JUNIPER NETWORKS

JunosE™ Software for E Series™ Broadband Services Routers

Policy Resources Management

Release
16.1.x

Modified: 2015-08-04

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

JunosE™ Software for E Series™ Broadband Services Routers Policy Resources Management
Release 16.1.x

Revision History
August 2015—FRS JunosE 16.1.x

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About the Documentation

E Series and JunosE Documentation and Release Notes

For a list of related JunosE documentation, see http://www.juniper.net/techpubs/software/index.html.

If the information in the latest release notes differs from the information in the documentation, follow the *JunosE Release Notes.*

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JunosE Text and Syntax Conventions

Table 1 on page viii defines notice icons used in this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page viii defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	• Issue the **clock source** command. • Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	**host1(config)#traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	**host1#show ip ospf 2**
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	• Emphasizes words. • Identifies variables. • Identifies chapter, appendix, and book names.	• There are two levels of access: *user* and *privileged*. • *clusterId, ipAddress.* • *Appendix A, System Specifications*
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*
| (pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic | line
[ ] (brackets)	Represent optional keywords or variables.	[internal | external]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Juniper Networks TechLibrary at http://www.juniper.net/techpubs/.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

http://www.juniper.net/techpubs/resources/index.html

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks website at http://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Policy Resources

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 21 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, GE-HDE, ES2 4G, ES2 10G, and ES2 10G Uplink line modules support content-addressable memory (CAM) hardware classifiers—all other line modules support FPGA hardware classifiers. Table 3 on page 4 lists the classifiers supported on OC48/STM16, GE-2, GE-HDE, ES2 4G, ES2 10G, and ES2 10G Uplink line modules; Table 4 on page 5 lists the classifiers supported on all other line modules.

Table 3: Classifier Support (OC48/STM16, GE-2, GE-HDE, ES2 4G, ES2 10G, and ES2 10G Uplink 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
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 4: Classifier Support (All Line Modules Except OC48/STM16, GE-2, GE-HDE, ES2 4G, ES2 10G, and ES2 10G Uplink)

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

Related Documentation

- CAM Hardware Classifiers and Interface Attachment Resources on page 16
- FPGA Hardware Classifiers on page 5
- Interface Attachment Resources Overview on page 21

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. "Policy Resources Overview" on page 3 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.

Related Documentation

- Interface Attachment Resources Overview on page 21
- Policy Resources Overview on page 3

Detection of Corruption in the Statistics FPGA and System Operations on Detecting Corruption

When a bit flip occurs in a DRAM or static RAM (SRAM) of a statistics FPGA of a router functioning as the Session and Resource Control (SRC) or RADIUS client, the router may transmit corrupted accounting statistics to a SRC or RADIUS server. This affects the computation of accounting information for subscriber sessions. You must replace the hardware to resolve the incorrect computation of accounting information caused by the corrupted statistics retrieved from the SRC or RADIUS client.

A parity error check mechanism is introduced in the statistics FPGA of an ES2 4G LM to check whether the statistics is corrupted. The parity error check mechanism checks the parity in both the DRAM and SRAM for all statistics entries. The mechanism populates the parity error status bit of the statistics entry to indicate parity check failure. The parity

check failed statistics entries are not updated after the parity error is detected by the mechanism.

NOTE: The parity error check mechanism is supported only on ES2 4G LMs (with any IOA combination) and is applicable for both the PPP and L2TP subscribers. The parity error check mechanism restricts the available number of bits of a 64 bits packet/byte counter to 60 bits and 32 bits packet counter to 30 bits.

The parity error check mechanism is triggered to check for parity error during the following events:

- Receipt of a decision (DEC) message from the SRC server to attach the service policy to an interface.
- Receipt of a DEC message from the SRC server to retrieve interim accounting statistics.
- Sending of the final accounting report to the SRC server when the subscriber is terminated.
- Execution of the ***show ip interface*** or ***show ipv6 interface*** command to display current status of a specific interface.

NOTE: When the parity error check mechanism is triggered by the execution of the ***show ip interface*** or ***show ipv6 interface*** command, only the corruption is detected, but the subsequent actions such as subscriber termination are not carried out. Therefore, the subscriber slot is not added to the defective slot.

- Receipt of accounting start request from the RADIUS server.
- Receipt of interim accounting request from the RADIUS server.
- Receipt of accounting stop request from the RADIUS server.

You can use the ***fpga-stats-monitoring-enable*** command to prevent the router from reporting parity check failed user and policy accounting statistics to the RADIUS or SRC server.

NOTE: The router performs actions (such as subscriber termination) only during interim update or subscriber logout, but not during subscriber login.

Actions Performed on Detecting Parity Error

If you have executed the ***fpga-stats-monitoring-enable*** command and parity error is detected, the router performs the following actions for user and policy accounting statistics:

- Terminates the subscriber:

- In a single-stack environment, terminates the corresponding IPv4 or IPv6 subscriber and blocks other subscribers (both IPv4 and IPv6) from logging on to the line module. For an AAA accounting model, sends Acct-Stop message to the RADIUS server with the older uncorrupted user and policy accounting statistics. For SRC accounting model, sends Common Open Policy Service rendezvous-point tree (COPS RPT) message to the SRC server with an error code in response to interim requests and sends COPS Delete Request (DRQ) message to the SRC server during subscriber login or logout.
- In a dual-stack environment, terminates both IPv4 and IPv6 sessions on an interface even if statistics of any sessions (IPv4 or IPv6) on the interface is corrupted. For AAA accounting model, sends Acct-Stop message to the RADIUS server with the older uncorrupted user and policy accounting statistics of both PPP and IPv6 interfaces. For SRC accounting model, sends COPS RPT message to the SRC server with an error code in response to interim requests and sends COPS DRQ message to the SRC server during subscriber login or logout.
- If the Tunnel Service line module (TSM) slot is affected, terminates the corrupted tunneled subscriber and changes the corresponding server port state as “draining” by setting the maximum interfaces of the TSM to zero. Also, allows new subscribers to log in if there are any uncorrupted TSM slots.

NOTE: **The corrupted slot information is not retained after the unified in-service software upgrade (ISSU), router reload, and line module re-insertion. However, the corrupted slot information is retained after line module reload.**

- Generates an SNMP trap indicating the user or policy accounting failure, if you have enabled the generation of SNMP trap by using the ***fpga-stats-monitoring trap enable*** command.
- Generates a syslog message indicating the statistics corruption.
- Periodically (every 60 seconds) monitors the Parity Error Register of the FPGA for all DRAM and SRAM banks in which the parity error is identified.
- Supports the recovery mechanism:
  - For LCR usage models, if the parity error is detected on the active line module then the standby line module takes over as the active line module.
  - For LCHA usage models, if the parity error is detected on the active line module then the router unconfigures the LCHA group. Both active and standby line modules act as separate standalone line modules. Also maximum interfaces of the affected TSM is set as zero to prevent new subscribers from logging in.
  - If the affected line module is removed and then re-inserted, any subscribers are allowed to log in.
  - If the affected line module is reload, all subscribers are still blocked from logging in.

If you have executed the ***fpga-stats-monitoring-enable*** command and parity error is detected, the router performs the following actions for statistics other than user and policy accounting statistics:

- Periodically (at every 60 seconds) monitors the Parity Error Register of the FPGA for all DRAM or SRAM banks in which the parity error is identified.
- For each DRAM or SRAM bank, stores the index of the last statistics entry whose parity error status bit is set.
- Stops the statistics counter.
- Allows you to retrieve corrupted statistics details through SNMP and through CLI commands.

NOTE: When the parity error is detected in the multicast statistics on a corresponding interface for a multicast traffic, the unicast packet statistics does not include the actual received unicast packet count as the unicast statistics count is derived from the multicast statistics counter (that is, unicast count = inReceived packets-inMulticast packets).

If you have executed the ***fpga-stats-monitoring-enable*** command and parity error is detected, the ***show ip interface*** and ***show ipv6 interface*** commands display an error message instead of the policy accounting statistics details for the policies whose statistics are corrupted.

If you have not executed the ***fpga-stats-monitoring-enable*** command and parity error is detected, the subscribers are not terminated. But, the router sends the older uncorrupted user and policy accounting statistics to the RADIUS or SRC server in all subsequent interim records and also in final accounting record during subscriber logout. Also, the software displays an error message in the output of the ***show ppp interface*** command instead of the corrupted user accounting statistics details.

Related Documentation

- Configuring the Router to Perform Various Actions on Detecting Parity Error in the FPGA User and Policy Accounting Statistics on page 28
- Monitoring the Detection of Corrupted FPGA Statistics Settings on page 39

CAM Hardware Classifiers Overview

Content-addressable memory (CAM) hardware classifiers are supported on the OC48/STM16, GE-2, ES2 4G, ES2 10G, ES2 10G Uplink, and GE-HDE line modules. "Policy Resources Overview" on page 3 lists CAM hardware classifiers and the software classifiers supported for each interface type.

The OC48/STM16 line module supports 128,000 144-bit CAM entries, and the GE-2 and GE-HDE line modules support 64,000 144-bit CAM entries. The ES2 4G LMs on E120 and E320 routers support 256,000 144-bit CAM entries, and the ES2 10G and ES2 10G Uplink LMs on E120 and E320 routers support 128,000 144-bit 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
```

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.

Related Documentation

- CAM Hardware Classifiers and Interface Attachment Resources on page 16
- Interface Attachment Resources Overview on page 21
- Policy Resources Overview on page 3
- Size Limit for IP and IPv6 CAM Hardware Classifiers on page 10

Size Limit for IP and IPv6 CAM Hardware Classifiers

In JunosE Release 10.1.x and lower-numbered releases, the maximum width of a CAM hardware classifier entry for IPv4 or IPv6 in a single policy was 128 bits. This limitation enabled only 128 bits of classification data to be supported per policy. Any policy configuration (sum of all CLACL entries) with more than 128 bits of classification data failed when a policy was attached to an interface. This 128-bit size limitation applied to both IPv4 and IPv6 classification data. Although this limitation was acceptable for IPv4 classification, it posed problems when full IPv6 classification was required to be performed. In JunosE Release 10.2.x and later, based on the size limit for a combined IPv6

classifier entry, a maximum of 336 bits of CAM entry is supported for full IPv6 classification.

Some independent classifiers share the same classifier entry location, while others are combined together to form a larger classifier field. The smallest IPv6 classifier can consume 8 bits and the largest IPv6 classifier can consume 336 bits. Beginning with JunosE Release 10.2.x, variable-sized CAM entries are supported for IPv6 policies to avoid wasteful use of CAM entries. In earlier releases, the number of CAM entries per line module was predefined because all CAM entries were of a fixed size of 128 bits. With the support for variable-sized CAM entries for IPv6 policies, a dynamic algorithm is used for CAM resource management. This feature is supported on GE-2 and GE-HDE line modules on ERX14xx models, ERX7xx models, and the ERX310 router and ES2 4G LMs on E120 and E320 routers.

NOTE: **OC48/STM16 line modules on ERX14xx models, ERX7xx models, and the ERX310 router support only 128-bit IPv6 classification.**

Based on the size limit for a combined IPv6 classifier entry, a maximum of 336 bits of CAM entry is supported for full IPv6 classification. An additional 16 bits that are reserved for rule set ID are added to the total classifier entry size, which causes the total CAM entry size required to be 352 bits. Some of the mutually exclusive classification fields share the same classifier entry location, while a few other smaller fields are combined to form a single larger classifier field.

NOTE: **Range vector hardware classifiers on line modules supported full IPv6 classification even in JunosE releases earlier than Release 10.2.x.**

IP Classifiers and Size Limits

Table 5 on page 11 lists all IP classifiers and the size limit of each classifier entry.

Table 5: 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

Table 5: Size Limit of Individual IP Classifiers *(continued)*

IP Classifier	Size Limit (Bits)
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 6 on page 12 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 6 on page 12 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 6: 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	–

Table 6: Size Limit of Combined IP Classifiers *(continued)*

IP Classifier Entry Combination	Size Limit (Bits)	Rule
[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 7 on page 13 lists all IPv6 and the size limit of each classifier entry.

Table 7: Size Limit of Individual IPv6 Classifiers

IPv6 Classifier Entry	Size Limit (Bits)
Color	2

Table 7: Size Limit of Individual IPv6 Classifiers *(continued)*

IPv6 Classifier Entry	Size Limit (Bits)
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 8 on page 14 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 8 on page 14 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 8: 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	–

Table 8: Size Limit of Combined IPv6 Classifiers *(continued)*

IPv6 Classifier Entry Combination	Size Limit (Bits)	Rule
Destination address (second word)	32	–
Destination address (third word)	32	–
Destination address (fourth word)	32	–
Destination address route class	8	–
[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.

Related Documentation

- CAM Hardware Classifiers and Interface Attachment Resources on page 16
- CAM Hardware Classifiers Overview on page 9

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.

Related Documentation

- CAM Hardware Classifiers Overview on page 9
- Interface Attachment Resources Overview on page 21

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.

Related Documentation

- Interface Attachment Resources Overview on page 21

Performance Impact and Scalability Considerations

The following sections describe how the memory usage and performance of the line modules on which the variable-sized CAM entries are supported is affected, and also of the maximum number of policies that can be supported with variable-sized CAM entries.

Performance Impact

Some performance impact might occur due to the variable size of the CAM entries. This performance impact is caused by CAM addressing, which works on 72 bits. 576-bit classification requests now require up to 8 lookups to the CAM hardware (8 * 72 = 576). The CAM device has a search rate of up to 83 million per second for 144 bit entries.

Scalability Considerations

One CAM entry is required per classifier for each unique policy on each line module. Regardless of the classifier definition for an IPv4 policy, each IPv4 classifier consumes 144 bits (one 144-bit CAM entry). However, default classifiers do not consume CAM entries.

As described in "Examples: Variable-Sized CAM Classification for IPv6 Policies" on page 31, an IPv6 CAM entry size is 144 bits, 288 bits, or 576 bits, depending on the sum of the classification fields in the policy definition. However, all IPv6 classifiers consume the same CAM entry size in a policy.

The following factors are used to determine the CAM resources available for policies when variable-sized CAM entries are present:

- CAM Device Block Size and CAM Entry Allocation on page 17
- Number of CAM Entries Per Allocation and Free Entries on page 17

CAM Device Block Size and CAM Entry Allocation

Using GE-2 line modules, for example, we can demonstrate how the number of CAM entries it supports is divided into different blocks to store policies. GE-2 line modules contain 64,000 144-bit CAM entries. Each entry is divided into eight 8000 144-bit blocks. Each block can hold equal-sized CAM entries only—144-bit, 288-bit, and 576-bit CAM entries. If no more IPv6 policies are created and when the remaining seven blocks are used, the 576-bit CAM block is not available to store IPv4 policies that require 144-bit CAM entries only.

A default classifier within a policy also consumes the same sized CAM entry as the size computed for the policy. In lower numbered releases, a single 144-bit entry was reserved for default classifiers. In this release, the number of 144-bit entries reserved for default classifiers depends on the number of blocks assigned for such CAM entries and whether the attached policy contains 288-bit or 576-bit entries. For example, if the first block is used by the 576-bit CAM entry, four 144-bit entries are reserved for the default classifier.

Number of CAM Entries Per Allocation and Free Entries

The total number of CAM blocks is divided into two equal partitions. The first or lower half of the CAM blocks is reserved for 144-bit CAM entries, and the second or higher half of CAM blocks is reserved for the combination of 288-bit and 576-bit CAM entries, when an IPv6 policy that contains 288-bit or 576-bit CAM entries is attached to an interface. If IPv6 policies do not contain 288-bit or 576-bit CAM entries, all the blocks are used for 144-bit entries.

Assume that, on a GE-2 line module, out of the total of eight blocks, four blocks are completely used for 144-bit CAM entries and the remaining four blocks are allocated in common for 144-bit, 288-bit, and 576-bit entries. Each of the blocks reserved exclusively for 144-bit entries can contain 8000 entries, while each of the blocks reserved for the combination of the variable-sized entries can either contain 2000 576-bit entries or 4000 288-bit entries. The block that is common to the variable-sized entries is available for

144-bit entries only if an IPv6 policy does not contain 288-bit or 576-bit entries. Otherwise, when the first IPv6 policy that contains 288-bit or 576-bit entries is attached to an interface and if previously configured policies consumes more than 4 blocks, the IPv6 policy attachment fails.

The block that is common to the variable-sized entries is not available for 144-bit CAM entries when you configure any 288-bit or 576-bit entries, even though you remove them later. It is also not available for any 288-bit or 576-bit entries when the 144-bit entries spill into this block, even though you remove the 144-bit entries later.

NOTE: **ES2 4G LMs contain a total of 32 blocks, of which 16 blocks are assigned for 144-bit entries. The remaining 16 blocks are assigned for the combination of 144-bit, 288-bit, and 576-bit entries (pool common to these three variable-sized entries).**

Table 9 on page 18 lists the maximum policies supported with variable length IPv6 CAM classification and one classifier per policy. The following note is referred to in Table 9 on page 18.

1. The number of unique policies supported depends on the line module and the numbers used are to illustrate the impact with CAM entries. The actual policies vary according to the line module.

Table 9: Maximum Policies with One Classifier per Policy for GE-2 LMs

Number/Type of Policies	Total 144-bit CAM entries	Number of IPv4 policies (144-bit) with one CLACL (See Note 1)	Number of IPv6 policies (144-bit) with one CLACL	Number of IPv6 policies (288-bit) with one CLACL (See Note 1)	Number of IPv6 policies (576-bit) with one CLACL (See Note 1)	Number of maximum policies per LM (one CLACL per policy) (See Note 1)
All IPv4 policies	64,000	64,000	0	0	0	64,000
All IPv6 policies	64,000	0	64,000	0	0	64,000
All IPv6 policies	64,000	0	0	16,000	0	16,000
All IPv6 policies	64,000	0	0	0	8000	8000
Equal number of identical IPv4/IPv6 policies	64,000	32,000	32,000	0	0	64,000
Equal number of identical IPv4/IPv6 policies	64,000	16,000	0	16,000	0	32,000 (+ 16,000 144-bit entries available)

Table 9: Maximum Policies with One Classifier per Policy for GE-2 LMs *(continued)*

Number/Type of Policies	Total 144-bit CAM entries	Number of IPv4 policies (144-bit) with one CLACL (See Note 1)	Number of IPv6 policies (144-bit) with one CLACL	Number of IPv6 policies (288-bit) with one CLACL (See Note 1)	Number of IPv6 policies (576-bit) with one CLACL (See Note 1)	Number of maximum policies per LM (one CLACL per policy) (See Note 1)
Equal number of identical IPv4/IPv6 policies	64,000	8000	0	0	8000	16,000 (+ 24,000 144-bit entries available)

Table 10 on page 19 lists the maximum policies supported with variable length IPv6 CAM classification and four classifiers per policy.

Table 10: Maximum Policies with Four Classifiers per Policy for GE-2 LMs

Number/Type of Policies	Total 144-bit CAM entries	Number of IPv4 policies (144-bit) with four CLACLs	Number of IPv6 policies (144-bit) with four CLACL s	Number of IPv6 policies (288-bit) with four CLACLs	Number of IPv6 policies (576-bit) with four CLACLs	Number of maximum policies per LM (four CLACLs per policy)
All IPv4 policies	64,000	16,000	0	0	0	16,000
All IPv6 policies	64,000	0	16,000	0	0	16,000
All IPv6 policies	64,000	0	0	4000	0	4000
All IPv6 policies	64,000	0	0	0	2000	2000
Equal number of identical IPv4/IPv6 policies	64,000	8000	8000	0	0	16,000
Equal number of identical IPv4/	64,000	4000	0	4000	0	8000 (+ 16,000 144-bit entries available)
Equal number of identical IPv4/IPv6 policies	64,000	2000	0	0	2000	4000 (+ 24,000 144-bit entries available)

Related Documentation

- Examples: Variable-Sized CAM Classification for IPv6 Policies on page 31
- Size Limit for IP and IPv6 CAM Hardware Classifiers on page 10

Software Classifiers Overview

An E Series router supports a variety of software classifiers, depending on the type of interface. "Policy Resources Overview" on page 3 lists 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 11 on page 21.

Table 11: Resource Consumption

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

Related Documentation

- Policy Resources Overview on page 3

Interface Attachment Resources Overview

JunosE Software allocates interface attachment resources when policies are attached to interfaces—that is, 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 IPv4 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 policy 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.

  You can use the **show policy-resources slot** command to monitor the policy resource consumption on a specific slot or on all slots to which the policies are attached. The **show policy-resources slot** command displays the type of policy resource, number of policy resources supported, number of policy resources consumed, number of policy resources that are free, and direction type for each resource type.

NOTE: The current system maximums of the E Series router are displayed in the **show policy-resources slot** command output as the number of policy resources supported by the line module. For the current system maximums, see *Appendix A*, *System Maximums* in the *JunosE Release Notes*.

Related Documentation

- Policy Resources Overview on page 3
- Enabling the Policy Resources Exhaustion Trap on page 27
- Monitoring the Utilization of Interface Attachment Resources on page 40
- *show policy-resources slot*

PART 2

Configuration

CHAPTER 2

Configuration Tasks for Policy Resources Management

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 ipCLAC
   host1(config-policy-list-classifier-group)#filter

6. Apply the policy list to an interface.

   host1(config)#interface atm 5/0/0.1
   host1(config-if)#ip policy input ipPol

Table 12 on page 26 lists the active classifiers in the policy named ipPol and the size of each classifier.

Table 12: 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 5/0/0.1
host1(config-if)#ip policy input ipPol
% too many classifier fields in policy
```

Table 13 on page 27 lists the active classifiers in the policy named ipPol and the size of each classifier.

Table 13: 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.

Related Documentation

- Interface Attachment Resources Overview on page 21

Enabling the Policy Resources Exhaustion Trap

You can use the **policy-resource-exhaustion trap enable** command to enable the policy resource exhaustion trap to send an SNMP trap notification to the SNMP manager when the policy resources are exhausted. An SNMP trap notification is sent for the following policy resource types when they exceed their maximum limits as per the system maximums:

- ipPolicyDescriptor (0)
- l2PolicyDescriptor (1)
- rateLimiter (2)
- statsBlock (3)

- camTotalEntries (4)
- softwareLookupRuleSet (5)
- parentGroup (6)

For more information about the system maximums, see *Appendix A*, *System Maximums* in the *JunosE Release Notes*.

An SNMP trap notification contains the following information:

- Slot number in which the policy resource is exhausted
- Type of the exhausted policy resource
- Direction of the exhausted policy resource: ingress, egress, or both.

To enable the policy resource exhaustion trap to send an SNMP trap notification:

- Issue the **policy-resource-exhaustion trap enable** command in Privileged Exec mode.

```
host1#policy-resource-exhaustion trap enable
```

Use the **no** version to disable the policy resource exhaustion trap from sending an SNMP trap notification when the policy resources are exhausted.

Related Documentation

- Policy Resources Overview on page 3
- Interface Attachment Resources Overview on page 21
- Monitoring the Status of a Policy Resources Trap on page 42
- *policy-resource-exhaustion-trap-enable*

Configuring the Router to Perform Various Actions on Detecting Parity Error in the FPGA User and Policy Accounting Statistics

You can configure the router, which functions as an SRC or RADIUS client, to perform various actions (such as subscriber termination) on detecting parity error in a statistics FPGA by using the parity error check mechanism. For more information about the parity error check mechanism and system operations on detecting corruption, see "Detection of Corruption in the Statistics FPGA and System Operations on Detecting Corruption" on page 6.

You can prevent the SRC or RADIUS client from sending incorrect and discrepant user and policy accounting statistics to the SRC or RADIUS server by enabling the router to perform various actions on parity error detection.

To configure the router to perform various actions on detecting parity error in the user and policy accounting statistics in the statistics FPGA:

- Enable the router to perform actions (such as subscriber termination) on detecting parity error.

```
host1#fpga-stats-monitoring-enable
```


You can use the **no** version of the ***fpga-stats-monitoring-enable*** command to disable this functionality. By default, the router is disabled from performing various actions on detecting parity error.

NOTE: The parity error check mechanism always checks for the parity error during various scenarios (such as policy attachment).

- Enable the capability to generate SNMP traps when corruption is determined in the user and policy accounting statistics.

  host1(config)#fpga-stats-monitoring trap enable

  You can use the **no** version of the ***fpga-stats-monitoring trap enable*** command to disable this functionality. By default, SNMP traps are not generated on detecting parity error.

Related Documentation

- Monitoring the Detection of Corrupted FPGA Statistics Settings on page 39

CHAPTER 3

Examples

Examples: Variable-Sized CAM Classification for IPv6 Policies

Variable-sized CAM entries are supported for IPv6 policies to avoid wasting memory space. For example, if the classifier entries in a policy consume a 576-bit CAM entry when a 144-bit CAM entry is sufficient to store the classifier, over 400 bits of CAM memory are wasted. CAM memory is divided into blocks at the hardware level. Each CAM block can support 8000 144-bit, 4000 288-bit, or 2000 576-bit CAM entries. Based on the IPv6 header CAM entry size calculation, the minimum entry size required for IPv6 classification is 8 bits and the maximum entry size required is 336 bits.

Policy Manager calculates the CAM bit size and configures the CAM entries on the line modules. The size of the CAM entry is determined using the limits defined for each of the IP classifier entry combination. In earlier releases, any policy configuration with CAM entries that exceeded the 128-bit limitation failed to be attached to the interface because it was not allowed by Policy Manager.

Beginning with JunosE Release 10.2.x, the IPv6 classification functionality is modified to classify traffic on more than 128 bits. To improve scalability for IPv6 policies, Policy Manager uses the optimum CAM entry size, depending on the IPv6 policy definition. The policy definition of IPv6 is used to determine which classification fields in the combined IPv6 classifier are present and the CAM entry length is computed dynamically. The following three different kinds of results are possible for an IPv6 policy:

- Sum of all classifier fields is less than or equal to 128 bits
- Sum of all classifier fields is between 128 bits and 272 bits
- Sum of all classifier fields is between 272 bits and 336 bits

CAM hardware classifiers support four types of CAM entries—72-bit, 144-bit, 288-bit, and 576-bits (16-bits are reserved for rule set id). Each of the policies fit into one of these four CAM entry types. The 72-bit CAM entry is not chosen as CAM devices on some line modules do not support this size limit. Therefore, the 144-bit, 288-bit, and 576-bit CAM entries are used as the variable-length CAM entries for IPv6 policies.

The following sections describe examples for each type of variable length IPv6 classification and the number of CAM entries for each case:

144-bit IPv6 Classification Example

In this example, a policy with a combination of IPv6 classifiers is created and attached. The configuration conforms to the 144 bit limit.

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

   host1(config)#ipv6 classifier-list tcpCLACL source-address 1:1::/32 tcp destination-port eq 2000 tcp-flags "SYN"

2. Match all IPv6 packets to net 2:2::.

   host1(config)#ipv6 classifier-list ipv6CLACL destination-address 2:2::/32

3. Match all ICMPv6 echo packets.

   host1(config)#ipv6 classifier-list icmpv6CLACL icmpv6 icmp-type 8 icmp-code 0

4. Match all frames with the color red.

   host1(config)#ipv6 classifier-list colorCLACL color red

5. Create an IPv6 policy list.

   host1(config)#ipv6 policy-list ipv6Pol
   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 icmpv6CLACL
   host1(config-policy-list-classifier-group)#filter
   host1(config-policy-list-classifier-group)#classifier-group ipv6CLACL
   host1(config-policy-list-classifier-group)#filter

   The policy ipv6Pol is requesting classification on Source Address (first word), Destination Address (first word), Destination Port, Protocol, TCP Flags, ICMPv6 Type, ICMPv6 Code, Color, and TC field. Table 14 on page 32 lists the active classifiers in the policy named ipv6Pol and the size of each classifier.

Table 14: IPv6 Classification Fields for a 144-bit CAM Entry

Classifiers	Size (Bits)
Source address (first word)	32
Destination address (first word)	32
Destination port, ICMPv6 type, ICMPv6 code	16
Protocol	8
Color and TCP flags	8
TC field	8

The sum of all classification fields requested in ipv6Pol is 104. This size causes Policy Manager to use 144-bit CAM entry for every classifier in this policy. One CAM entry is

needed for each classifier in the policy and therefore, four 144-bit CAM entries are needed in all.

288-bit IPv6 Classification Example

The following example creates and attaches a policy, which requests classification on a single host address and TCP. The configuration exceeds the 128 bit limit.

1. Match all TCP packets from host 1:1:1:1:1:1:1:1 to any DA

   host1(config)#ipv6 classifier-list sourceCLACL source-address 1:1:1:1:1:1:1:1/128 tcp

2. Create an IPv6 policy list.

   host1(config)#ipv6 policy-list ipv6Pol
   host1(config-policy-list)#classifier-group sourceCLACL
   host1(config-policy-list-classifier-group)#forward
   host1(config-policy-list-classifier-group)#classifier-group *
   host1(config-policy-list-classifier-group)#filter

   The policy ipv6Pol is requesting classification on Source Address (all 4 words) and Protocol. Table 15 on page 33 lists the active classifiers in the policy named ipv6Pol and the size of each classifier.

Table 15: IPv6 Classification Fields for a 288-bit CAM Entry

Classifiers	Size (Bits)
Source address (first word)	32
Source address (second word)	32
Source Address (third word)	32
Source Address (fourth word)	32
Protocol	8

The sum of all classification fields requested in ipv6Pol is 136, which is greater than 128-bit CAM entry size limit. Although this configuration fails to attach to the interface in JunosE releases earlier than Release 10.2.0, it is successfully attached to the interface, beginning with JunosE Release 10.2.x, and the next higher 288-bit CAM entry is allocated for this policy (two 288-bit entries because of two classifiers being defined in the policy).

576-bit IPv6 Classification Example

In this example, a policy with a combination of IPv6 classifiers is created and attached.

1. Match all TCP packets from host 1:1:1:1:1:1:1:1 to host 100::1 destined to port 80 from source port 10000

   host1(config)#ipv6 classifier-list tcpCLACL source-host 1:1:1:1:1:1:1:1 destination-host 100::1 tcp source-port eq 10000 destination-port eq 80

2. Match all frames with the color red

   host1(config)#ipv6 classifier-list colorCLACL color red

3. Create an IPv6 policy list.

   host1(config)#ipv6 policy-list ipv6Pol
   host1(config-policy-list)#classifier-group tcpCLACL
   host1(config-policy-list-classifier-group)#forward
   host1(config-policy-list-classifier-group)#classifier-group colorCLACL
   host1(config-policy-list-classifier-group)#forward
   host1(config-policy-list-classifier-group)#classifier-group *
   host1(config-policy-list-classifier-group)#filter

   The policy ipv6Pol is requesting classification on Source Address (all 4 words), Destination address (all 4 words) and Protocol. Table 16 on page 34 lists the active classifiers in the policy named ipv6Pol and the size of each classifier.

Table 16: IPv6 Classification Fields for a 576-bit CAM Entry

Classifiers	Size (Bits)
Source address (first word)	32
Source address (second word)	32
Source Address (third word)	32
Source address (fourth word)	32
Destination Address (first word)	32
Destination address (second word)	32
Destination Address (third word)	32
Destination Address (fourth word)	32
Protocol	8
Destination Port	16
Source Port	16
Color	8

The sum of all classification fields requested in ipv6Pol is 304, which is greater than 128-bit CAM entry size limit. Although this configuration fails to attach to the interface in earlier releases, it is successfully attached to the interface, beginning with this release, and the maximum 576-bit CAM entry is allocated for this policy (three 576-bit entries, one for each classifier in the policy).

Although each CAM block can contain 2000 576-bit CAM entries, the hardware considers the CAM block to contain 8000 144-bit entries that are clustered together

as 4 sets each of 144-bit entries. In this example, although three 576-bit entries are used, one for each classifier in the policy, these entries are essentially three sets of 144-bit entries from the 576-bit CAM block. The sum of the unique classification fields in the policy determines the group from which the CAM resources are allocated for the entire policy (the 144-bit, the 288-bit, or the 576-bit group).

Related Documentation

- CAM Hardware Classifiers Overview on page 9
- Performance Impact and Scalability Considerations on page 16
- Size Limit for IP and IPv6 CAM Hardware Classifiers on page 10

PART 3

Administration

CHAPTER 4

Monitoring Task for Policy Resources Management

Monitoring the Detection of Corrupted FPGA Statistics Settings

Purpose Display the configuration details of the FPGA statistics detection utility.

Action To display the router settings to perform various actions on detecting corruption in user and policy accounting statistics retrieved from the statistics FPGA:

```
host1#show fpga-stats-monitoring
FPGA statistics monitoring is enabled
FPGA statistics monitoring trap is enabled
```

Meaning Table 17 on page 39 lists the **show fpga-stats-monitoring** command output fields.

Table 17: show fpga-stats-monitoring Output Fields

Field Name	Field Description
FPGA statistics monitoring	Displays whether the router is enabled or disabled to perform various actions (such as subscriber termination) on detecting corruption in the user and policy accounting statistics retrieved from the statistics FPGA. For more information about the parity error check mechanism and system operations on detecting corruption, see "Detection of Corruption in the Statistics FPGA and System Operations on Detecting Corruption" on page 6.
FPGA statistics monitoring trap	Displays whether the capability to generate SNMP traps when corruption is identified in the FPGA is enabled or disabled.

Related Documentation

- Configuring the Router to Perform Various Actions on Detecting Parity Error in the FPGA User and Policy Accounting Statistics on page 28

- *show fpga-stats-monitoring*

Displaying the Slot Numbers with Corrupted Statistics FPGA for AAA-Based Policy Accounting

Purpose Display the list of slot numbers in which corruption of FPGA statistics is detected while reporting policy or user accounting to the RADIUS server through AAA.

NOTE: The corrupted slot information is not retained after the unified ISSU, router reload, and line module re-insertion. However, the corrupted slot information is retained after line module reload.

Action To display corrupted slot numbers:

```
host1#show aaa-corrupted-slots
Corrupted Slot List :
1
2
```

Related Documentation

- Detection of Corruption in the Statistics FPGA and System Operations on Detecting Corruption on page 6
- *show aaa-corrupted-slots*

Monitoring the Utilization of Interface Attachment Resources

Purpose Display policy resource consumption information about a particular slot or all slots to which the policies are attached.

Action To display policy resource consumption information about all slots to which the policies are attached:

```
host1#show policy-resources slot all

Slot number 4

Resource   Supported    Used    Remaining       Direction
--------   --------    ------   ----------     ----------

IpPolicyDesc    16000   0       16000          Ingress
IpPolicyDesc    8191    0       8191           Egress
L2PolicyDesc    8191    0       8191           Ingress
L2PolicyDesc    8191    0       8191           Egress
RateLimiter     24575   0       24575          Ingress
RateLimiter     24575   0       24575          Egress
StatsBlock      262140  0       262140         Ingress
StatsBlock      262140  0       262140         Egress
SwLookupRuleSet 16383   0       16383          NA
ParentGroups    8191    0       8191           Ingress
ParentGroups    8191    0       8191           Egress
```

```
Slot number 5

Resource   Supported    Used    Remaining       Direction
--------   --------    ------   ----------     ----------

IpPolicyDesc    16000   0       16000           Ingress
IpPolicyDesc    8191    0       8191            Egress
L2PolicyDesc    8191    0       8191            Ingress
L2PolicyDesc    8191    0       8191            Egress
RateLimiter     24575   0       24575           Ingress
RateLimiter     24575   0       24575           Egress
StatsBlock      262140  0       262140          Ingress
StatsBlock      262140  0       262140          Egress
SwLookupRuleSet 16383   0       16383           NA
ParentGroups    24575   0       24575           Ingress
ParentGroups    24575   0       24575           Egress

Slot number 6

Resource   Supported    Used    Remaining       Direction
--------   --------    ------   ----------     ----------

IpPolicyDesc    16000   0       16000           Ingress
IpPolicyDesc    8191    0       8191            Egress
L2PolicyDesc    8191    0       8191            Ingress
L2PolicyDesc    8191    0       8191            Egress
RateLimiter     24575   0       24575           Ingress
RateLimiter     24575   0       24575           Egress
StatsBlock      262140  0       262140          Ingress
StatsBlock      262140  0       262140          Egress
SwLookupRuleSet 16383   0       16383           NA
ParentGroups    8191    0       8191            Ingress
ParentGroups    8191    0       8191            Egress
```

To display policy resource consumption information about a particular slot to which the policies are attached:

```
host1#show policy-resources slot 5

Slot number 5

Resource   Supported    Used    Remaining       Direction
--------   --------    ------   ----------     ----------

IpPolicyDesc    16000   0       16000           Ingress
IpPolicyDesc    8191    0       8191            Egress
L2PolicyDesc    8191    0       8191            Ingress
L2PolicyDesc    8191    0       8191            Egress
RateLimiter     24575   0       24575           Ingress
RateLimiter     24575   0       24575           Egress
StatsBlock      262140  0       262140          Ingress
StatsBlock      262140  0       262140          Egress
SwLookupRuleSet 16383   0       16383           NA
ParentGroups    24575   0       24575           Ingress
ParentGroups    24575   0       24575           Egress
```

Meaning Table 18 on page 42 lists the output fields for the **show policy-resources slot** command.

Table 18: show policy-resources slot Output Fields

Field Name	Field Description
Slot number	Number of the chassis slot
Resource	Type of policy resources: • IpPolicyDesc – L3 policy interface attachments per line module • L2PolicyDesc – L2 policy interface attachments per line module • RateLimiter – Rate limiters per line module • StatsBlock – Policy statistics blocks per line module • CamTotalEntries – Policy classification (CLACL) entries per line module • SwLookupRuleSet – Software lookup blocks per line module • ParentGroups – Parent groups per line module
Supported	Number of policy resources supported by the line module
Used	Number of policy resources consumed by the line module
Remaining	Number of policy resources that are free in the line module
Direction	Direction type of the policy resources: • Ingress – Input policy resource attached to the interface • Egress – Output policy resource attached to the interface • Both – Input and output policy resources attached to the interface

Related Documentation

- Interface Attachment Resources Overview on page 21
- *show policy-resources slot*

Monitoring the Status of a Policy Resources Trap

Purpose Display the status of a policy resources trap.

Action To display the status of a policy resources trap:

```
host1#show policy-resources trap

Policy Resource exhaustion trap is enabled
```

Related Documentation

- Enabling the Policy Resources Exhaustion Trap on page 27
- *show policy-resources trap*

PART 4

Index

Index

Symbols

A

C

D

F

