Chapter 8

Policy Resources

This chapter provides information about configuring policy resources. The chapter discusses the following topics:

Policy Resources Overview

The maximum number of policies that you can attach to interfaces on an E-series router depends on the classifier entries that make up the policy and the number of attachment resources available on the interface. JUNOSe software allocates interface attachment resources when you attach policies to interfaces. See *Interface Attachment Resources Overview* on page 153 for information about attachment resources.

An E-series router supports software and hardware classifiers. A policy can be made up of any combination of software and hardware classifiers. You use the **classifier-list** command to configure all classifiers.

There are two categories of hardware classifiers, depending on the type of line module being used. OC48/STM16, GE-2, and GE-HDE line modules support content-addressable memory (CAM) hardware classifiers—all other line modules support FPGA hardware classifiers. Table 13 lists the classifiers supported on OC48/STM16, GE-2, and GE-HDE line modules; Table 14 lists the classifiers supported on all other line modules.

Table 13: Classifier Support (OC48/STM16, GE-2, and GE-HDE Line Modules)

Interface Type	Hardware Classifier	Software Classifier
All interface types (except IP and IPv6)	–	■ Color ■ Traffic class ■ User packet class
Frame Relay	Not supported	■ DE bit
GRE tunnels	Not supported	■ ToS
IP	■ Color ■ Destination address ■ Destination port ■ Destination route class ■ ICMP type and code ■ IGMP type ■ IP flags ■ IP fragmentation ■ Local ■ Protocol ■ Source address ■ Source port ■ Source route class ■ TCP flags ■ ToS ■ Traffic class ■ User packet class	Not supported

Table 13: Classifier Support (OC48/STM16, GE-2, and GE-HDE Line Modules)

Interface Type	Hardware Classifier	Software Classifier
IPv6	■ Color ■ Destination address ■ Destination port ■ Destination route class ■ ICMPv6 type and code ■ Local ■ Protocol ■ Source address ■ Source port ■ Source route class ■ TC flags ■ TCP flags ■ Traffic class ■ User packet class	Not supported
MPLS	Not supported	■ EXP
VLAN	Not supported	■ User priority

Table 14: Classifier Support (All Line Modules Except OC48/STM16, GE-2, and GE-HDE)

Interface Type	Hardware Classifier	Software Classifier
All interface types	–	■ Color ■ Traffic class ■ User packet class
Frame Relay	Not supported	■ DE bit
GRE tunnels	Not supported	■ ToS
IP	■ Destination address ■ Destination port ■ ICMP type and code ■ IGMP type ■ Protocol ■ Source address ■ Source port	■ Destination route class ■ IP flags ■ IP fragmentation ■ Local ■ Source route class ■ TCP flags ■ ToS
IPv6	■ Destination address ■ Destination port ■ ICMPv6 type and code ■ Protocol ■ Source address ■ Source port	■ Destination route class ■ Local ■ Source route class ■ TC field ■ TCP flags
MPLS	Not supported	■ EXP
VLAN	Not supported	■ User priority

FPGA Hardware Classifiers

Classification is the process of taking a single data stream in and sorting it into multiple output substreams. The classifier engine on an E-series router is a combination of PowerPC processors, working with an FPGA for a hardware assist.

In the Differentiated Services (DiffServ) architecture, two basic types of classifiers exist. The first classifier type is a multifield (MF) classifier. The MF classifier can examine multiple fields in the IP datagram header to determine the service class to which a packet belongs.

FPGA hardware classifiers are supported on all line modules except the OC48/STM16, GE-2, and GE-HDE line modules. Table 14 lists the FPGA classifiers and software classifiers supported for each interface type.

An E-series router supports two versions of policies that are based on FPGA hardware classifiers. One version has a maximum of 16 classifier entries per policy, and the second version has 17 to 32 classifier entries per policy. The line module supports 16,255 policies when all policies have 16 hardware classifier entries or fewer, and supports 8127 policies when all policies have 17 to 32 hardware classifier entries.

You can configure a combination of the two versions of FPGA hardware classifier-based policies—you can have some that contain 16 or fewer classifier entries and others with more than 16 entries. In this case, between 8127 and 16,255 policies are supported, depending on the actual configuration.

You can also configure hardware classifier-based policies that have more than 32 classifier entries. The router groups the classifiers into blocks of 32. For example, if you configure a policy with 100 classifier entries, the router groups these as 3 policies that have 32 classifier entries and 1 policy with 4 classifier entries. The group with 4 classifier entries actually consumes 16 classifier resources, which is the minimum number consumed for a group in a mixed-mode hardware classifier configuration.

Unlike policies that are based on software classifiers, policies that are based on FPGA hardware classifiers consume resources at a rate of one resource per policy, regardless of the number of different hardware classifier categories in the policy. For example, if a classifier list has three hardware classifiers, such as destination address, source address, and protocol, the policy referencing that classifier list consumes only a single hardware classifier resource.

The same is true when multiple policy rules reference the classifier list. For example, if four policy rules reference the same classifier list (which contains three hardware classifiers), then still only one classifier entry is consumed.

CAM Hardware Classifiers Overview

Content-addressable memory (CAM) hardware classifiers are supported on the OC48/STM16, GE-2, and GE-HDE line modules. Table 13 on page 142 lists CAM hardware classifiers and the software classifiers supported for each interface type.

The OC48/STM16 line module supports 128,000 CAM entries, and the GE-2 and GE-HDE line modules support 64,000 CAM entries. For most configurations, each classifier entry in a policy consumes one CAM entry. However, a policy that has only the default classifier consumes no CAM resources.

In this example, the policy consumes a total of four CAM entries: two entries for clacl1, one for clacl2, and one for the default classifier.

```
host1(config)#ip classifier-list clacl1 ip host 192.168.1.1 host 192.168.2.2 tos 1
host1(config)#ip classifier-list clacl1 ip host 192.168.1.1 host 192.168.2.2 tos 2
host1(config)#ip classifier-list clacl2 tcp any any tcp-flags "SYN"
host1(config)#ip policy-list policy1
host1(config-policy-list)#classifier-group clacl1
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group clacl2
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group *
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
host1(config)#
```

A single classifier entry consumes more than one CAM entry when:

- A classifier entry contains a port range. For example:

  ```
  host1(config)#ip classifier-list clacl3 tcp any any range 5 8
  ```

- A classifier entry contains the **not** keyword. Although this keyword is supported for IP classifier lists, we recommend that you not use it—you can usually achieve the desired behavior without this keyword.

  ```
  host1(config)#ip classifier-list clacl4 ip not host 1.1.1.1 any
  ```

In these cases, the actual number of entries that are consumed depends on the configuration.

Size Limit for IP and IPv6 CAM Hardware Classifiers

The maximum width of a CAM hardware classifier entry for IP or IPv6 in a single policy is 128 bits.

Some independent classifiers share the same classifier entry location, while others are combined together to form a larger classifier field. However, you cannot configure any combination of classifiers that exceeds the total classifier entry size of 128 bits.

IP Classifiers and Size Limits

Table 15 lists all IP classifiers and the size limit of each classifier entry.

Table 15: Size Limit of Individual IP Classifiers

IP Classifier	Size Limit (Bits)
Color	2
Destination address	32
Destination port	16
Destination route class	8
ICMP type	8
ICMP code	8
IGMP type	8
IP flags	3
IP fragmentation	2
Local	1
Protocol	8
Source address	32
Source port	16
Source route class	8
TCP flags	6
ToS	8
Traffic class	3
User packet class	4

Table 16 lists the IP classifiers that share the same classifier entry location and those that are combined to form a larger classifier field. The table also lists the rules that apply to these types of classifier combinations.

The format in the classifier entry combinations in Table 16 is based on the conventions for CLI commands, except that the pipe symbol (|) represents a choice of one or both options to the left and right of the pipe symbol.

Table 16: Size Limit of Combined IP Classifiers

IP Classifier Entry Combination	Size Limit (Bits)	Rule
Color or TCP flags or both	8	When you specify one or both of the color and TCP flags classifiers, 8 bits are added to the total classifier entry size.
Destination address	32	–
Destination address route class	8	–
[Destination port] and [[ICMP type] | [ICMP code] | [IGMP type] or nil]	16	The ICMP type, ICMP code, IGMP type, and destination port classifiers share the same classifier field location. When you specify the destination port classifier, 16 bits are added to the total classifier entry size. If you also specify the ICMP type, ICMP code, and IGMP type classifier, no additional bits are added.
[IP flags] | [IP fragmentation] | [Traffic class]	8	When you specify one or more of the IP flags, traffic class, and IP fragmentation classifiers, 8 bits are added to the total classifier entry size.
Protocol	8	–
[Source port] and [[ICMP type] | [ICMP code] | [IGMP type]]	16	The ICMP type, ICMP code, IGMP type, and source port classifiers share the same classifier field location. When you specify the source port classifier, 16 bits are added to the total classifier entry size. When you also specify the ICMP type, ICMP code, and IGMP type classifiers, no additional bits are added.
Source address	32	–
[not Source port] and [not Destination port] and [[ICMP type] | [ICMP code] | [IGMP type]]	16	When you do not specify the source port and destination port classifiers, but you specify one or more of ICMP type, ICMP code, and IGMP type, 16 bits are added to the total classifier entry size. ICMP type, ICMP code, and IGMP type require 16 bits even if the source port and destination port classifications are not configured.
ToS	8	–
User packet class or local or both	8	When you specify one or both of the user packet class and local classifiers, 8 bits are added to the total classifier entry size.

IPv6 Classifiers and Size Limits

Table 17 lists all IPv6 and the size limit of each classifier entry.

Table 17: Size Limit of Individual IPv6 Classifiers

IPv6 Classifier Entry	Size Limit (Bits)
Color	2
Destination address	128
Destination port	16
Destination route class	8
ICMPv6 type	8
ICMPv6 code	8
Local	1
Protocol	8
Source address	128
Source port	16
Source route class	8
TC field	8
TCP Flags	6
Traffic class	3
User packet class	4

Table 18 lists the IPv6 classifiers that share the same classifier entry location and those that are combined to form a larger classifier field. The table also lists the rules that apply to these types of classifier combinations.

The format in the classifier entry combinations in Table 18 is based on the conventions for CLI commands, except that the pipe symbol (|) represents a choice of one or both options to the left and right of the pipe symbol.

Table 18: Size Limit of Combined IPv6 Classifiers

IPv6 Classifier Entry Combination	Size Limit (Bits)	Rule
Color or TCP flags or both	8	When you specify the color and/or TCP flags classifiers, 8 bits are added to the total classifier entry size.
Destination address (first word)	32	–
Destination address (second word)	32	–
Destination address (third word)	32	–
Destination address (fourth word)	32	–
Destination address route class	8	–

Table 18: Size Limit of Combined IPv6 Classifiers (continued)

IPv6 Classifier Entry Combination	Size Limit (Bits)	Rule
[Destination port] and [[ICMPv6 type] | [ICMPv6 code or nil]]	16	When you specify the destination port classifier, 16 bits are added to the total classifier entry size. If you also specify the ICMPv6 type and ICMPv6 code classifiers, no additional bits are added to the total classifier entry size.
[No source port] and [no destination port] and [[ICMPv6 type] | [ICMPv6 code]]	16	When you do not specify the source port and destination port classifiers, and you have already specified one or more of the ICMPv6 Type and ICMPv6 code classifiers, 16 bits are added to the total classifier entry size. The ICMPv6 type and ICMPv6 code classifiers require 16 bits even if you have not specified the source port and destination port classifiers.
Protocol	8	–
Source address (first word)	32	–
Source address (second word)	32	–
Source address (third word)	32	–
Source address (fourth word)	32	–
Source address route class	8	–
[source port] and [[ICMPv6 type] | [ICMPv6 code]]	16	When you specify the source port classifier, 16 bits are added to the total classifier entry size. If you also specify the ICMPv6 type and ICMPv6 code classifiers, no additional bits are added.
TC field	8	–
[User packet class] | [traffic class] | [local]	8	When you specify one or more of the user packet class, traffic class, and local classifiers, 8 bits are added to the total classifier entry size.

Creating and Attaching a Policy with IP Classifiers

In this example, a policy with a combination of IP classifiers is created and attached. The configuration conforms to the 128 bit limit.

1. Match all TCP SYN packets from 1.1.1.1 to any DA with port 2000.

   host1(config)#**ip classifier-list tcpCLACL tcp host 1.1.1.1 any eq 2000 tcp-flags "SYN"**

2. Match all IP packets with the don't fragment flag set to host 2.2.2.2.

   host1(config)#**ip classifier-list ipCLACL ip any host 2.2.2.2 ip-flags "dont-fragment"**

3. Match all ICMP echo packets.

   host1(config)#**ip classifier-list icmpCLACL icmp any any 8 0**

4. Match all frames with the color red.

```
host1(config)#ip classifier-list colorCLACL color red ip any any
```

5. Create a policy list.

```
host1(config)#ip policy-list ipPol
host1(config-policy-list)#classifier-group colorCLACL
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#classifier-group tcpCLACL
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#classifier-group icmpCLACL
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#classifier-group ipCLACL
host1(config-policy-list-classifier-group)#filter
```

6. Apply the policy list to an interface.

```
host1(config)#interface atm 5/0.1
host1(config-if)#ip policy input ipPol
```

Table 19 lists the active classifiers in the policy named ipPol and the size of each classifier.

Table 19: Classification Fields for Example 1

Classifiers	Size (Bits)
Source address	32
Destination address	32
Destination port, ICMP type, ICMP code	16
Protocol	8
Color and TCP flags	8
TOS	8
IP flags	8

The total value of the classifiers requested in the ipPol policy is 112, which is less than 128 bit CAM entry size limit.

In this example, a policy with a combination of IP classifiers is created and attached. The configuration exceeds the 128 bit limit.

1. Match all TCP packets from 1.1.1.1 port 10 to 2.2.2.2 port 20.

```
host1(config)#ip classifier-list tcpCLACL tcp host 1.1.1.1 eq 10 host 2.2.2.2 eq
20
```

2. Match all IP fragmentation offset equal to 1.

```
host1(config)#ip classifier-list ipFragCLACL ip any any ip-frag-offset eq 1
```

3. Match all frames with the color red.

```
host1(config)#ip classifier-list colorCLACL color red traffic-class best-effort ip any
any
```

4. Match all frames with UPC 1.

```
host1(config)#ip classifier-group upcCLACL user-packet-class 1 ip any any
```

5. Create a policy list.

```
host1(config)#ip policy-list ipPol
host1(config-policy-list)#classifier-group colorCLACL
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#classifier-group ipFragCLACL
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#classifier-group igmpCLACL
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#classifier-group lowDelayCLACL
host1(config-policy-list-classifier-group)#traffic-class strict-priority
host1(config-policy-list-classifier-group)#classifier-group tcpCLACL
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#classifier-group *
host1(config-policy-list-classifier-group)#filter
```

6. Apply the policy list to an interface.

```
host1(config)#interface atm 5/0.1
host1(config-if)#ip policy input ipPol
% too many classifier fields in policy
```

Table 20 lists the active classifiers in the policy named ipPol and the size of each classifier.

Table 20: Classification Fields for Example 2

Classifiers	Size (Bits)
Source address	32
Source port	16
Destination port	16
Protocol	8
User packet class	8
Color	8
IP fragmentation	8
ToS	8

The configuration fails because the total value of the classifiers requested in the ipPol policy is 136, which is greater than 128 bit CAM entry size limit.

Software Classifiers Overview

An E-series router supports a variety of software classifiers, depending on the type of interface. Table 13 on page 142 and Table 14 on page 143 list the supported software classifiers for each interface type.

A line module supports 16,383 software classifiers. Software classifiers are consumed at a rate of one resource per classifier category per policy. For example, if you configure a policy that has three different destination route class rules, then because all three rules are for the same classifier category, that policy consumes only one software classifier resource. However, if you configure a policy that requires classification on three different classifier categories, such as ToS, color, and TCP flags, then that policy consumes three of the available 16,383 software classifier resources.

NOTE: Policy consumption is per policy definition per line module.

In this example, the policy list named polWestford5 references four classifier lists with a combination of software and hardware classifiers.

```
host1(config)#ip classifier-list clacl100 color red ip any any
host1(config)#ip classifier-list clacl200 color yellow user-packet-class 6 ip host
10.1.1.1 host 10.1.1.2
host1(config)#ip classifier-list clacl300 color green user-packet-class 5 ip any any
host1(config)#ip classifier-list clacl400 color red ip host 10.1.1.10 any
host1(config)#ip policy-list polWestford5
host1(config-policy-list)#classifier-group clacl100
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group clacl200
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group clacl300
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group clacl400
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group *
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
```

For a given line module, the policy list named polWestford5 consumes a total of one FPGA hardware classifier resource and two software classifier resources, as indicated in Table 21.

Table 21: Resource Consumption

Number of Resources Consumed	Classifier Category
1 hardware	■ Protocol ■ Destination address ■ Source address
1 software	Color
1 software	User-packet-class

Interface Attachment Resources Overview

JUNOSe software allocates interface attachment resources when policies are attached to interfaces—when you attach a policy to an interface, the policy consumes one of the interface's attachment resources. Each interface has two attachment resource pools. IP and IPv6 policy attachments are allocated from the interface's IP attachment resource pool; all other attachments are allocated from the interface's layer 2 attachment resource pool.

- The type of line module determines the number of policies attachments supported by interfaces. See *ERX Module Guide, Appendix A, Module Protocol Support* for more information about supported line modules. See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support BGP.
- On ASIC-based line modules (OC48/STM16, GE-2, and GE-HDE line modules), you can have a maximum of 8191 IP policy attachments and 8191 layer 2 policy attachments for ingress policies per forwarding controller, and 8191 IP policy attachments and 8191 layer 2 policy attachments for egress policies per forwarding controller.
- On FPGA-based line modules, you can have a maximum of 8191 IP policy attachments and 8191 layer 2 policy attachments per forwarding controller.

CAM Hardware Classifiers and Interface Attachment Resources

CAM hardware classifiers are supported on OC48/STM16, GE-2, and GE-HDE ASIC-based line modules. Policies that use CAM hardware classifiers consume one interface attachment resource, regardless of the number of classifier entries in a policy.

Range Vector Hardware Classifiers and Interface Attachment Resources

Range vector classifiers, which include all software classifiers and FPGA-based hardware classifiers, consume one interface attachment resource for every 32 classifier entries in a policy.

The following examples illustrate how JUNOSe software allocates interface attachment resources. These examples apply to software and FPGA-based hardware policies:

- A policy with 0 classifier entries consumes 1 interface attachment resource.
- A policy with 1–32 classifier entries consumes 1 interface attachment resource.
- A policy with 33–64 classifier entries consumes 2 interface attachment resources.
- A policy with 65–96 classifier entries consumes 3 interface attachment resources.
- A policy with 487–512 classifier entries consumes 16 interface attachment resources.