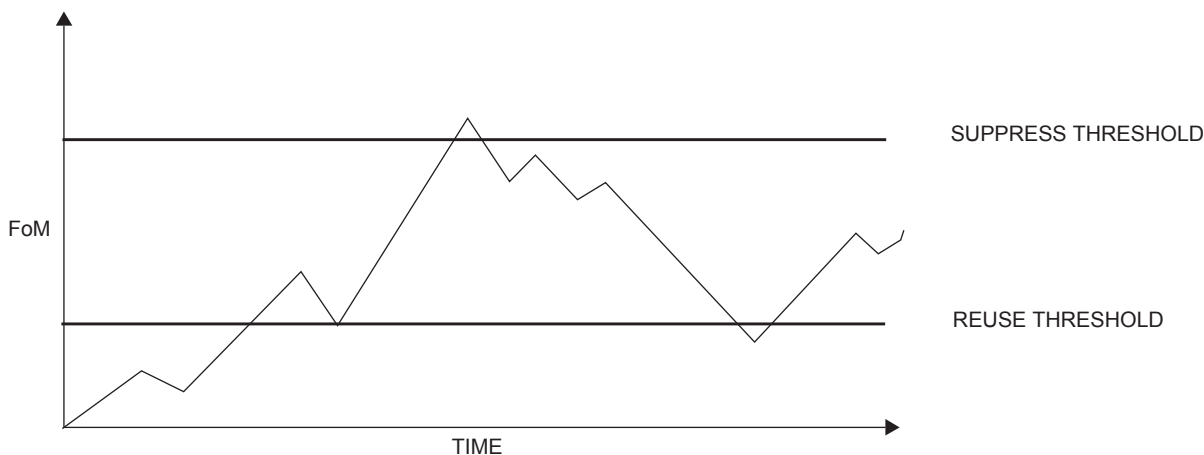

Figure 40: Damping Example

Basic Configurations

This section provides information to configure route policies and configuration examples of common tasks. The minimal route policy parameters that need to be configured are:

- Policy statement with the following parameters specified:
    - → At least one entry
    - → Entry action

Following is a sample route policy configuration:

```
A:ALA-B>config>router>policy-options# info
----------------------------------------------
        community "all-types" members "5000:[1-6][1-9][0-9]"
        community "all-normal" members "5000:[1-5][1-9][0-9]"
  . . .
      as-path "Outside madeup paths" ".* 5001 .*"
        as-path "Outside Internet paths" ".* 5002 .*"
        policy-statement "RejectOutsideASPaths"
            entry 1
                from
                    protocol bgpospf
                    as-path "Outside madeup paths"
                exit
                action reject
                exit
            exit
            entry 2
                from
                    protocol bgpospf
                    as-path "Outside Internet paths"
                exit
                action reject
                exit
            exit
            entry 3
                from
                    protocol ospf
                exit
                to
                    protocol bgpospf
                exit
                action reject
                exit
            exit
            entry 4
                from
                    protocol isis
                exit
                to
                    protocol bgpospf
                exit
                action reject
                exit
            exit
            default-action accept
            exit
        exit
        policy-statement "aggregate-customer-peer-only"
```

```
            entry 1
                from
                    community "all-customer-announce"
                exit
                action accept
                exit
            exit
            default-action reject
            exit
        exit
----------------------------------------------
A:ALA-B>config>router>policy-options#
```

Configuring Route Policy Components

Use the CLI syntax displayed below to configure:

Beginning the Policy Statement

Use the following CLI syntax to begin a policy statement configuration. In order for a policy statement to be complete an entry must be specified (see).

CLI Syntax: `config>router>policy-options`
`    begin`
`        policy-statement` *name*
`            description` *text*

The following error message displays when the you try to modify a policy options command without entering `begin` first.

```
A:ALA-B>config>router>policy-options# policy-statement "allow all"
MINOR: CLI The policy-options must be in edit mode by calling begin before any changes can
be made.
```

The following example displays policy statement configuration command usage. These commands are configured in the `config>router` context.

Example: `config>router# policy-options`
`        policy-options# begin`

There are no default policy statement options. All parameters must be explicitly configured.

Creating a Route Policy

To enter the mode to create or edit route policies, you must enter the **begin** keyword at the **config>router>policy-options** prompt. Other editing commands include:

- The **commit** command saves changes made to route policies during a session.

- The **abort** command discards changes that have been made to route policies during a session.

The following error message displays when the you try to modify a policy options command without entering **begin** first.

```
A:ALA-B>config>router>policy-options# policy-statement "allow all"
MINOR: CLI The policy-options must be in edit mode by calling begin before any changes can
be made.

A:ALA-B>config>router>policy-options# info
#----------------------------------------
# Policy
#----------------------------------------

        policy-options
            begin
            policy-statement "allow all"
         description "General Policy"
        ...
            exit
    exit
--------------------------------------------
A:ALA-B>config>router>policy-options#
```

Configuring a Default Action

Specifying a default action is optional. The default action controls those packets not matching any policy statement entries. If no default action is specified for the policy, then the action associated with the protocol to which the routing policy was applied is performed. The default action is applied only to those routes that do not match any policy entries.

A policy statement must include at least one entry (see).

To enter the mode to create or edit route policies, you must enter the `begin` keyword at the **config>router>policy-options** prompt. Other editing commands include:

- The **commit** command saves changes made to route policies during a session.
- The **abort** command discards changes that have been made to route policies during a session.

The following example displays the default action configuration:

```
A:ALA-B>config>router>policy-options# info
----------------------------------------------
            policy-statement "1"
                default-action accept
                    as-path add "test"
                    community add "365"
                    damping "flaptest"
                    next-hop 10.10.10.104
                exit
            exit
----------------------------------------------
A:ALA-B>config>router>policy-options#
```

Configuring an Entry

An entry action must be specified. The other parameters in the **entry action** context are optional. Refer to the for the commands and syntax.

The following example displays entry parameters and includes the default action parameters which were displayed in the previous section.

```
A:ALA-B>config>router>policy-options# info
---------------------------------------------
        policy-statement "1"
            entry 1
                to
                    protocol bgp
                    neighbor 10.10.10.104
                exit
                action accept
                exit
            exit
            entry 2
                from
                    protocol ospf 1
                exit
                to
                    protocol ospf
                    neighbor 10.10.0.91
                exit
                action accept
                exit
            exit
            default-action accept
                . . .
            exit
        exit
---------------------------------------------
A:ALA-B>config>router>policy-options#
        policy-statement "exporttmsgrt"
            entry 1
                from
                    protocol vpn-leak
                exit
                action accept
                exit
            exit
            entry 2
                from
                    protocol tms
                exit
                action accept
                exit
            exit
        exit
        commit
    exit
exit
```

Configuring a Community List

Community lists are composed of a group of destinations which share a common property. Community lists allow you to administer actions on a configured group instead of having to execute identical commands for each member.

The following example displays a community list configuration:

```
A:ALA-B>config>router>policy-options# info
---------------------------------------------
    community "eastern" members "100:200"
    community "western" members "100:300"
    community "northern" members "100:400"
    community "southern" members "100:500"
    community "headquarters" members "100:1000"
    policy-statement "1"
            entry 1
                to
                    protocol bgp
                    neighbor 10.10.10.104
                exit
                action accept
. . .
---------------------------------------------
A:ALA-B>config>router>policy-options#
```

Configuring Damping

NOTES:

- For each damping profile, all parameters must be configured.
- The `suppress` value must be greater than the `reuse` value (see).
- Damping can be enabled in the `config>router>bgp` context on the BGP global, group, and neighbor levels. If damping is enabled, but route policy does not specify a damping profile, the default damping profile will be used. This profile is always present and consists of the following parameters:

half-life:	15 minutes
max-suppress:	60 minutes
suppress:	3000
reuse:	750

The following example displays a damping configuration:

```
*A:cses-A13>config>router>policy-options# info
---------------------------------------------
        damping "damptest123"
            half-life 15
            max-suppress 60
            reuse 750
            suppress 1000
        exit
---------------------------------------------
*A:cses-A13>config>router>policy-options#
```

Configuring a Prefix List

The following example displays a prefix list configuration:

```
A:ALA-B>config>router>policy-options# info
----------------------------------------------
            prefix-list "western"
                    prefix 10.10.0.1/32 exact
                    prefix 10.10.0.2/32 exact
                    prefix 10.10.0.3/32 exact
                    prefix 10.10.0.4/32 exact
            exit
            damping "damptest123"
                half-life 15
                max-suppress 60
                reuse 750
            exit
----------------------------------------------
A:ALA-B>config>router>policy-options#
```

Configuring PIM Join/Register Policies

Join policies are used in Protocol Independent Multicast (PIM) configurations to prevent the transportation of multicast traffic across a network and the dropping of packets at a scope at the edge of the network. PIM Join filters reduce the potential for denial of service (DoS) attacks and PIM state explosion—large numbers of Joins forwarded to each router on the RPT, resulting in memory consumption. See Importing PIM Join/Register Policies on page 78.

*,G or S,G is the information used to forward unicast or multicast packets.

- **group-address** matches the group in join/prune messages

  ```
  group-address 229.55.150.208/32 exact
  ```

- **source-address** matches the source in join/prune messages

  ```
  source-address 192.168.0.0/16 longer
  ```

- **interface** matches any join message received on the specified interface

  ```
  interface port 1/1/1
  ```

- **neighbor** matches any join message received from the specified neighbor

  ```
  neighbor 1.1.1.1
  ```

The following configuration example will not allow join messages for group 229.50.50.208/32 and source 192.168.0.0/16 but allows other join messages.

Configuring policy-statement

```
A:ALA-B>config>router# policy-options
A:ALA-B>config>router>policy-options# begin
A:ALA-B>config>router>policy-options# policy-statement foo
A:ALA-B>config>router>policy-options>policy-statement$ entry 10
A:ALA-B>config>router>policy-options>policy-statement>entry$ from
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ group-address
229.50.50.208/32
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ source-address
192.168.0.0
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ exit
A:ALA-B>config>router>policy-options>policy-statement>entry# action reject
A:ALA-B>config>router>policy-options>policy-statement>entry#
```

The following configuration example allows registers for *, 224,0.0.0/8.

```
A:ALA-B>config>router>policy-options# policy-statement reg-pol
A:ALA-B>config>router>policy-options>policy-statement$ entry 10
A:ALA-B>config>router>policy-options>policy-statement>entry$ from
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ group-address 224.0.0.0/
8
A:ALA-B>config>router>policy-options>policy-statement>entry# action accept
A:ALA-B>config>router>policy-options>policy-statement>entry>action# exit
A:ALA-B>config>router>policy-options>policy-statement>entry# exit
A:ALA-B>config>router>policy-options>policy-statement# exit
```

```
A:ALA-B>config>router>policy-options# info
----------------------------------------------
...
          policy-statement "foo"
              entry 10
                  from
                      group-address "229.50.50.208/32"
                      source-address 192.168.0.0
                  exit
                  action reject
              exit
          exit
          policy-statement "reg-pol"
              entry 10
                  from
                      group-address "224.0.0.0/8"
                  exit
                  action accept
                  exit
              exit
          exit
...
----------------------------------------------
A:ALA-B>config>router>policy-options#
```

Configuring Bootstrap Message Import and Export Policies

Bootstrap import and export policies are used to control the flow of bootstrap messages to and from the RP.

The following configuration example specifies that no BSR messages received or sent out of interface port 1/1/1.

```
A:ALA-B>config>router>policy-options# policy-statement pim-import
:A:ALA-B>config>router>policy-options>policy-statement$ entry 10
:A:ALA-B>config>router>policy-options>policy-statement>entry$ from
:A:ALA-B>config>router>policy-options>policy-statement>entry>from$ interface port 1/1/1
:A:ALA-B>config>router>policy-options>policy-statement>entry>from$ exit
:A:ALA-B>config>router>policy-options>policy-statement>entry# action reject
:A:ALA-B>config>router>policy-options>policy-statement>entry# exit
:A:ALA-B>config>router>policy-options>policy-statement# exit

:A:ALA-B>config>router>policy-options# policy-statement pim-export
:A:ALA-B>config>router>policy-options>policy-statement$ entry 10
:A:ALA-B>config>router>policy-options>policy-statement>entry$ to
:A:ALA-B>config>router>policy-options>policy-statement>entry>to$ interface port 1/1/1
:A:ALA-B>config>router>policy-options>policy-statement>entry# action reject
:A:ALA-B>config>router>policy-options>policy-statement>entry# exit
:A:ALA-B>config>router>policy-options>policy-statement# exit

:A:ALA-B>configure router pim rp bootstrap-import pim-import
:A:ALA-B>configure router pim rp bootstrap-export pim-export
```

Route Policy Configuration Management Tasks

This section discusses the following route policy configuration management tasks:

Editing Policy Statements and Parameters

Route policy statements can be edited to modify, add, or delete parameters. To enter the mode to edit route policies, you must enter the `begin` keyword at the `config>router> policy-options` prompt. Other editing commands include:

- The **commit** command saves changes made to route policies during a session.
- The **abort** command discards changes that have been made to route policies during a session.

The following example displays a changed configuration:

```
A:ALA-B>config>router>policy-options>policy-statement# info
----------------------------------------------
            description "Level 1"
            entry 1
                to
                    protocol bgp
                    neighbor 10.10.10.104
                exit
                action accept
                exit
            exit
            entry 2
                from
                    protocol ospf
                exit
                to
                    protocol ospf
                    neighbor 10.10.0.91
                exit
                action accept
                exit
            exit
            entry 4
                description "new entry"
                from
                    protocol isis
                    area 0.0.0.20
                exit
                action reject
```

```
                exit
                default-action accept
                    as-path add "test"
                    community add "365"
                    damping "flapper"
                    next-hop 10.10.10.104
        exit
        ---------------------------------------------
```

Deleting an Entry

Use the following CLI syntax to delete a policy statement entry:

CLI Syntax: `config>router>policy-options`
```
        begin
        commit
        abort
        policy-statement name
            no entry entry-id
```

The following example displays the commands required to delete a policy statement entry.

Example: `config>router>policy-options# begin`
```
        policy-options# policy-statement "1"
        policy-options>policy-statement# no entry 4
        policy-options>policy-statement# commit
```

Deleting a Policy Statement

Use the following CLI syntax to delete a policy statement:

CLI Syntax: `config>router>policy-options`
```
        begin
        commit
        abort
        no policy-statement name
```

The following example displays the commands required to delete a policy statement.

Example: `config>router>policy-options# begin`
```
        policy-options# no policy-statement 1
        policy-options# commit
```