Configuring Filter Policies with CLI

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

Topics in this section include:

Basic Configuration

The most basic IP, IPv6 and MAC filter policies must have the following:

- A filter ID
- Template scope, either *exclusive* or *template*
- Default action, either drop or forward
- At least one filter entry
  - → Specified action, either drop or forward
  - → Specified matching criteria

The following example displays a sample configuration of an IP filter policy. The configuration blocks all incoming TCP session except Telnet and allows all outgoing TCP sessions from IP net 10.67.132.0/24. Figure 24 depicts the interface to apply the filter.

```
A:ALA-1>config>filter# info
----------------------------------------------
        ip-filter 3 create
            entry 10 create
                match protocol 6
                    dst-port eq 23
                    src-ip 10.67.132.0/24
                exit
                action forward
            exit
            entry 20 create
                match protocol 6
                    tcp-syn true
                    tcp-ack false
                exit
                action drop
            exit
        exit
----------------------------------------------
A:ALA-1>config>filter#
```

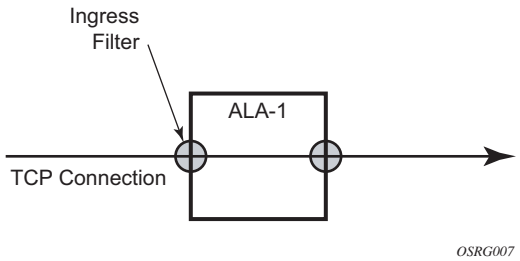

Figure 24: Applying an IP Filter to an Ingress Interface

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed for both IP and MAC filter configurations and provides the CLI commands.

To configure a filter policy, perform the following tasks:

- Creating an IP Filter Policy on page 449
- Creating an IPv6 Filter Policy on page 454
- Creating a MAC Filter Policy on page 455
- Creating a Match List for Filter Policies on page 459
- Applying (IPv4/v6) Filter Policies to a Network Port on page 461

Creating an IP Filter Policy

Configuring and applying filter policies is optional. Each filter policy must have the following:

- The filter type specified (IP)
- A filter policy ID
- A default action, either drop or forward
- Filter policy scope specified, either *exclusive* or *template*
- At least one filter entry with matching criteria specified
- Optionally, an existing filter policy can have a Filter Name assigned, that can then be used in CLI to reference that filter policy including assigning it to SAPs and/or network interfaces.

IP Filter Policy

The following displays an exclusive filter policy configuration example:

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        ip-filter 12 create
            description "IP-filter"
            scope exclusive
        exit
...
----------------------------------------------
A:ALA-7>config>filter#
```

IP Filter Entry

Within a filter policy, configure filter entries which contain criteria against which ingress, egress, or network traffic is matched. The action specified in the entry determine how the packets are handled, either dropped or forwarded.

- Enter a filter entry ID. The system does not dynamically assign a value.
- Assign an action, either drop or forward.
- Specify matching criteria.

The following displays an IP filter entry configuration example.

```
A:ALA-7>config>filter>ip-filter# info
----------------------------------------------
            description "filter-main"
            scope exclusive
            entry 10 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                no action
            exit
----------------------------------------------
A:ALA-7>config>filter>ip-filter#
```

Configuring the HTTP-Redirect Option

If http-redirect is specified as an action, a corresponding forward entry must be specified before the redirect. Note that http-redirect is not supported on 7450 ESS-1 models.

The following displays an http-redirect configuration example:

```
A:ALA-48>config>filter>ip-filter# info
----------------------------------------------
            description "filter-main"
            scope exclusive
            entry 10 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                no action
            exit
            entry 20 create
                match protocol tcp
                    dst-ip 100.0.0.2/32
                    dst-port eq 80
                exit
                action forward
            exit
            entry 30 create
                match protocol tcp
                    dst-ip 10.10.10.91/24
                    dst-port eq 80
                exit
                action http-redirect "http://100.0.0.2/login.cgi?mac=$MAC$sap=$S
AP&ip=$IP&orig_url=$URL"
            exit
----------------------------------------------
A:ALA-48>config>filter>ip-filter#
```

Cflowd Filter Sampling

Within a filter entry, you can specify that traffic matching the associated IP filter entry is sampled. if the IP interface is set to cflowd acl mode. Enabling filter-sample enables the cflowd tool.

The following displays an IP filter entry configuration example.

```
A:ALA-7>config>filter>ip-filter# info
----------------------------------------------
            description "filter-main"
            scope exclusive
            entry 10 create
                description "no-91"
                filter-sample
                interface-disable-sample
                match
                exit
                action forward redirect-policy redirect1
            exit
----------------------------------------------
A:ALA-7>config>filter>ip-filter#
```

Within a filter entry, you can also specify that traffic matching the associated IP filter entry is not sampled by cflowd if the IP interface is set to cflowd interface mode. The following displays an IP filter entry configuration example:

```
A:ALA-7>config>filter>ip-filter# info
----------------------------------------------
            description "filter-main"
            scope exclusive
            entry 10 create
                description "no-91"
                no filter-sample
                no interface-disable-sample
                match
                exit
                action forward redirect-policy redirect1
            exit
----------------------------------------------
A:ALA-7>config>filter>ip-filter#
```

Creating an IPv6 Filter Policy

Configuring and applying IPv6 filter policies is optional. IPv6 Filter Policy must be configured separately from IP (IPv4) filter policy. The configuration mimics IP Filter policy configuration. Please see Creating an IP Filter Policy on page 449.

Creating a MAC Filter Policy

Configuring and applying filter policies is optional. Each filter policy must have the following:

- The filter policy type specified (MAC normal, MAC isid, MAC vid).
- A filter policy ID.
- A default action, either drop or forward.
- Filter policy scope, either *exclusive* or *template.*
- At least one filter entry.
- Matching criteria specified.

MAC Filter Policy

The following displays an MAC filter policy configuration example:

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        mac-filter 90 create
            description "filter-west"
            scope exclusive
            type normal
        exit
----------------------------------------------
A:ALA-7>config>filter#
```

MAC ISID Filter Policy

The following displays an ISID filter configuration example:

```
A;ALA-7>config>filter# info
----------------------------------------------
mac-filter 90 create
     description "filter-wan-man"
     scope template
     type isid
     entry 1 create
          description "drop-local-isids"
          match
               isid 100 to 1000
          exit
          action drop
     exit
     entry 2 create
          description "allow-wan-isids"
          match
               isid 150
          exit
          action forward
     exit
```

MAC VID Filter Policy

The following displays VID filter configuration example:

```
A:TOP_NODE>config>filter>mac-filter# info
----------------------------------------------
      default-action forward
      type vic
      entry 1 create
         match frame-type ethernet_II
           ouiter-tag 85 4095
         exit
         action drop
      exit
      entry 2 create
         match frame-type ethernet_II
           ouiter-tag 43 4095
         exit
         action drop
      exit
----------------------------------------------
A:TOP_NODE>config>filter>mac-filter#
```

MAC Filter Entry

Within a filter policy, configure filter entries which contain criteria against which ingress, egress, or network traffic is matched. The action specified in the entry determine how the packets are handled, either dropped or forwarded.

- Enter a filter entry ID. The system does not dynamically assign a value.
- Assign an action, either drop or forward.
- Specify matching criteria.

The following displays a MAC filter entry configuration example:

```
A:sim1>config>filter# info
----------------------------------------------
        mac-filter 90 create
            entry 1 create
                description "allow-104"
                match
                exit
                action drop
            exit
        exit
----------------------------------------------
A:sim1>config>filter#
```

Creating a Match List for Filter Policies

IP filter policies support usage of match lists as a single match criteria. To create a match list you must:

- Specify a type of a match list (IPv4 address prefix for example).
- Define a unique match list name (IPv4PrefixBlacklist for example).
- Specify at least one list argument (a valid IPv4 address prefix for example).

Optionally a description can also be defined.

The following displays an IPv4 address prefix list configuration example and usage in an IP filter policy:

```
*A:ala-48>config>filter# info
----------------------------------------------
      match-list
        ip-prefix-list "IPv4PrefixBlacklist"
           description "default IPv4 prefix blacklist"
           prefix 10.0.0.0/21
           prefix 10.254.0.0/24
        exit
      exit
      ip-filter 10
         scope template
         filter-name "IPv4PrefixBlacklistFilter"
         entry 10
            match
               src-ip ip-prefix-list IPv4PrefixBlacklist
            exit
            action drop
         exit
       exit
----------------------------------------------
```

Apply IP (v4/v6) and MAC Filter Policies to a Service

IP and MAC filter policies are applied by associating them with a SAP and/or spoke-sdp in ingress and/or egress direction as desired. Filter ID is used to associate an existing filter policy, or if defined, a Filter Name for that Filter ID policy can be used in the CLI.

The following output displays IP and MAC filters assigned to an ingress and egress SAP and spoke SDP:

```
A:ALA-48>config>service>epipe# info
----------------------------------------------
            sap 1/1/1.1.1 create
                ingress
                    filter ip 10
                exit
                egress
                    filter mac 92
                exit
            exit
            spoke-sdp 8:8 create
                ingress
                    filter ip "epipe sap default filter"
                exit
                egress
                    filter mac 91
                exit
            exit
            no shutdown
----------------------------------------------
A:ALA-48>config>service>epipe#
```

The following output displays an IPv6 filters assigned to an IES service interface:

```
A:ALA-48>config>service>ies# info
----------------------------------------------
            interface "testA" create
                address 192.22.1.1/24
                sap 2/1/3:0 create
                exit
                ipv6
                 ingress
                    filter ipv6 100
                 egress
                    filter ipv6 100
                exit
            exit
...
----------------------------------------------
A:ALA-48>config>service>ies#
```

Applying (IPv4/v6) Filter Policies to a Network Port

IP filter policies can be applied to network IP (v4/v6)interfaces. MAC filters cannot be applied to network IP interfaces or to routable IES services. Similarly to applying filter policies to service, IP (v4/v6) filter policies are applied to network interfaces by associating a policy with ingress and/or egress direction as desired. Filter ID is used to associate an existing filter policy, or if defined, a Filter Name for that Filter ID policy can be used in the CLI.

The following displays an IP filter applied to an interface at ingress.

```
A:ALA-48>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
...
        interface "to-104"
            address 10.0.0.103/24
            port 1/1/1
            ingress
                filter ip 10
            exit
            egress
                filter ip "default network egress policy"
            exit
        exit
...
#------------------------------------------
A:ALA-48>config>router#
```

The following displays IPv4 and IPv6 filters applied to an interface at ingress and egress.

```
A:config>router>if# info
----------------------------------------------
            port 1/1/1
            ipv6
                address 3FFE::101:101/120
            exit
            ingress
                filter ip 2
                filter ipv6 1
            exit
            egress
                filter ip 2
                filter ipv6 1
            exit
----------------------------------------------
A:config>router>if#
```

Creating a Redirect Policy

Configuring and applying redirect policies is optional. Each redirect policy must have the following:

- A destination IP address
- A priority (default is 100)
- At least one of the following tests must be enabled:
  - → Ping test
  - → SNMP test
  - → URL test

The following displays a redirection policy configuration:

```
A:ALA-7>config>filter# info
----------------------------------------------
        redirect-policy "redirect1" create
            destination 10.10.10.104 create
                description "SNMP_to_104"
                priority 105
                snmp-test "SNMP-1"
                    interval 30
                    drop-count 30 hold-down 120
                exit
                no shutdown
            exit
            destination 10.10.10.105 create
                priority 95
                ping-test
                    timeout 30
                    drop-count 5
                exit
                no shutdown
            exit
            destination 10.10.10.106 create
                priority 90
                url-test "URL_to_106"
                    url "http://aww.alcatel.com/ipd/"
                    interval 60
                    return-code 2323 4567 raise-priority 96
                exit
                no shutdown
            exit
...
----------------------------------------------
A:ALA-7>config>filter#
```

Configuring Policy-Based Forwarding for Deep Packet Inspection in VPLS

The purpose policy-based forwarding is to capture traffic from a customer and perform a deep packet inspection (DPI) and forward traffic, if allowed, by the DPI.

In the following example, the split horizon groups are used to prevent flooding of traffic. Traffic from customers enter at SAP 1/1/5:5. Due to the mac-filter 100 that is applied on ingress, all traffic with dot1p 07 marking will be forwarded to SAP 1/1/22:1, which is the DPI.

DPI performs packet inspection/modification and either drops the traffic or forwards the traffic back into the box through SAP 1/1/21:1. Traffic will then be sent to spoke-sdp 3:5.

SAP 1/1/23:5 is configured to see if the VPLS service is flooding all the traffic. If flooding is performed by the router then traffic would also be sent to SAP 1/1/23:5 (which it should not).

Figure shows an example to configure policy-based forwarding for deep packet inspection on a VPLS service. For information about configuring services, refer to the 7750 SR OS Services Guide.

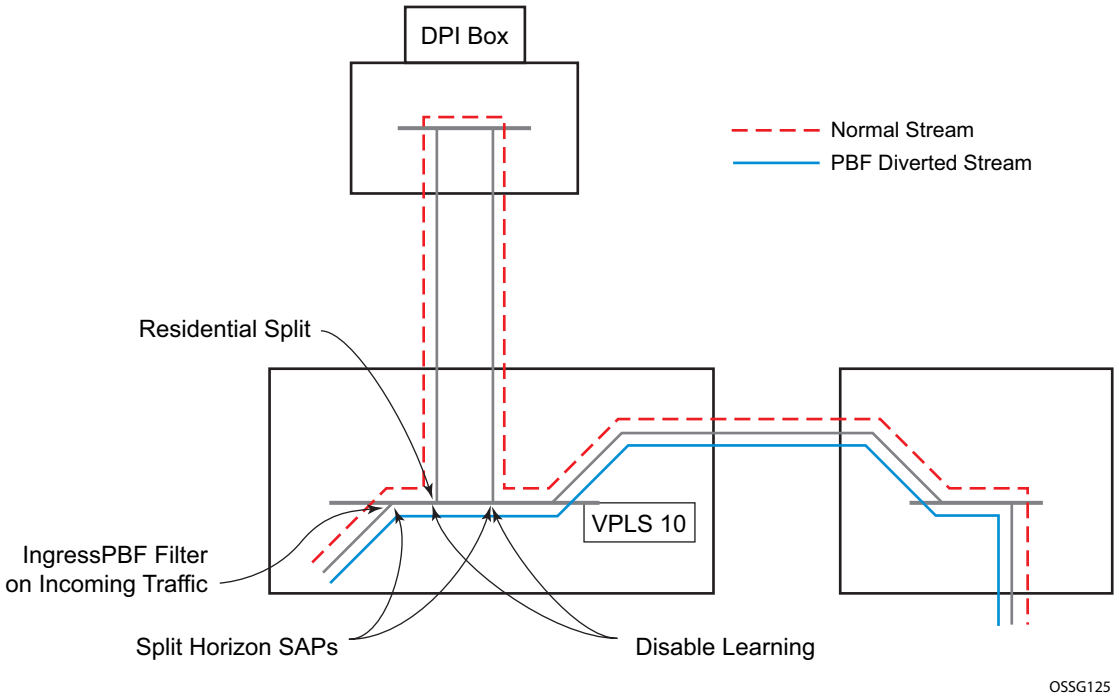

Figure 25: Policy-Based Forwarding for Deep Packet Inspection

The following displays a VPLS service configuration with DPI example:

```
*A:ALA-48>config>service# info
----------------------------------------------
...
        vpls 10 customer 1 create
            service-mtu 1400
            split-horizon-group "dpi" residential-group create
            exit
            split-horizon-group "split" create
            exit
            stp
                shutdown
            exit
            sap 1/1/21:1 split-horizon-group "split" create
                disable-learning
                static-mac 00:00:00:31:11:01 create
            exit
            sap 1/1/22:1 split-horizon-group "dpi" create
                disable-learning
                static-mac 00:00:00:31:12:01 create
            exit
            sap 1/1/23:5 create
                static-mac 00:00:00:31:13:05 create
            exit
            no shutdown
        exit
...
----------------------------------------------
*A:ALA-48>config>service#
```

The following displays a MAC filter configuration example:

```
*A:ALA-48>config>filter# info
----------------------------------------------
...
        mac-filter 100 create
            default-action forward
            entry 10 create
                match
                    dot1p 7 7
                exit
                log 101
                action forward sap 1/1/22:1
            exit
        exit
...
----------------------------------------------
*A:ALA-48>config>filter#
```

The following displays the MAC filter added to the VPLS service configuration:

```
*A:ALA-48>config>service# info
----------------------------------------------
...
        vpls 10 customer 1 create
            service-mtu 1400
            split-horizon-group "dpi" residential-group create
            exit
            split-horizon-group "split" create
            exit
            stp
                shutdown
            exit
            sap 1/1/5:5 split-horizon-group "split" create
                ingress
                    filter mac 100
                exit
                static-mac 00:00:00:31:15:05 create
            exit
            sap 1/1/21:1 split-horizon-group "split" create
                disable-learning
                static-mac 00:00:00:31:11:01 create
            exit
            sap 1/1/22:1 split-horizon-group "dpi" create
                disable-learning
                static-mac 00:00:00:31:12:01 create
            exit
            sap 1/1/23:5 create
                static-mac 00:00:00:31:13:05 create
            exit
            spoke-sdp 3:5 create
            exit
            no shutdown
        exit
....
----------------------------------------------
*A:ALA-48>config>service#
```

Filter Management Tasks

This section discusses the following filter policy management tasks:

Renumbering Filter Policy Entries

The system exits the matching process when the first match is found and then executes the actions in accordance with the specified action. Because the ordering of entries is important, the numbering sequence may need to be rearranged. Entries should be numbered from the most explicit to the least explicit.

The following example illustrates renumbering of filter entries.

Example:

```
config>filter>ip-filter# renum 10 15
config>filter>ip-filter# renum 20 10
config>filter>ip-filter# renum 40 1
```

The following displays the original filter entry order on the left side and the reordered filter entries on the right side:

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "filter-main"
            scope exclusive
            entry 10 create
                description "no-91"
                filter-sample
                interface-disable-sample
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
               action forward redirect-policy redirect1
            exit
            entry 20 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                action drop
            exit
            entry 30 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.200/24
                exit
                action forward
            exit
            entry 40 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
        exit
...
----------------------------------------------
A:ALA-7>config>filter#
```

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "filter-main"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
            entry 10 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                action drop
            exit
            entry 15 create
                description "no-91"
                filter-sample
                interface-disable-sample
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
               action forward redirect-policy
                  redirect1
            exit
            entry 30 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.200/24
                exit
                action forward
            exit
        exit
...
----------------------------------------------
A:ALA-7>config>filter#
```

Modifying a Filter Policy

There are several ways to modify an existing filter policy. A filter policy can be modified dynamically as part of subscriber management dynamic insertion/removal of filter policy entries (see SROS Triple Play Guide for details). A filter policy can be modified indirectly by configuration change to a match list the filter policy uses (as described earlier in this guide). In addition, a filter policy can be directly edited as described below.

To access a specific IP (v4/v6), or MAC filter, you must specify the filter ID, or if defined, filter name. Use the **no** form of the command to remove the command parameters or return the parameter to the default setting.

Example:

```
config>filter>ip-filter# description "New IP filter info"
config>filter>ip-filter# entry 2 create
config>filter>ip-filter>entry$ description "new entry"
config>filter>ip-filter>entry# action drop
config>filter>ip-filter>entry# match dst-ip 10.10.10.104/32
config>filter>ip-filter>entry# exit
config>filter>ip-filter#
```

The following output displays the modified IP filter output:

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "New IP filter info"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
            entry 2 create
                description "new entry"
                match
                    dst-ip 10.10.10.104/32
                exit
                action drop
            exit
            entry 10 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                action drop
            exit
```

```
            entry 15 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
                action forward
            exit
            entry 30 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.200/24
                exit
                action forward
            exit
        exit
..
-------------------------------------------
A:ALA-7>config>filter#
```

Deleting a Filter Policy

Before you can delete a filter, you must remove the filter association from all the applied ingress and egress SAPs and network interfaces by executing **no filter** command in all context where the filter is used.

The following illustrates an example of removing a filter (filter ID 11) from an ingress ePipe SAP:

Example:
```
config>service# epipe 5
config>service>epipe# sap 1/1/2:3
config>service>epipe>sap# ingress
config>service>epipe>sap>ingress# no filter
```

After you have removed the filter from the SAPs network interfaces, you can delete the filter as shown in the following example.

Example:
```
config>filter# no ip-filter 11
```

Modifying a Redirect Policy

To access a specific redirect policy, you must specify the policy name. Use the `no` form of the command to remove the command parameters or return the parameter to the default setting.

Example:
```
config>filter# redirect-policy redirect1
config>filter>redirect-policy# description "New redirect info"
config>filter>redirect-policy# destination 10.10.10.106
config>filter>redirect-policy>dest# no url-test "URL_to_106"
config>filter>redirect-policy>dest# url-test "URL_to_Proxy"
config>filter>redirect-policy>dest>url-test$ url http://
            www.alcatel.com
config>filter>redirect-policy>dest>url-test# interval 10
config>filter>redirect-policy>dest>url-test# timeout 10
config>filter>redirect-policy>dest>url-test# return-code 1
            4294967295 raise-priority 255
```

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        redirect-policy "redirect1" create
            description "New redirect info"
            destination 10.10.10.104 create
                description "SNMP_to_104"
                priority 105
                snmp-test "SNMP-1"
                    interval 30
                    drop-count 30 hold-down 120
                exit
                no shutdown
            exit
            destination 10.10.10.105 create
                priority 95
                ping-test
                    timeout 30
                    drop-count 5
                exit
                no shutdown
            exit
            destination 10.10.10.106 create
                priority 90
                url-test "URL_to_Proxy"
                    url "http://www.alcatel.com"
                    interval 10
                    timeout 10
                    return-code 1 4294967295 raise-priority 255
                exit
                no shutdown
            exit
            no shutdown
        exit
...
----------------------------------------------
A:ALA-7>config>filter#
```

Deleting a Redirect Policy

Before you can delete a redirect policy from the filter configuration, you must remove the policy association from the IP filter.

The following example shows the command usage to replace the configured redirect policy (**redirect1**) with a different redirect policy (**redirect2**) and then removing the **redirect1** policy from the filter configuration.

Example:
```
config>filter>ip-filter 11
       config>filter>ip-filter# entry 1
       config>filter>ip-filter>entry# action forward redirect-policy
redirect2
       config>filter>ip-filter>entry# exit
       config>filter>ip-filter# exit
       config>filter# no redirect-policy redirect1


A:ALA-7>config>filter>ip-filter# info
----------------------------------------------
           description "This is new"
           scope exclusive
           entry 1 create
             filter-sample
             interface-disable-sample
               match
                   dst-ip 10.10.10.91/24
                   src-ip 10.10.10.106/24
               exit
               action forward redirect-policy redirect2
           exit
           entry 2 create
               description "new entry"
...
----------------------------------------------
A:ALA-7>config>filter>ip-filter#
```

Copying Filter Policies

When changes are to be made to an existing filter policy applied to a one or more SAPs/network interfaces, it is recommended to first copy the applied filter policy, then modify the copy and then overwrite the applied policy with the modified copy. This ensures that a policy being modified is not applied when partial changes are done as any filter policy edits are applied immediately to all services where the policy is applied.

New filter policies can also be created by copying an existing policy and renaming the new filter.

The following displays the command usage to copy an existing IP filter (**11**) to create a new filter policy (**12**) that can then be edited. And once edits are completed, it can be used to overwrite existing policy (**11**).

Example: `config>filter# copy ip-filter 11 to 12`

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "This is new"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
            entry 2 create
...
        ip-filter 12 create
            description "This is new"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
            entry 2 create
...
----------------------------------------------
A:ALA-7>config>filter#
```