# Control Plane Policing (CoPP)

# Table of contents

Control Plane Policing or Policies (CoPP) ensures the CPU and control plane are not over-utilized which is essential for the robustness of the switch. CoPP limits the number of control plane packets.

This software implements several CoPP mechanisms:

- ACLs may be used to limit the rate of packets or bytes of a certain type, including L3 control packets (L2 control packets are forwarded to the CPU before the ACL)
- Policers on traffic going to the CPU—these policers are configured by the operating system and cannot be modified by the user
- IP filter tables limit the traffic to the CPU coming in from the management ports

# IP Table Filtering

IP table filtering is a mechanism that allows the user to apply actions to a specific control packet flow identified by a certain flow key.

This mechanism is used in order to protect switch control traffic against attacks. For example, it could allow traffic coming from a specific trusted management subnet only, block the SNMP UDP port from receiving traffic, and force ping rate to be lower than a specific threshold.

Each IP table rule is defined by key, priority, and action:

- Key—the key is a combination of physical port and layer 3 parameters (e.g. SIP, DIP, SPORT, DPORT, etc.), and other fields. Each part of the key, can be set to a specific value or masked.
- Priority—each rule in the IP table is assigned a priority, and the rule with the highest priority whose key matches the packet executes the action.
- Action—the action describes the behavior of packets which match the key. The action type may be drop, accept, rate limit, etc.

An IP-table rule is bound to an IP interface that can be a management out-of-band interface, VLAN interface, or router port interface. Once bound, all traffic received (ingress rule) or transmitted (egress rule) in this direction is being verified with all bounded rules.

Once a match was found, the rule action is executed. If no match is found, the default policy of the chain shall apply.

**Note**

IP table rules get a lower priority than ACL mechanism.

**Note**

In the rare case that IP filter is used while the input policy is "drop" (i.e., ip filter chain input policy drop) and an NTP server or an InfiniBand switch with SM HA enabled is used, then the following rule needs to be added that allows src-ip 127.0.0.1 (which is a requirement for any clustered application (e.g., sm-ha) and NTP):

ip filter chain input rule append tail target accept dup-delete source-addr 127.0.0.1 /32

## Configuring IP Table Filtering

Prerequisite for IPv6:

```
switch (config) # ipv6 enable
```

To configure IPv4 table filtering:

1. Select the policy that applies to the input/output chain (default is “accept”).

   ```
   switch (config)# ip filter chain input policy drop
   switch (config)# ip filter chain output policy accept
   ```

2. Append filtering rules to the list or set a specific rule number, select a target, and (optional) any additional filter conditions. For example:

```
switch (config) # ip filter chain input rule append tail target
rate-limit 2 protocol udp
switch (config) # ip filter chain input rule set 2 target drop
protocol icmp in-intf mgmt1
switch (config) # ip filter chain output rule append tail
target drop protocol icmp
```

3. Enable IP table filtering.

```
switch (config) # ip filter enable
```

4. Verify IP table filtering configuration.

```
switch (config) # show ip filter configured

Packet filtering for IPv4: enabled

IPv4 configuration:
  Chain 'input' Policy 'accept':
    Rule 1:
      Target      : rate-limit 2 pps
      Protocol    : udp
      Source      : all
      Destination : all
      Interface   : all
      State       : any
      Other Filter:  -

    Rule 2:
      Target      : drop
      Protocol    : icmp
```

```
      Source      : all
      Destination : all
      Interface   : mgmt1 (ingress)
      State       : any
      Other Filter:  -

  Chain 'output' Policy 'accept':
    Rule 1:
      Target      : drop
      Protocol    : icmp
      Source      : all
      Destination : all
      Interface   : all
      State       : any
      Other Filter: -
```

## Modifying IP Table Filtering

To modify IP table filtering configuration:

```
switch (config) # ip filter chain input rule modify 3 target
reject-with icmp6-adm-prohibited source-addr 10::0 /126
```

To delete an existing IP table filtering rule:

```
switch (config) # no ip filter chain input rule 2
```

To delete all existing IP table filtering rules:

```
switch (config) # no ip filter chain output rule all
```

To insert an IP table filtering rule in a chain:

```
switch (config) # ip filter chain input rule 2 set target drop
protocol tcp dest-port 22 in-intf mgmt1
```

## Rate-Limit Rule Configuration

Using a rate-limit target allows to create a rule to limit the rate of certain traffic types. The limit is specified in packets per second (pps) and can be anywhere between 1-1000 pps. When enabled, the system takes the user specified rate and converts it into units of 1/10000 of a second. Therefore, any value greater than 100 can have a slight difference when the rule is displayed using the show command.

Rate limits can be set using the parameter "rate-limit-above" in order to drop packets whenever traffic is above the set limit. For example: ip filter chain input rule append tail target drop rate-limit-above 1/second source-addr 1.1.1.1 /32.

Another option is to use the parameter "rate-limit". This should be followed by a rule that drops additional packets of the same “type”. Alternatively, this can be implicitly achieved by setting the chain policy to “drop” so that it drops packets not processed by matching rules. Otherwise, no effect of the rule is observed as the remaining traffic simply gets accepted.

> **Note**
>
> Rate-limit is implemented with an average rate and a burst-limit. Rate values are specified in pps and take a range from 1-1000 pps. For rate values in the range 1-100, the burst value is set equal to the rate value. For rate values in the range 101-1000, the burst limit is set to 100.

# IP Table Filtering Default Rules

IP table filtering is enabled on both ipv4 and ipv6 and Firewall default IP filter rules are applied.

- To reset/apply default rules on system, run the command “ip filter reset-to-default-rules” for ipv4 **or** "ipv6 filter reset-to-default-rules" for IPv6.
- To enable IP Filter, run the command “ip filter enable”, "ipv6 filter enable".
- To list the default firewall rules, run the command “show ip filter”, "show ipv6 filter".
- Note when touching a default rule (delete/move/modify) all IP Filter rules will be reflected on “show running-config”, to restore default rules, run the command “ip filter reset-to-default-rules” **or "**ipv6 filter reset-to-default-rules**"**
- Restoring factory default configuration will reset the default rules and enable the feature

## IPv4 Firewall Default Rules

| Prerouting-Mangle Chain Rules |
| --- |
| • ip filter chain prerouting-mangle rule append tail target drop in-intf mgmt0 protocol tcp conntrack new tcp-op-mss mss-not-in-range 536:65535 not-dest-port 22-23 |
| Input Chain Rules |
| • ip filter chain input rule append tail target accept in-intf lo<br>• ip filter chain input rule append tail target drop dup-delete dest-addr 127.0.0.0 /8 in-intf mgmt0<br>• ip filter chain input rule append tail target accept dup-delete in-intf mgmt0 state established,related<br>• ip filter chain input rule append tail target drop dup-delete not-dest-port 22-23 in-intf mgmt0 protocol tcp state new tcp-op syn match-not-syn<br>• ip filter chain input rule append tail target drop dup-delete in-intf mgmt0 fragment enable<br>• ip filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp tcp-op flags all<br>• ip filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp tcp-op flags none |

| Prerouting-Mangle Chain Rules |
| --- |
| • ip filter chain input rule append tail target drop dup-delete in-intf mgmt0 state invalid<br>• ip filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp tcp-op flags reset rate-limit-above 2/second burst-limit-above 2<br>• ip filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp state new rate-limit-above 50/second burst-limit-above 50<br>• ip filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp conntrack new rate-limit-above 60/second burst-limit-above 20<br>• ip filter chain input rule append tail target drop dup-delete in-intf mgmt0 recent name portscan recent rcheck-sec 86400<br>• ip filter chain input rule append tail target none dup-delete in-intf mgmt0 recent name portscan recent remove<br>• ip filter chain input rule append tail target none dup-delete dest-port 22 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ip filter chain input rule append tail target drop dup-delete dest-port 22 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 50<br>• ip filter chain input rule append tail target none dup-delete dest-port 23 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ip filter chain input rule append tail target drop dup-delete dest-port 23 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 50<br>• ip filter chain input rule append tail target none dup-delete dest-port 443 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ip filter chain input rule append tail target drop dup-delete dest-port 443 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 150<br>• ip filter chain input rule append tail target none dup-delete dest-port 80 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ip filter chain input rule append tail target drop dup-delete dest-port 80 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 150<br>• ip filter chain input rule append tail target none dup-delete dest-port 23108 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ip filter chain input rule append tail target drop dup-delete dest-port 23108 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 150<br>• ip filter chain input rule append tail target none dup-delete dest-port 161 in-intf mgmt0 protocol udp conntrack new recent set<br>• ip filter chain input rule append tail target drop dup-delete dest-port 161 in-intf mgmt0 protocol udp conntrack new recent update-sec 60 recent hitcount 100<br>• ip filter chain input rule append tail target accept dup-delete dest-port 22 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 23 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 443 in-intf mgmt0 protocol tcp conntrack new,established |

| Prerouting-Mangle Chain Rules |
| --- |
| • ip filter chain input rule append tail target accept dup-delete dest-port 80 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 23108 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 179 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 68 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 122 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 161 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 6306 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 69 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 389 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 389 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 1812-1813 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 49 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 49 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete source-port 53 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete source-port 53 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 500 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 4500 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 1293 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 1293 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 1707 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 1707 in-intf mgmt0 protocol tcp conntrack new,established |

| Prerouting-Mangle Chain Rules |
| --- |
| • ip filter chain input rule append tail target accept dup-delete dest-port 3786 in-intf lo protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 33000 in-intf lo protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol icmp<br>• ip filter chain input rule append tail target accept dup-delete source-port 5353 dest-port 5353 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target reject-with icmp-port-unreachable dup-delete dest-port 33434-33523 in-intf mgmt0 protocol udp<br>• ip filter chain input rule append tail target accept dup-delete dest-port 123 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 514 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete dest-port 67 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dup-delete comment "Feature HA port" dest-port 60102 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target accept dest-port 636 in-intf mgmt0 protocol udp conntrack new,established<br>• ip filter chain input rule append tail target accept dest-port 636 in-intf mgmt0 protocol tcp conntrack new,established<br>• ip filter chain input rule append tail target logging dup-delete in-intf mgmt0 |
| Output Chain Rules |
| • ip filter chain output rule append tail target drop out-intf mgmt0 state invalid<br>• ip filter chain output rule append tail target accept out-intf mgmt0 |
| Logging Chain Rules |
| • ip filter chain logging rule append tail target nflog in-intf mgmt0 rate-limit 1/minute logging-options prefix "IPTables-Dropped-<Domain>: " logging-options group 3<br>• ip filter chain logging rule append tail target drop in-intf mgmt0 |

## IPv6 Firewall Default Rules

| Prerouting-Mangle Chain Rules |
| --- |
| • ipv6 filter chain prerouting-mangle rule append tail target drop dup-delete not-dest-port 22-23 in-intf mgmt0 protocol tcp conntrack new tcp-op-mss mss-not-in-range 1280:65535 |
| Input Chain Rules |
| • ipv6 filter chain input rule append tail target accept dup-delete in-intf lo<br>• ipv6 filter chain input rule append tail target drop dup-delete dest-addr ::1 /128 in-intf mgmt0<br>• ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 state established,related<br>• ipv6 filter chain input rule append tail target drop dup-delete not-dest-port 22-23 in-intf mgmt0 protocol tcp state new tcp-op syn match-not-syn<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 fragment enable<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp tcp-op flags all<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp tcp-op flags none<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 state invalid<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp tcp-op flags reset rate-limit-above 2/second burst-limit-above 2<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp state new rate-limit-above 50/second burst-limit-above 50<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 protocol tcp conntrack new rate-limit-above 60/second burst-limit-above 20<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 recent name portscan recent rcheck-sec 86400<br>• ipv6 filter chain input rule append tail target none dup-delete in-intf mgmt0 recent name portscan recent remove<br>• ipv6 filter chain input rule append tail target none dup-delete dest-port 22 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ipv6 filter chain input rule append tail target drop dup-delete dest-port 22 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 50<br>• ipv6 filter chain input rule append tail target none dup-delete dest-port 23 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ipv6 filter chain input rule append tail target drop dup-delete dest-port 23 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 50<br>• ipv6 filter chain input rule append tail target none dup-delete dest-port 443 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ipv6 filter chain input rule append tail target drop dup-delete dest-port 443 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 150 |

| Prerouting-Mangle Chain Rules |
| --- |
| • ipv6 filter chain input rule append tail target none dup-delete dest-port 80 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ipv6 filter chain input rule append tail target drop dup-delete dest-port 80 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 150<br>• ipv6 filter chain input rule append tail target none dup-delete dest-port 23108 in-intf mgmt0 protocol tcp conntrack new recent set<br>• ipv6 filter chain input rule append tail target drop dup-delete dest-port 23108 in-intf mgmt0 protocol tcp conntrack new recent update-sec 60 recent hitcount 150<br>• ipv6 filter chain input rule append tail target none dup-delete dest-port 161 in-intf mgmt0 protocol udp conntrack new recent set<br>• ipv6 filter chain input rule append tail target drop dup-delete dest-port 161 in-intf mgmt0 protocol udp conntrack new recent update-sec 60 recent hitcount 100<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 routing-header-type 0<br>• ipv6 filter chain input rule append tail target drop dup-delete in-intf mgmt0 hop-by-hop-header enable<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 22 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 23 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 443 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 80 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 23108 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 179 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 547 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 122 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 161 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 6306 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 69 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 389 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 389 in-intf mgmt0 protocol tcp conntrack new,established |

| Prerouting-Mangle Chain Rules |
| --- |
| • ipv6 filter chain input rule append tail target accept dup-delete dest-port 1812-1813 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 49 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 49 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete source-port 53 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete source-port 53 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 500 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 4500 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 1293 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 1293 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 1707 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 1707 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 3786 in-intf lo protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 33000 in-intf lo protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete source-port 5353 dest-port 5353 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target reject-with icmp6-port-unreachable dup-delete dest-port 33434-33523 in-intf mgmt0 protocol udp<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 123 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 514 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 546 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete comment "Feature HA port" dest-port 60102 in-intf mgmt0 protocol tcp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 636 in-intf mgmt0 protocol udp conntrack new,established<br>• ipv6 filter chain input rule append tail target accept dup-delete dest-port 636 in-intf mgmt0 protocol tcp conntrack new,established |

| Prerouting-Mangle Chain Rules |
| --- |
| • ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol-icmp-type destination-unreachable<br>• ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol-icmp-type packet-too-big<br>• ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol-icmp-type time-exceeded<br>• ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol-icmp-type parameter-problem<br>• ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol-icmp-type echo-request<br>• ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol-icmp-type echo-reply<br>• ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol-icmp-type router-advertisement<br>• ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol-icmp-type neighbor-solicitation<br>• ipv6 filter chain input rule append tail target accept dup-delete in-intf mgmt0 protocol-icmp-type neighbor-advertisement<br>• ipv6 filter chain input rule append tail target logging dup-delete in-intf mgmt0 |
| Output Chain Rules |
| • ipv6 filter chain output rule append tail target accept dup-delete out-intf mgmt0 |
| Logging Chain Rules |
| • ipv6 filter chain logging rule append tail target nflog dup-delete in-intf mgmt0 logging-options prefix IP6Tables-Dropped: logging-options group 3<br>• ipv6 filter chain logging rule append tail target drop dup-delete in-intf mgmt0 |

# Control Plane Policing Commands

# ip filter enable | ipv6 filter enable

| | |
| --- | --- |
| | {ip \| ipv6} filter enable<br>no {ip \| ipv6} filter enable<br>Enables IP filtering.<br>The no form of the command disables IP filtering. |

| | |
|---|---|
| Syntax Description | N/A |
| Default | ip Enabled<br>ip6 Disabled |
| Configuration Mode | config |
| History | 3.5.1000<br>3.10.3000 IP Filter is enabled by default |
| Example | switch (config) # ip filter enable |
| Related Commands | |
| Notes | It is recommended to run this command only after configuring all of the IP table filter parameters. |

# ip filter chain policy | ipv6 filter chain policy

| | | |
|---|---|---|
| | {ip \| ipv6} filter chain <chain_name> policy {accept \| drop}<br>no {ip \| ipv6} filter chain <chain_name> policy<br>Configures default policy for a specific chain (if no rule matches this default policy action shall apply).<br>The no form of the command resets default policy for a specific chain. | |
| Syntax Description | chain_name | Selects a chain for which to add or modify a filter:<br>• input – input chain or ingress interfaces<br>• output – output chain or egress interfaces |
| | accept | Accepts all traffic by default for this chain |
| | drop | Drops all traffic by default for this chain |
| Default | Accept for input and output chains | |
| Configuration Mode | config | |
| History | 3.5.1000 | |
| Example | switch (config) # ipv6 filter chain input policy accept | |

| | |
|---|---|
| Related Commands | |
| Notes | |

# ip filter chain rule target | ipv6 filter chain rule target

| | | |
|---|---|---|
| | no {ip \| ipv6} filter chain <chain_name> rule {<number> \| all}<br>Inserts rule before specified rule number.<br>The no form of the command deletes rule for a specific chain. | |
| Syntax Description | chain_name | A chain to which to add or modify a filter:<br>• input – input chain or ingress interfaces<br>• output – output chain or egress interfaces |
| | rule | • append tail – appends operation to the bottom of operation list<br>• insert <oper_num> – inserts operation at specified position (existing operation at that position moves back in the list)<br>• modify <oper_num> – modifies existing operation at specified position. Only the parameters specified in this invocation are altered; everything else is left untouched.<br>• move <oper_num1> to <oper_num2> – moves one operation to another place in the operation list<br>• set <oper_num> – sets operation at specified position (overwrites existing) |
| | target | • accept – allows the packets that match the rule into the management plane<br>• drop – drops packets that match the rule<br>• rate-limit – allows with rate limiting in packets per sec (PPS)<br>• reject-with – drops the packet and replies with an ICMP error message |
| | param | • rate-limit /[second \| minute \| hour] - matches is traffic is less than the set limit<br>• rate-limit-above /[second \| minute \| hour] - matches is traffic is more than the set limit<br>• burst-limit - Maximum initial number of packets to match when setting rate-limit. The default is 5. |

| | | |
|---|---|---|
| | | • burst-limit-above - Maximum initial number of packets to match when setting rate-limit-above. The default is 5.<br>• comment <text> – specifies description string for this rule (60 chars max)<br>• dest-addr <ip> – IP matching a specific destination address or address range. A specific IPv4 address can be provided or an entire subnet by giving an address along with netmask in dot notation or as a CIDR notation (e.g. /24).<br>• not-dest-addr <ip> – IP not matching a specific destination address range<br>• dest-port <port(s)> – matching a specific destination port or port range<br>• not-dest-port <port(s)> – port not matching a specific destination port or port range<br>• dup-delete – deletes any preexisting duplicates of this rule<br>• in-intf – interface matching a specific inbound interface<br>• not-in-intf <if_name> – interface not matching a specific inbound interface<br>• out-intf <if_name> – matches a specific outbound interface<br>• not-out-intf <if_name> – interface not matching a specific outbound interface |
| | param4 (cont.) | • protocol <if_name> – matches a specific protocol<br>  ◦ tcp<br>  ◦ udp<br>  ◦ icmp<br>  ◦ all<br>• not-protocol <protocol> – does not match a specific protocol<br>  ◦ tcp<br>  ◦ udp<br>  ◦ icmp<br>  ◦ all<br>• source-addr <ip> – matches a specific source address range<br>• not-source-addr <ip> – does not match a specific source address range<br>• source-port <port(s)> – matches a specific source port or port range<br>• not-source-port <port(s)> – does not match a specific source port or port range |

| | | |
|---|---|---|
| | | • state – matches packets in a particular state. Possible values:<br>◦ established – packet associated with an established connection which has seen traffic in both directions<br>◦ related – packet that starts a new connection but is related to an existing connection<br>◦ new – packet that starts a new, unrelated connection<br>◦ A combination can be entered separated by commas |
| | param (cont.) | • routing-header-type <type> – matches IPv6 routing header type. (only supported for ipv6)<br>• hop-by-hop-header enable - matches IPv6 packet with hop by hop header. (only supported for ipv6) |
| Default | N/A | |
| Configuration Mode | config | |
| History | 3.5.1000 | |
| Example | switch (config) # ipv6 filter enable chain input rule append tail target drop state related protocol all dup-delete | |
| Related Commands | | |
| Notes | • The source and destination ports may each be either a single number, or a range specified as “<low>-<high>”. For example: “10-20” would specify ports 10 through 20 (inclusive).<br>• The port parameter only works in conjunction with TCP and UDP<br>• Setting a “positive” rule removes any corresponding “not-” rules, and vice-versa<br>• The “state” parameter is a classification of the packet relative to existing connections<br>• If TCP or UDP are selected for the “protocol” parameter, source and/or destination ports may be specified. If ICMP is selected, these options are either ignored, or an error is produced. | |

# ip filter options include-bridges

| | |
|---|---|
| | {ip \| ipv6} filter options include-bridges<br>no {ip \| ipv6} filter options include-bridges<br>Applies IP filters to bridges |
| Syntax Description | N/A |
| Default | Disabled |
| Configuration Mode | config |
| History | 3.5.1000 |
| Example | switch (config) # ip filter options include-bridges |
| Related Commands | |
| Notes | |

## ip filter reset-to-default-rules | ipv6 filter reset-to-default-rules

| | |
|---|---|
| | {ip \| ipv6} filter reset-to-default-rules<br>Deletes all configured IP filter rules and add the default rules defined in the user manual under section "IP Table Filtering Default Rules", above. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 3.10.3000<br>3.11.4002: Added support for support IPv6 |
| Example | switch (config) # ip filter reset-to-default-rules<br>switch (config) # ipv6 filter reset-to-default-rules |
| Related Commands | |
| Notes | |

# show ip filter

| | show ip filter<br>Displays IPv4 filtering state. |
|---|---|
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 3.6.6000 |
| Example | switch (config) # show ip filter<br>Packet filtering for IPv4: enabled<br>Active IPv4 filtering rules (omitting any not from configuration):<br>  Chain 'input' Policy 'accept':<br>  Rule 1:<br>  Target : accept<br>  Protocol : all<br>  Source : all<br>  Destination : 1.1.1.0/24<br>  Interface : all<br>  State : any<br>  Other Filter: -<br>Chain 'output' Policy 'accept':<br>  Rule 1:<br>  Target : reject-with icmp-net-unreachable<br>  Protocol : tcp<br>  Source : all<br>  Destination : all<br>  Interface : all<br>  State : any<br>  Other Filter: dest-port 1000 |
| Related Commands | |
| Notes | |

# show ip filter all

| | show ip filter all<br>Displays IPv4 filtering state (including un-configured rules). |
|---|---|
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 3.6.6000 |
| Example | switch (config) # show ip filter all<br>Destination : 1.1.1.0/24<br>Interface : all<br>State : any<br>Other Filter: -<br>Chain 'output' Policy 'accept':<br>Rule 1:<br>Target : reject-with icmp-net-unreachable<br>Protocol : tcp<br>Source : all<br>Destination : all<br>Interface : all<br>State : any<br>Other Filter: dest-port 1000 |
| Related Commands | |
| Notes | |

# show ip filter configured

| | show ip filter configured<br>Displays IPv4 filtering configuration. |
|---|---|
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 3.6.6000 |

| | |
|---|---|
| Example | switch (config) # show ip filter configured<br>Packet filtering for IPv4: enabled<br>IPv4 configuration:<br>  Chain 'input' Policy 'accept':<br>  Rule 1:<br>  Target  : accept<br>  Protocol  : all<br>  Source  : all<br>  Destination : 1.1.1.0/24<br>  Interface  : all<br>  State  : any<br>  Other Filter:  -<br>  Chain 'output' Policy 'accept':<br>  Rule 1:<br>  Target  : reject-with icmp-net-unreachable<br>  Protocol  : tcp<br>  Source  : all<br>  Destination : all<br>  Interface  : all<br>  State  : any<br>  Other Filter: dest-port 1000 |
| Related Commands | |
| Notes | |

# show ipv6 filter

| | show ipv6 filter<br>Displays IPv6 filtering state. |
|---|---|
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 3.6.6000 |
| Example | switch (config) # show ipv6 filter<br>Packet filtering for IPv6: enables<br>Active IPv6 filtering rules (omitting any not from configuration):<br>  Chain 'input' Policy 'accept':<br>  Rule 1:<br>  Target  : accept |

| | |
|---|---|
| | Protocol : all<br>Source : all<br>Destination : 1.1.1.0/24<br>Interface : all<br>State : any<br>Other Filter: -<br>Chain 'output' Policy 'accept':<br>Rule 1:<br>Target : reject-with icmp-net-unreachable<br>Protocol : tcp<br>Source : all<br>Destination : all<br>Interface : all<br>State : any<br>Other Filter: dest-port 1000 |
| Related Commands | |
| Notes | |

# show ipv6 filter all

| | show ipv6 filter all<br>Displays IPv6 filtering state (including un-configured rules). |
|---|---|
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 3.6.6000 |
| Example | switch (config) # show ipv6 filter all<br>Packet filtering for IPv6: enables<br>All active IPv6 filtering rules:<br>Chain 'input' Policy 'accept':<br>Rule 1:<br>Target : accept<br>Protocol : all<br>Source : all<br>Destination : 1.1.1.0/24<br>Interface : all<br>State : any<br>Other Filter: -<br>Chain 'output' Policy 'accept': |

| | |
|---|---|
| | Rule 1:<br>Target : reject-with icmp-net-unreachable<br>Protocol : tcp<br>Source : all<br>Destination : all<br>Interface : all<br>State : any<br>Other Filter: dest-port 1000 |
| Related Commands | |
| Notes | |

# show ipv6 filter configured

| | show ipv6 filter configured<br>Displays IPv6 filtering configuration. |
|---|---|
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 3.6.6000 |
| Example | switch (config) # show ipv6 filter configured<br>Packet filtering for IPv6: enables<br>IPv6 configuration:<br>Chain 'input' Policy 'accept':<br>Rule 1:<br>Target : accept<br>Protocol : all<br>Source : all<br>Destination : 1.1.1.0/24<br>Interface : all<br>State : any<br>Other Filter: -<br>Chain 'output' Policy 'accept':<br>Rule 1:<br>Target : reject-with icmp-net-unreachable<br>Protocol : tcp<br>Source : all<br>Destination : all<br>Interface : all<br>State : any |

| | |
|---|---|
| | Other Filter: dest-port 1000 |
| Related Commands | |
| Notes | |

**Notice**

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation (“NVIDIA”) makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer (“Terms of Sale”). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer’s own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer’s sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer’s product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, “MATERIALS”) ARE BEING PROVIDED “AS IS.” NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF

ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

**Trademarks**

NVIDIA and the NVIDIA logo are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.