

Classifying Packets by Behavior Aggregate on EX9200 Switches



Published: 2015-05-15

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Classifying Packets by Behavior Aggregate on EX9200 Switches
Copyright © 2015, Juniper Networks, Inc.
All rights reserved.

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.

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

	About the Documentation	ix
	Documentation and Release Notes	ix
	Supported Platforms	ix
	Using the Examples in This Manual	ix
	Merging a Full Example	x
	Merging a Snippet	x
	Documentation Conventions	xi
	Documentation Feedback	xiii
	Requesting Technical Support	xiii
	Self-Help Online Tools and Resources	xiii
	Opening a Case with JTAC	xiv
Part 1	Overview	
Chapter 1	Behavior Aggregate Classifier	3
	Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic	4
	Default Behavior Aggregate Classification Overview	7
	Understanding DSCP Classification for VPLS	8
	BA Classifiers and ToS Translation Tables	8
	Classifiers and Rewrite Rules at the Global and Physical Interface Levels	
	Overview	9
Chapter 2	BA Classifier Default Values	11
	Default IP Precedence Classifier (ipprec-compatibility)	11
	Default MPLS EXP Classifier	12
	Enabling Default DSCP and DSCP IPv6 Classifiers	12
	Default IEEE 802.1p Classifier	14
	Default IEEE 802.1ad Classifier	15
	Default IP Precedence Classifier (ipprec-default)	16
Part 2	Configuration	
Chapter 3	Configuration Tasks for Classifiers	19
	Defining Classifiers	19
	Importing a Classifier	20
	Applying Classifiers to Logical Interfaces	20
	DSCP Classifier Configuration Examples	24
	Managing Congestion by Setting Packet Loss Priority for Different Traffic	
	Flows	26
	Example: Overriding the Default PLP on M320 Routers	26
	Mapping PLP to RED Drop Profiles	27

Chapter 4	Configuration Tasks for BA Classifiers	29
	DSCP IPv6 Rewrites and Forwarding Class Maps	29
	Tunneling and BA Classifiers	30
	Configuring Classifiers and Rewrite Rules at the Global and Physical Interface Levels	30
Chapter 5	Configuration Task for DSCP IPv6 Classifiers	33
	Applying DSCP IPv6 Classifiers	33
Chapter 6	Configuration Tasks for MPLS EXP Classifiers	35
	Applying MPLS EXP Classifiers to Routing Instances	35
	Configuring Global Classifiers and Wildcard Routing Instances	36
	Examples: Applying MPLS EXP Classifiers to Routing Instances	37
	Applying MPLS EXP Classifiers for Explicit-Null Labels	39
Chapter 7	Configuration Task for IEEE 802.1ad Classifiers	41
	Configuring and Applying IEEE 802.1ad Classifiers	41
	Defining Custom IEEE 802.1ad Maps	41
	Applying Custom IEEE 802.1ad Maps	41
	Verifying Custom IEEE 802.1ad Map Configuration	42
Chapter 8	Configuration Statements	43
	[edit class-of-service] Hierarchy Level	43
	classifiers (Logical Interface)	48
	classifiers (Routing Instance)	49
	classifiers (Definition)	50
	classifiers (Physical Interface)	51
	code-points	52
	copy-plp-all	52
	dscp (AS PIC Classifiers)	53
	dscp (CoS Interfaces)	53
	dscp-ipv6 (CoS Rewrite Rules)	54
	exp	55
	forwarding-class (BA Classifiers)	56
	ieee-802.1 (Rewrite Rules on Logical Interface)	57
	ieee-802.1 (Classifier on Physical Interface)	58
	ieee-802.1ad	59
	import (Classifiers)	60
	inet-precedence (CoS Rewrite Rules)	60
	inet-precedence (Classifier on Physical Interface)	61
	interfaces (CoS)	62
	loss-priority (BA Classifiers)	64
	routing-instances (CoS)	65
	system-defaults	66
	unit	67

List of Figures

Part 1	Overview	
Chapter 1	Behavior Aggregate Classifier	3
	Figure 1: How a Classifier Works	4

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	xi
	Table 2: Text and Syntax Conventions	xi
Part 1	Overview	
Chapter 2	BA Classifier Default Values	11
	Table 3: Default IP Precedence Classifier	11
	Table 4: Default MPLS Classifier	12
	Table 5: Default DSCP Classifier	13
	Table 6: Default IEEE 802.1p Classifier	14
	Table 7: Default IEEE 802.1ad Classifier	15
	Table 8: Default IP Precedence (ipprec-default) Classifier	16
Part 2	Configuration	
Chapter 3	Configuration Tasks for Classifiers	19
	Table 9: Logical Interface Classifier Combinations	21
Chapter 6	Configuration Tasks for MPLS EXP Classifiers	35
	Table 10: Default MPLS EXP Classifier	35

About the Documentation

- Documentation and Release Notes on page ix
- Supported Platforms on page ix
- Using the Examples in This Manual on page ix
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

Documentation and 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/>.

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

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- EX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

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 xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide names.Identifies RFC and Internet draft titles.	<ul style="list-style-type: none">A policy <i>term</i> is a named structure that defines match conditions and actions.<i>Junos OS CLI User Guide</i>RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

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 JNASC 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

- [Behavior Aggregate Classifier on page 3](#)
- [BA Classifier Default Values on page 11](#)

CHAPTER 1

Behavior Aggregate Classifier

- [Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic on page 4](#)
- [Default Behavior Aggregate Classification Overview on page 7](#)
- [Understanding DSCP Classification for VPLS on page 8](#)
- [BA Classifiers and ToS Translation Tables on page 8](#)
- [Classifiers and Rewrite Rules at the Global and Physical Interface Levels Overview on page 9](#)

Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic

The idea behind class of service (CoS) is that packets are not treated identically by the routers or switches on the network. In order to selectively apply service classes to specific packets, the packets of interest must be classified in some fashion.

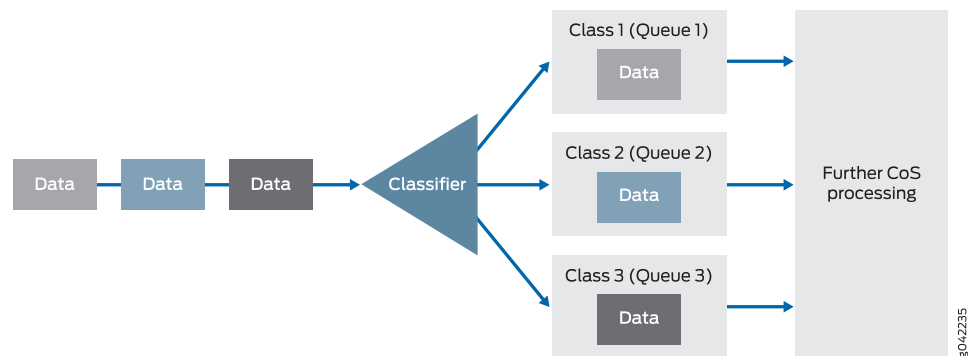
The simplest way to classify a packet is to use behavior aggregate (BA) classification. The DSCP, DSCP IPv6, or IP precedence bits of the IP header convey the behavior aggregate class information. The information might also be found in the MPLS EXP bits, IEEE 802.1ad, or IEEE 802.1p CoS bits.

BA classification is useful if the traffic comes from a trusted source and the CoS value in the packet header is trusted. If the traffic is untrusted, multifield classifiers (see *Overview of Assigning Service Levels to Packets Based on Multiple Packet Header Fields*) are used to classify packets based on multiple packet fields. It is common to use multifield classifiers to classify traffic at the ingress of a network, rewrite the packet headers (see *Rewriting Packet Headers to Ensure Forwarding Behavior*), then use the more efficient BA classification for transversing the network.

The BA classifier maps a CoS value in the packet header to a forwarding class and loss priority. The forwarding class determines the output queue. The loss priority is used by schedulers in conjunction with the random early discard (RED) algorithm to control packet discard during periods of congestion.

Figure 1 on page 4 provides a high-level illustration of how a classifier works.

Figure 1: How a Classifier Works



The types of BA classifiers are based on which part of the incoming packet the classifier examines:

- DSCP, DSCP IPv6, or IP precedence—IP packet classification (Layer 3 headers)
- MPLS EXP—MPLS packet classification (Layer 2 headers)
- IEEE 802.1p—Packet classification (Layer 2 headers)
- IEEE 802.1ad—Packet classification for IEEE 802.1ad formats (including DEI bit)

Unlike multifield classifiers, BA classifiers are based on fixed-length fields, which makes them computationally more efficient than multifield classifiers. For this reason, core

devices are normally configured to perform BA classification, because of the higher traffic volumes they handle.

In most cases, you need to rewrite a given marker (IP precedence, DSCP, IEEE 802.1p, IEEE 802.1ad, or MPLS EXP settings) at the ingress node to accommodate BA classification by core and egress devices. For more information about rewrite markers, see *Rewriting Packet Headers to Ensure Forwarding Behavior*.

If you apply an IEEE 802.1 classifier to a logical interface, this classifier takes precedence and is not compatible with any other classifier type. On Juniper Networks MX Series Ethernet Services Routers and EX Series switches using IEEE 802.1ad frame formats, you can apply classification on the basis of the IEEE 802.1p bits (three bits in either the inner virtual LAN (VLAN) tag or the outer VLAN tag) and the drop eligible indicator (DEI) bit. On routers with IQ2 PICs using IEEE 802.1ad frame format, you can apply classification based on the IEEE 802.1p bits and the DEI bit. Classifiers for IP (DSCP or IP precedence) and MPLS (EXP) can coexist on a logical interface if the hardware requirements are met. (See [“Applying Classifiers to Logical Interfaces” on page 20.](#))

The Enhanced Queuing DPC (EQ DPC) does not support BA classification for packets received from a Layer 3 routing interface or a virtual routing and forwarding (VRF) interface and routed to an integrated routing and bridging interface (IRB) to reach the remote end of a pseudowire connection. The EQ DPC also does not support BA classification for Layer 2 frames received from a Virtual Private LAN Service (VPLS) pseudowire connection from a remote site and routed to a Layer 3 routing interface through an IRB interface.

For Juniper Networks M Series Multiservice Edge Routers, four classes can forward traffic independently. For M320 Multiservice Edge Routers and Juniper Networks T Series Core Routers, eight classes can forward traffic independently. Therefore, you must configure additional classes to be aggregated into one of these classes. You use the BA classifier to configure class aggregation.

For Juniper M Series Multiservice Edge Routers with Intelligent Queuing 2 (IQ2) and Enhanced Intelligent Queuing 2 (IQ2E) PICs, the following restrictions apply:

- You can only use BA classifiers for IPv4 DSCP bits for virtual private LAN service (VPLS).
- You cannot use BA classifiers for IPv4 DSCP bits for Layer 2 VPNs.
- You cannot use BA classifiers for IPv6 DSCP bits for VPLS.
- You cannot use BA classifiers for IPv6 DSCP bits for Layer 2 VPNs.

For Juniper Networks MX Series 3D Universal Edge Routers, the following restrictions apply:

- You can only use multifield classifiers (but *not* BA classifiers) for IPv4 DSCP bits for virtual private LAN service (VPLS).
- You cannot use BA classifiers for IPv4 DSCP bits for Layer 2 VPNs.
- You cannot use BA classifiers for IPv6 DSCP bits for VPLS.
- You cannot use BA classifiers for IPv6 DSCP bits for Layer 2 VPNs.

For the 10-port 10-Gigabit Oversubscribed Ethernet (OSE) PICs, the following restrictions on BA classifiers apply:

- Multiple classifiers can be configured to a single logical interface. However, there are some restrictions on which the classifiers can coexist.

For example, the DSCP and IP precedence classifiers cannot be configured on the same logical interface. The DSCP and IP precedence classifiers can coexist with the DSCP IPv6 classifier on the same logical interface. An IEEE 802.1 classifier can coexist with other classifiers and is applicable only if a packet does not match any of the configured classifiers. For information about the supported combinations, see [“Applying Classifiers to Logical Interfaces” on page 20](#).

- If the classifiers are not defined explicitly, then the default classifiers are applied as follows:
 - All MPLS packets are classified using the MPLS (EXP) classifier. If there is no explicit MPLS (EXP) classifier, then the default MPLS (EXP) classifier is applied.
 - All IPv4 packets are classified using the IP precedence and DSCP classifiers. If there is no explicit IP precedence or DSCP classifier, then the default IP precedence classifier is applied.
 - All IPv6 packets are classified using a DSCP IPv6 classifier. If there is no explicit DSCP IPv6 classifier, then the default DSCP IPv6 classifier is applied.
 - If the IEEE 802.1p classifier is configured and a packet does not match any explicitly configured classifier, then the IEEE 802.1p classifier is applied.



NOTE: For a specified interface, you can configure both a multifield classifier and a BA classifier without conflicts. Because the classifiers are always applied in sequential order, the BA classifier followed by the multifield classifier, any BA classification result is overridden by a multifield classifier if they conflict. For more information about multifield classifiers, see *Overview of Assigning Service Levels to Packets Based on Multiple Packet Header Fields*.

**Related
Documentation**

- *Overview of Assigning Service Levels to Packets Based on Multiple Packet Header Fields*
- *Rewriting Packet Headers to Ensure Forwarding Behavior*

Default Behavior Aggregate Classification Overview

The software automatically assigns an implicit default IP precedence classifier to all logical interfaces.



NOTE: Only the IEEE 802.1p classifier is supported in Layer 2 interfaces. You must explicitly apply this classifier to the interface as shown in [“Default IEEE 802.1p Classifier” on page 14](#).

If you enable the MPLS protocol family on a logical interface, a default MPLS EXP classifier is automatically applied to that logical interface.

Other default classifiers (such as those for IEEE 802.1p bits and DSCP) require that you explicitly associate a default classification table with a logical interface. When you explicitly associate a default classifier with a logical interface, you are in effect overriding the implicit default classifier with an explicit default classifier.



NOTE: Although several code points map to the expedited-forwarding (ef) and assured-forwarding (af) classes, by default no resources are assigned to these forwarding classes. All af classes other than af1x are mapped to best-effort, because RFC 2597, *Assured Forwarding PHB Group*, prohibits a node from aggregating classes.

You can apply IEEE 802.1p classifiers to interfaces that are part of VPLS routing instances.

Related Documentation

- [Default IP Precedence Classifier \(ipprec-compatibility\) on page 11](#)
- [Default MPLS EXP Classifier on page 12](#)
- [Enabling Default DSCP and DSCP IPv6 Classifiers on page 12](#)
- [Default IEEE 802.1p Classifier on page 14](#)
- [Default IEEE 802.1ad Classifier on page 15](#)
- [Default IP Precedence Classifier \(ipprec-default\) on page 16](#)

Understanding DSCP Classification for VPLS

You can perform Differentiated Services Code Point (DSCP) classification for IPv4 packets on Ethernet interfaces that are part of a virtual private LAN service (VPLS) routing instance on the ingress provider edge (PE) router. This is supported on the M320 router with Enhanced type III FPC and the M120 router. On the Intelligent Queuing 2 (IQ2) or Intelligent Queuing 2 Enhanced (IQ2E) PICs, the **vlan-vpls** encapsulation statement is required. DSCP for IPv6 and Internet precedence for IPv6 are not supported.

In order to perform DSCP classification for IPv4 packets on Ethernet interfaces that are part of a VPLS routing instance on the ingress PE router, you must make sure of the following:

- The correct encapsulation statement based on PIC type is configured for the interface.
- The DSCP classifier is defined (default is allowed) at the **[edit class-of-service classifiers]** hierarchy level.
- The defined DSCP classifier is applied to the interface.
- The interface is included in the VPLS routing instance on the ingress of the PE router.

Related Documentation

- [Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic on page 4](#)

BA Classifiers and ToS Translation Tables

On some PICs, the behavior aggregate (BA) translation tables are included for every logical interface (unit) protocol family configured on the logical interface. The proper default translation table is active even if you do not include any explicit translation tables. You can display the current translation table values with the **show class-of-service classifiers** command.

On Juniper Networks M40e, M120, M320 Multiservice Edge Routers, and T Series Core Routers with Enhanced IQ (IQE) PICs, or on any router or switch with IQ2 or Enhanced IQ2 (IQ2E) PICs, you can replace the type-of-service (ToS) bit value on the incoming packet header on a logical interface with a user-defined value. The new ToS value is used for all class-of-service processing and is applied before any other class-of-service or firewall treatment of the packet. The PIC uses the **translation-table** statement to determine the new ToS bit values.

You can configure a physical interface (port) or logical interface (unit) with up to three translation tables. For example, you can configure a port or unit with BA classification for IPv4 DSCP, IPv6 DSCP, and MPLS EXP. The number of frame relay data-link connection identifiers (DLCIs) (units) that you can configure on each PIC varies based on the number and type of BA classification tables configured on the interfaces.

For more information on configuring ToS translation tables, along with examples, see *Configuring ToS Translation Tables*.

Classifiers and Rewrite Rules at the Global and Physical Interface Levels Overview

On ACX Series Universal Access Routers and EX Series switches, CoS supports classification and rewrite at the global level and physical interface levels.

At a global level, you can define EXP classification.

At a physical interface level, you can define the following features:

- DSCP and inet-precedence classifiers
- DSCP and inet-precedence rewrites
- ieee-802.1 classifiers (inner and outer)
- ieee-802.1 rewrites (outer)

At a logical interface level, you can define the fixed classification and EXP rewrites.

To configure global EXP classifiers, include the **classifiers exp classifier-name** statement at the **[edit class-of-service] system-defaults** hierarchy level.

To configure classifiers or rewrite rules at the physical interface, include either the **classifiers** statement or the **rewrite-rules** statement at the **[edit class-of-service] interfaces interface-name]** hierarchy level.

To display classifiers configured under **system-defaults**, enter the **show class-of-service system-defaults** command.

To display classifiers and rewrite rules bound to physical interfaces, enter the **show class-of-service interfaces interface-name** command.

Related Documentation

- [Configuring Classifiers and Rewrite Rules at the Global and Physical Interface Levels on page 30](#)

CHAPTER 2

BA Classifier Default Values

- [Default IP Precedence Classifier \(ipprec-compatibility\) on page 11](#)
- [Default MPLS EXP Classifier on page 12](#)
- [Enabling Default DSCP and DSCP IPv6 Classifiers on page 12](#)
- [Default IEEE 802.1p Classifier on page 14](#)
- [Default IEEE 802.1ad Classifier on page 15](#)
- [Default IP Precedence Classifier \(ipprec-default\) on page 16](#)

Default IP Precedence Classifier (ipprec-compatibility)

By default, all logical interfaces are automatically assigned an implicit IP precedence classifier called **ipprec-compatibility**. The **ipprec-compatibility** IP precedence classifier maps IP precedence bits to forwarding classes and loss priorities, as shown in [Table 3 on page 11](#).

Table 3: Default IP Precedence Classifier

IP Precedence CoS Values	Forwarding Class	Loss Priority
000	best-effort	low
001	best-effort	high
010	best-effort	low
011	best-effort	high
100	best-effort	low
101	best-effort	high
110	network-control	low
111	network-control	high

Default MPLS EXP Classifier

For all PICs except PICs mounted on Juniper Networks M Series Multiservice Edge Router standard (nonenhanced) FPCs, if you enable the MPLS protocol family on a logical interface, the default MPLS EXP classifier is automatically applied to that logical interface.

To configure code point aliases for MPLS EXP CoS markers, map alias names to bit patterns at the **[edit class-of-service code-point-aliases exp]** hierarchy level.

Table 4 on page 12 lists the default MPLS classifier mapping of EXP bits to forwarding classes and loss priorities.

Table 4: Default MPLS Classifier

Code Point	Forwarding Class	Loss Priority
000	best-effort	low
001	best-effort	high
010	expedited-forwarding	low
011	expedited-forwarding	high
100	assured-forwarding	low
101	assured-forwarding	high
110	network-control	low
111	network-control	high

- Related Documentation**
- *Default CoS Value Aliases Overview*
 - *code-point-aliases*

Enabling Default DSCP and DSCP IPv6 Classifiers

To enable the default DiffServ code point (DSCP) classifier, include the **default** statement at the **[edit class-of-service interfaces *interface-name* unit *unit-number* classifiers dscp]** hierarchy level.

To enable the default DSCP IPv6 classifier, include the **default** statement at the **[edit class-of-service interfaces *interface-name* unit *unit-number* classifiers dscp-ipv6]** hierarchy level.



NOTE: If you deactivate or delete the `dscp-ipv6` statement from the configuration, the default IPv6 classifier is not activated on the M5, M10, M7i, M10i, M20, M40, M40e, and M160 routing platforms. As a workaround, explicitly specify the default option to the `dscp-ipv6` statement.

Table 5 on page 13 shows the forwarding class and packet loss priority (PLP) that are assigned to each well-known DSCP when you apply the explicit default DSCP or DSCP IPv6 classifier.

Table 5: Default DSCP Classifier

DSCP and DSCP IPv6	Forwarding Class	PLP
ef	expedited-forwarding	low
af11	assured-forwarding	low
af12	assured-forwarding	high
af13	assured-forwarding	high
af21	best-effort	low
af22	best-effort	low
af23	best-effort	low
af31	best-effort	low
af32	best-effort	low
af33	best-effort	low
af41	best-effort	low
af42	best-effort	low
af43	best-effort	low
be	best-effort	low
cs1	best-effort	low
cs2	best-effort	low
cs3	best-effort	low
cs4	best-effort	low

Table 5: Default DSCP Classifier (*continued*)

DSCP and DSCP IPv6	Forwarding Class	PLP
cs5	best-effort	low
nc1/cs6	network-control	low
nc2/cs7	network-control	low
other	best-effort	low

- Related Documentation**
- [Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic on page 4](#)
 - [Default CoS Value Aliases Overview](#)
 - [Changing the Default Queuing and Marking of Host Outbound Traffic](#)
 - [classifiers \(Logical Interface\) on page 48](#)

Default IEEE 802.1p Classifier

Table 6 on page 14 shows the forwarding class and PLP that are assigned to the IEEE 802.1p CoS bits when you apply the explicit default IEEE 802.1p classifier. To do this, include the **default** statement at the `[edit class-of-service interfaces interface-name unit logical-unit-number classifiers ieee-802.1]` hierarchy level:



NOTE: Only the IEEE 802.1p classifier is supported in Layer 2 interfaces. You must explicitly apply this classifier as shown.

```
[edit class-of-service interfaces interface-name unit logical-unit-number classifiers
  ieee-802.1]
default;
```

Table 6: Default IEEE 802.1p Classifier

Code Point	Forwarding Class	PLP
000	best-effort	low
001	best-effort	high
010	expedited-forwarding	low
011	expedited-forwarding	high
100	assured-forwarding	low
101	assured-forwarding	high

Table 6: Default IEEE 802.1p Classifier (*continued*)

Code Point	Forwarding Class	PLP
110	network-control	low
111	network-control	high

Default IEEE 802.1ad Classifier

Table 7 on page 15 shows the code point, forwarding class alias, and PLP that are assigned to the IEEE 802.1ad bits when you apply the explicit default IEEE 802.1ad classifier. The table is very similar to the IEEE 802.1p default table, but the loss priority is determined by the DEI bit. To apply the default table, include the **default** statement at the `[edit class-of-service interfaces interface-name unit logical-unit-number classifiers ieee-802.1]` hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number classifiers
  ieee-802.1ad]
  default;
```

Table 7: Default IEEE 802.1ad Classifier

IEEE 802.1ad Code Point	Forwarding Class Alias	PLP
0000	be	low
0010	be1	low
0100	ef	low
0110	ef1	low
1000	af11	low
1010	af12	low
1100	nc1	low
1110	nc2	low
0001	be-dei	high
0011	be1-dei	high
0101	ef-dei	high
0111	ef1-dei	high
1001	af11-dei	high

Table 7: Default IEEE 802.1ad Classifier (*continued*)

IEEE 802.1ad Code Point	Forwarding Class Alias	PLP
1011	af12-dei	high
1101	nc1-dei	high
1111	nc2-dei	high

Default IP Precedence Classifier (ipprec-default)

There are two separate tables for default IP precedence classification. All logical interfaces are implicitly assigned the **ipprec-compatibility** classifier by default, as described in [Table 3 on page 11](#).

The other default IP precedence classifier (called **ipprec-default**) overrides the **ipprec-compatibility** classifier when you explicitly associate it with a logical interface. To do this, include the **default** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number* classifiers inet-precedence]** hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number classifiers
  inet-precedence]
  default;
```

[Table 8 on page 16](#) shows the forwarding class and PLP that are assigned to the IP precedence CoS bits when you apply the default IP precedence classifier.

Table 8: Default IP Precedence (ipprec-default) Classifier

Code Point	Forwarding Class	PLP
000	best-effort	low
001	assured-forwarding	low
010	best-effort	low
011	best-effort	low
100	best-effort	low
101	expedited-forwarding	low
110	network-control	low
111	network-control	high

PART 2

Configuration

- [Configuration Tasks for Classifiers on page 19](#)
- [Configuration Tasks for BA Classifiers on page 29](#)
- [Configuration Task for DSCP IPv6 Classifiers on page 33](#)
- [Configuration Tasks for MPLS EXP Classifiers on page 35](#)
- [Configuration Task for IEEE 802.1ad Classifiers on page 41](#)
- [Configuration Statements on page 43](#)

CHAPTER 3

Configuration Tasks for Classifiers

- [Defining Classifiers on page 19](#)
- [Applying Classifiers to Logical Interfaces on page 20](#)
- [DSCP Classifier Configuration Examples on page 24](#)
- [Managing Congestion by Setting Packet Loss Priority for Different Traffic Flows on page 26](#)

Defining Classifiers

You can override the default IP precedence classifier by defining a classifier and applying it to a logical interface. To define new classifiers for all code point types, include the **classifiers** statement at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
classifiers {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) classifier-name {
    import [classifier-name | default];
    forwarding-class class-name {
      loss-priority level code-points [ aliases ] [ bit-patterns ];
    }
  }
}
```

The map sets the forwarding class and PLP for a specific set of code-point aliases and bit patterns. The inputs of the map are code-point aliases and bit patterns. The outputs of the map are the forwarding class and the PLP. For more information about how CoS maps work, see *Mapping CoS Component Inputs to Outputs*.

The classifiers work as follows:

- **dscp**—Handles incoming IPv4 packets.
- **dscp-ipv6**—Handles incoming IPv6 packets. For more information, see [“Applying DSCP IPv6 Classifiers” on page 33](#).
- **exp**—Handles MPLS packets using Layer 2 headers.
- **ieee-802.1**—Handles Layer 2 CoS.
- **inet-precedence**—Handles incoming IPv4 packets. IP precedence mapping requires only the upper three bits of the DSCP field.

A classifier takes a specified bit pattern as either the literal pattern or as a defined alias and attempts to match it to the type of packet arriving on the interface. If the information in the packet's header matches the specified pattern, the packet is sent to the appropriate queue, defined by the forwarding class associated with the classifier.

The code-point aliases and bit patterns are the input for the map. The loss priority and forwarding class are outputs of the map. In other words, the map sets the PLP and forwarding class for a given set of code-point aliases and bit patterns.



NOTE: On M Series, MX Series, and T Series routers, and EX Series switches that do not have tricolor marking enabled, the loss priority can be configured only by setting the PLP within a multifield classifier. This setting can then be used by the appropriate drop profile map and rewrite rule. For more information, see [“Managing Congestion by Setting Packet Loss Priority for Different Traffic Flows”](#) on page 26.

Importing a Classifier

You can use any table, including the default, in the definition of a new classifier by including the **import** statement. The imported classifier is used as a template and is not modified. Whenever you commit a configuration that assigns a new **class-name** and **loss-priority** value to a code-point alias or set of bits, it replaces that entry in the imported classifier template. As a result, you must explicitly specify every CoS value in every designation that requires modification.

To do this, include the **import default** statement at the **[edit class-of-service classifiers type classifier-name]** hierarchy level:

```
[edit class-of-service classifiers type classifier-name]
import default;
```

For instance, to import the default DSCP classifier, include the **dscp default** statement at the **[edit class-of-service classifiers dscp classifier-name]** hierarchy level:

```
[edit class-of-service classifiers dscp classifier-name]
import default;
```

Applying Classifiers to Logical Interfaces

To apply the classification map to a logical interface:

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
user@host#set classifiers (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence)
(classifier-name | default);
```

You can use interface wildcards for **interface-name** and **logical-unit-number**.

For most PICs, if you apply an IEEE 802.1 classifier to a logical interface, you cannot apply non-IEEE classifiers to other logical interfaces on the same physical interface. This restriction does not apply to Gigabit Ethernet IQ2 PICs.

There are some restrictions on applying multiple BA classifiers to a single logical interface. [Table 9 on page 21](#) shows the supported combinations. In this table, the OSE PICs refer to the 10-port 10-Gigabit OSE PICs.

Table 9: Logical Interface Classifier Combinations

Classifier Combinations	Gigabit Ethernet IQ2 PICs	OSE PICs	Other PICs on M320, MX Series, T Series routers and on EX Series Switches	Other M Series with Regular FPCs	Other M Series with Enhanced FPCs
dscp and inet-precedence	No	No	No	No	No
dscp-ipv6 and (dscp inet-precedence)	Yes	Yes	Yes	No	No
exp and ieee 802.1	Yes	Yes	No	No	No
ieee 802.1 and (dscp dscp-ipv6 exp inet-precedence)	Yes	Yes	No	No	Yes
exp and (dscp dscp-ipv6 inet-precedence)	Yes	Yes	Yes	No	Yes

For Gigabit Ethernet IQ2 and 10-port 10-Gigabit Oversubscribed Ethernet (OSE) interfaces, family-specific classifiers take precedence over IEEE 802.1p BA classifiers. For example, if you configure a logical interface to use both an MPLS EXP and an IEEE 802.1p classifier, the EXP classifier takes precedence. MPLS-labeled packets are evaluated by the EXP classifier, and all other packets are evaluated by the IEEE 802.1p classifier. The same is true about other classifiers when combined with IEEE 802.1p classifiers on the same logical interface.

In Junos OS Releases 9.6 and later, the DSCP and IPv6 DSCP classifiers are not compatible with older formats. You cannot directly replace the old classifier with the new one. You must first delete the old classifier and then apply the new one, although both steps can be done in one configuration session. Otherwise, the commit will fail.



NOTE: If an interface is mounted on an M Series router FPC, you can apply only the default **exp** classifier. If an interface is mounted on an enhanced FPC, you can create a new **exp** classifier and apply it to an interface.

On MX960, MX480, MX240, MX80, M120, and M320 routers and EX Series switches with Enhanced Type III FPCs only, you can configure user-defined DSCP-based BA classification for MPLS interfaces (this feature is not available for IQE PICs or on MX Series routers and EX Series switches when ingress queuing is used) or VPLS/L3VPN routing instances (LSI interfaces). The DSCP-based classification for MPLS packets for Layer 2 VPNs is not supported. To classify MPLS packets on the routing instance at the egress PE, include the **dscp** or **dscp-ipv6** statements at the **[edit class-of-service routing-instances**

routing-instance-name classifiers] hierarchy level. To classify MPLS packets at the core-facing interface, apply the classifier at the [*edit class-of-service interface interface-name unit unit-name classifiers (dscp | dscp-ipv6) classifier-name family mpls*] hierarchy level.



NOTE: If you do not apply a DSCP classifier, the default EXP classifier is applied to MPLS traffic.

You can apply DSCP classification for MPLS traffic in the following usage scenarios:

- In a Layer 3 VPN (L3VPN) using an LSI routing instance.
 - Supported on the M120, M320, MX960, MX480, MX240, and MX80 routers.
 - DSCP classifier configured under [*edit class-of-service routing-instances*] on the egress PE router.
- In VPLS using an LSI routing instance.
 - Supported on the M120, M320, MX960, MX480, MX240, and MX80 routers.
 - DSCP classifier configured under [*edit class-of-service routing-instances*] on the egress PE router.
- In a Layer 3 VPN (L3VPN) using a VT routing instance.
 - Supported on the M120, M320, MX960, MX480, MX240, and MX80 routers.
 - DSCP classifier configured under [*edit class-of-service interfaces*] on the core-facing interface on the egress PE router.
- In VPLS using the VT routing instance.
- MPLS forwarding.
 - Supported on the M120, M320, MX960, MX480, MX240, and MX80 routers (not supported on IQE and MX when ingress queuing is enabled).
 - DSCP classifier configured under [*edit class-of-service interfaces*] on the ingress core-facing interface on the P or egress PE router.

MPLS forwarding when the label stacking is greater than 2 is not supported:

The following example configures a DSCP classifier for IPv4 named **dscp-ipv4-classifier** for the **fc-af11-class** forwarding class and a corresponding IPv6 DSCP classifier:

```
class-of-service {
  routing-instances routing-instance-one {
    classifiers {
      dscp dscp-ipv4-classifier {
        loss-priority low code-points 000100;
      }
      dscp dscp-ipv6-classifier {
        forwarding-class fc-af11-class {
          loss-priority low {
```

```

        code-points af11;
    }
}
}
}
}
}

```



NOTE: This is not a complete configuration.

This example applies the IPv4 classifier to MPLS traffic and the IPv6 classifier to Internet traffic on interface **ge-2/0/3.0**:

```

class-of-service {
  interfaces ge-2/0/3 {
    unit 0 {
      classifiers {
        dscp dscp-ipv4-classifier {
          family mpls;
        }
        dscp-ipv6 dscp-ipv6-classifier {
          family inet; # This is the default if not present.
        }
      }
    }
  }
}

```



NOTE: This is not a complete configuration.

This example applies the same classifier to both MPLS and IP traffic on interface **ge-2/2/0**.

```

[edit class-of-services interface ge-2/2/0]
unit 0 {
  classifiers {
    dscp dscp-mpls {
      family [ mpls inet ];
    }
  }
}

```



NOTE: This is not a complete configuration.



NOTE: You can apply DSCP and DSCP IPv6 classifiers to explicit null MPLS packets. The **family mpls** statement works the same on both explicit null and non-null MPLS labels.

Related Documentation • [DSCP Classifier Configuration Examples on page 24](#)

DSCP Classifier Configuration Examples

On MX960, MX480, MX240, MX80, M120, and M320 routers with Enhanced Type III FPCs and EX Series switches only, you can configure user-defined DSCP-based BA classification for MPLS interfaces (this feature is not available for IQE PICs or on MX Series routers or EX Series switches when ingress queuing is used) or VPLS/L3VPN routing instances (LSI interfaces). The following examples show how you can apply DSCP classifiers for MPLS traffic in these cases.

Applying a DSCP Classifier to MPLS Packets on the Core-facing Interface

Configure the core-facing interface and associated logical interfaces:

```
interfaces ge-5/3/1 {
  unit 0 {
    family inet {
      address 1.1.1.1/24;
    }
    family iso;
    family inet6 {
      address 2000::1/64;
    }
    family mpls
  }
}
```

Configure the DSCP classifier.

```
class-of-service {
  classifiers {
    dscp dscp11 {
      forwarding-class expedited-forwarding {
        loss-priority low code-points [ ef cs5 ];
      }
      forwarding-class assured-forwarding {
        loss-priority low code-points [ af21 af31 af41 cs4 ];
        loss-priority high code-points [ af23 af33 af43 cs2 af22 af32 af42 cs3 ];
      }
      forwarding-class best-effort {
        loss-priority low code-points [ af11 cs1 af12 ];
        loss-priority high code-points af13;
      }
      forwarding-class network-control {
        loss-priority low code-points [ cs6 cs7 ];
      }
    }
  }
}
```

Attach the classifier to the logical interface for the mpls family. You cannot configure more than one classifier per family.

```
class-of-service {
  interfaces {
    ge-5/3/1 {
```

```

unit 0 {
  classifiers {
    dscp dscp11 {
      family mpls;
    }
  }
}

```

The above classifiers are applicable on egress PE routers for VPLS and L3VPN cases. For plain interfaces (not VPLS/L3VPN (LSI) interfaces), these classifiers are applicable on P and egress PE routers on core facing interfaces.

Applying a DSCP Classifier to MPLS Traffic for L3VPN/VPLS

Configure routing instances of type either vrf or vpls.

```

routing-instances {
  vpls1 {
    instance-type vpls;
    interface ge-2/2/2.0; #customer facing interface for VPLS
    route-distinguisher 10.255.245.51:1;
    vrf-target target:1234:1;
    protocols {
      vpls {
        site-range 10;
        no-tunnel-services;
        site vpls-1-site-1 {
          site-identifier 1;
        }
      }
    }
  }
}

```

Configure the DSCP classifier.

```

class-of-service {
  classifiers {
    dscp dscp11 {
      forwarding-class expedited-forwarding {
        loss-priority low code-points [ ef cs5 ];
      }
      forwarding-class assured-forwarding {
        loss-priority low code-points [ af21 af31 af41 cs4 ];
        loss-priority high code-points [ af23 af33 af43 cs2 af22 af32 af42 cs3 ];
      }
      forwarding-class best-effort {
        loss-priority low code-points [ af11 cs1 af12 ];
        loss-priority high code-points af13;
      }
      forwarding-class network-control {
        loss-priority low code-points [ cs6 cs7 ];
      }
    }
  }
}

```

Attach the classifier to a routing instance. You cannot configure more than one classifier per routing instance.

```
class-of-service {
  routing-instances {
    vpls1 {
      classifiers {
        dscp dscp11;
      }
    }
  }
}
```

Related Documentation • [Applying Classifiers to Logical Interfaces on page 20](#)

Managing Congestion by Setting Packet Loss Priority for Different Traffic Flows

By default, the least significant bit of the CoS value sets the packet loss priority (PLP) value. For example, CoS value 000 is associated with PLP **low**, and CoS value 001 is associated with PLP **high**. In general, you can change the PLP by configuring a behavior aggregate (BA) or multifield classifier, as discussed in [“Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic” on page 4](#) and [Overview of Assigning Service Levels to Packets Based on Multiple Packet Header Fields](#).

However, on Juniper Networks M320 Multiservice Edge Routers, MX Series 3D Universal Edge Routers, and T Series Core Routers and EX Series switches that do not have tricolor marking enabled, the loss priority can be configured by setting the PLP within a multifield classifier or by behavior aggregate (BA) classifier. This setting can then be used by the appropriate drop profile map and rewrite rule.

On M320 routers and T Series routers with Enhanced II Flexible PIC Concentrators (FPCs) and tricolor marking enabled, you can set the PLP with a BA or multifield classifier, as described in [Using BA Classifiers to Set PLP](#) and [Using Multifield Classifiers to Set Packet Loss Priority](#).

On T Series routers with different Packet Forwarding Engines (non-Enhanced Scaling and Enhanced Scaling FPCs), you can configure PLP bit copying for ingress and egress unicast and multicast traffic. To configure, include the [copy-plp-all](#) statement at the [\[edit class-of-service\]](#) hierarchy level.

Example: Overriding the Default PLP on M320 Routers

The following example shows a two-step procedure to override the default PLP settings on M320 routers:

1. The following example specifies that while the DSCP code points are 110, the loss priority is set to **high**; however, on M320 routers, overriding the default PLP this way has no effect.

```
class-of-service {
  classifiers {
    dscp ba-classifier {
```



```

        forwarding-class expedited-forwarding {
            loss-priority high code-points 110;
        }
    }
}

```

2. For M320 routers, this multifield classifier sets the PLP.

```

firewall {
  filter ef-filter {
    term ef-multifield {
      from {
        precedence 6;
      }
      then {
        loss-priority high;
        forwarding-class expedited-forwarding;
      }
    }
  }
}

```

Mapping PLP to RED Drop Profiles

Loss priority settings help determine which packets are dropped from the network during periods of congestion. The software supports multiple packet loss priority (PLP) designations: **low** and **high**. (In addition, **medium-low** and **medium-high** PLPs are supported when you configure tricolor marking.) You can set PLP by configuring a behavior aggregate or multifield classifier.

A drop-profile map examines the loss priority setting of an outgoing packet: **high**, **medium-high**, **medium-low**, **low**, or any.

Obviously, *low*, *medium-low*, *medium-high*, and *high* are relative terms, which by themselves have no meaning. Drop profiles define the meanings of the loss priorities. In the following example, the **low-drop** drop profile defines the meaning of **low** PLP as a 10 percent drop probability when the fill level is 75 percent and a 40 percent drop probability when the fill level is 95 percent. The **high-drop** drop profile defines the meaning of **high** PLP as a 50 percent drop probability when the fill level is 25 percent and a 90 percent drop probability when the fill level is 50 percent.

In this example, the scheduler includes two drop-profile maps, which specify that packets are evaluated by the **low-drop** drop profile if they have a **low** loss priority and are from any protocol. Packets are evaluated by the **high-drop** drop profile if they have a **high** loss priority and are from any protocol.

```

[edit class-of-service]
drop-profiles {
  low-drop {
    interpolate {
      drop-probability [ 10 40];
      fill-level [ 75 95];
    }
  }
}

```

```
    }
    high-drop {
      interpolate {
        drop-probability [ 50 90];
        fill-level [ 25 50];
      }
    }
  }
  schedulers {
    best-effort {
      drop-profile-map loss-priority low protocol any drop-profile low-drop;
      drop-profile-map loss-priority high protocol any drop-profile high-drop;
    }
  }
}
```

**Related
Documentation**

- *Defining Packet Drop Behavior by Configuring RED Drop Profiles*
- *Determining Packet Drop Behavior by Configuring Drop Profile Maps for Schedulers*
- *Configuring Schedulers*

CHAPTER 4

Configuration Tasks for BA Classifiers

- [DSCP IPv6 Rewrites and Forwarding Class Maps on page 29](#)
- [Tunneling and BA Classifiers on page 30](#)
- [Configuring Classifiers and Rewrite Rules at the Global and Physical Interface Levels on page 30](#)

DSCP IPv6 Rewrites and Forwarding Class Maps

You cannot configure a DSCP IPv6 rewrite rule and output forwarding class map on the same logical interface (unit). These must be used on different logical interfaces. Although a warning is issued, there is nothing in the CLI that prevents this configuration. An error message appears when you attempt to commit the configuration.

This example shows the warning and error message that results when the default DSCP IPv6 rewrite rule is configured on logical interface **ge-1/0/4.0** with output forwarding class map **vg1**.

```
[edit class-of-service]
interfaces {
  ge-1/0/4 {
    unit 0 {
      ##
      ## Warning: DSCP-IPv6 rewrite and forwarding class map not allowed on same unit
      ##
      output-forwarding-class-map vg1;
      rewrite-rules {
        dscp-ipv6 default;
      }
    }
  }
}

user@router# commit
[edit class-of-service interfaces ge-1/0/4 unit 0 output-forwarding-class-map]
'output-forwarding-class-map vg1'
DSCP-IPv6 rewrite and forwarding class map not allowed on same unit
error: commit failed: (statements constraint check failed)
```

Related Documentation

- [Applying Forwarding Classes to Interfaces](#)

Tunneling and BA Classifiers

BA classifiers can be used with GRE and IP-IP tunnels on the following routers and switches:

- EX Series switches
- M7i and M10i routers
- M Series routers with E-FPC or EP-FPC
- M120 routers
- M320 routers
- T Series routers

When a GRE or IP-IP tunnel is configured on an incoming (core-facing) interface, the queue number and PLP information are carried through the tunnel. At the egress (customer-facing) interface, the packet is queued and the CoS bits rewritten based on the information carried through the tunnel.

If no BA classifier is configured in the incoming interface, the default classifier is applied. If no rewrite rule is configured, the default rewrite rule is applied.

Configuring Classifiers and Rewrite Rules at the Global and Physical Interface Levels

On ACX Series Universal Access Routers and EX Series switches, CoS supports classification and rewrite at the global and physical interface levels.

To configure the global EXP classifier, include the following statements at the **[edit class-of-service] system-defaults** hierarchy level.

```
[edit class-of-service]
{
  system-defaults
  {
    classifiers exp classifier-name
  }
}
```

CoS supports one global system default classifier of the EXP type, as shown in the following example:

```
[edit class-of-service]
{
  system-defaults {
    classifiers {
      exp exp-classf-core;
    }
  }
}
```

To configure classifiers and rewrite rules at the physical interface level, include the following statements at the **[edit class-of-service] interfaces** hierarchy level.

```
[edit class-of-service]
interfaces {
  interface-name
    classifiers dscp classifier-name
    classifiers inet-precedence classifier-name
    classifiers ieee-802.1 [vlan-tag (outer | inner)] classifier-name
    rewrite-rules dscp rewrite-name
    rewrite-rules inet-prec rewrite-name
    rewrite-rules ieee-802.1 rewrite-name
}
```

The following example shows classifiers and rewrite rules configured on physical interfaces:

```
ge-0/1/0 {
  unit 0 {
    rewrite-rules {
      exp custom-exp;
    }
  }
  classifiers {
    dscp d1;
    ieee-802.1 ci;
  }
  rewrite-rules {
    dscp default;
  }
}
ge-0/1/2 {
  classifiers {
    ieee-802.1 ci;
  }
  rewrite-rules {
    ieee-802.1 ri;
  }
}
ge-0/1/3 {
  unit 0 {
    rewrite-rules {
      exp custom-exp2;
    }
  }
}
ge-0/1/7 {
  classifiers {
    dscp d1;
  }
}
ge-0/1/8 {
  classifiers {
    dscp d1;
  }
}
```

Related Documentation

- [Classifiers and Rewrite Rules at the Global and Physical Interface Levels Overview on page 9](#)

CHAPTER 5

Configuration Task for DSCP IPv6 Classifiers

- [Applying DSCP IPv6 Classifiers on page 33](#)

Applying DSCP IPv6 Classifiers

For M320 and T Series routers and EX Series switches, you can apply separate classifiers for IPv4 and IPv6 packets per logical interface by including the **classifiers** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]** hierarchy level and specifying the **dscp** and **dscp-ipv6** classifier types:

```
[edit class-of-service interfaces interface-name unit logical-unit-number]  
  classifiers dscp (classifier-name | default) family (mpls | inet);  
  classifiers dscp-ipv6 (classifier-name | default) family (mpls | inet));
```

For M Series router enhanced FPCs, you cannot apply separate classifiers for IPv4 and IPv6 packets on a single logical interface. Instead, classifier assignment works as follows:

- If you assign a DSCP classifier only, IPv4 and IPv6 packets are classified using the DSCP classifier.
- If you assign an IP precedence classifier only, IPv4 and IPv6 packets are classified using the IP precedence classifier. In this case, the lower three bits of the DSCP field are ignored because IP precedence mapping requires the upper three bits only.
- If you assign either the DSCP or the IP precedence classifier in conjunction with the DSCP IPv6 classifier, the commit fails.
- If you assign a DSCP IPv6 classifier only, IPv4 and IPv6 packets are classified using the DSCP IPv6 classifier, but the commit displays a warning message.

For more information, see [“Applying Classifiers to Logical Interfaces” on page 20](#).

Configuration Tasks for MPLS EXP Classifiers

- [Applying MPLS EXP Classifiers to Routing Instances on page 35](#)
- [Applying MPLS EXP Classifiers for Explicit-Null Labels on page 39](#)

Applying MPLS EXP Classifiers to Routing Instances

When you enable VRF table labels and you do not explicitly apply a classifier configuration to the routing instance, the default MPLS EXP classifier is applied to the routing instance. For detailed information about VRF table labels, see the *Junos OS VPNs Library for Routing Devices*.

The default MPLS EXP classification table contents are shown in [Table 10 on page 35](#).

Table 10: Default MPLS EXP Classifier

Forwarding Class	Loss Priority	CoS Value
best-effort	low	000
best-effort	high	001
expedited-forwarding	low	010
expedited-forwarding	high	011
assured-forwarding	low	100
assured-forwarding	high	101
network-control	low	110
network-control	high	111

For PICs that are installed on enhanced FPCs, you can override the default MPLS EXP classifier and apply a custom classifier to the routing instance. To do this, perform the following configuration tasks:

1. Filter traffic based on the IP header by including the **vrf-table-label** statement at the **[edit routing-instances *routing-instance-name*]** hierarchy level:

```
[edit routing-instances routing-instance-name]
vrf-table-label;
```

2. Configure a custom MPLS EXP classifier by including the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
classifiers {
  exp classifier-name {
    import (classifier-name | default);
    forwarding-class class-name {
      loss-priority level code-points [ aliases ] [ bit-patterns ];
    }
  }
}
forwarding-classes {
  queue queue-number class-name priority (high | low);
}
```

3. Configure the routing instance to use the custom MPLS EXP classifier by including the **exp** statement at the **[edit class-of-service routing-instances *routing-instance-name* classifiers]** hierarchy level:

```
[edit class-of-service routing-instances routing-instance-name classifiers]
exp classifier-name;
```

To display the MPLS EXP classifiers associated with all routing instances, issue the **show class-of-service routing-instances** command.



NOTE: The following caveats apply to custom MPLS EXP classifiers for routing instances:

- An enhanced FPC is required.
- Logical systems are not supported.

For more details, see the following sections:

- [Configuring Global Classifiers and Wildcard Routing Instances on page 36](#)
- [Examples: Applying MPLS EXP Classifiers to Routing Instances on page 37](#)

Configuring Global Classifiers and Wildcard Routing Instances

To configure a global routing instance classifier, include the **all** statement at the **[edit class-of-service routing-instances]** hierarchy level:

```
[edit class-of-service routing-instances]
all {
  classifiers {
    exp classifier-name;
  }
}
```

```
}
```

For routing instances associated with specific classifiers, the global configuration is ignored.

To use a wildcard in the routing instance classifier configuration, include an asterisk (*) in the name of the routing instance:

```
[edit class-of-service routing-instances]
routing-instance-name* {
  classifiers {
    exp classifier-name;
  }
}
```

The wildcard configuration follows the longest match. If there is a specific configuration, it is given precedence over the wildcard configuration.



NOTE: Wildcards and the `all` keyword are supported at the `[edit class-of-service routing-instances]` hierarchy level but not at the `[edit routing-instances]` hierarchy level.

If you configure a routing instance at the `[edit routing-instances]` hierarchy level with, for example, the name `vpn*`, the Junos OS treats `vpn*` as a valid and distinct routing instance name. If you then try to apply a classifier to the `vpn*` routing instance at the `[edit class-of-service routing-instances]` hierarchy level, the Junos OS treats the `vpn*` routing instance name as a wildcard, and all the routing instances that start with `vpn` and do not have a specific classifier applied receive the classifier associated with `vpn*`. This same behavior applies with the `all` keyword.

Examples: Applying MPLS EXP Classifiers to Routing Instances

Configure a global classifier for all routing instances and override the global classifier for a specific routing instance. In this example, there are three routing instances: `vpn1`, `vpn2`, and `vpn3`, each with VRF table label enabled. The classifier `exp-classifier-global` is applied to `vpn1` and `vpn2` (that is, all but `vpn3`, which is listed separately). The classifier `exp-classifier-3` is applied to `vpn3`.

Configuring a Global Classifier

```
[edit routing-instances]
vpn1 {
  vrf-table-label;
}
vpn2 {
  vrf-table-label;
}
vpn3 {
  vrf-table-label;
}

[edit class-of-service routing-instances]
all {
```

```

        classifiers {
            exp exp-classifier-global;
        }
    }
    vpn3 {
        classifiers {
            exp exp-classifier-3;
        }
    }
}

```

Configure a wildcard routing instance and override the wildcard with a specific routing instance. In this example, there are three routing instances: **vpn-red**, **vpn-yellow**, and **vpn-green**, each with VRF table label enabled. The classifier **exp-class-wildcard** is applied to **vpn-yellow** and **vpn-green**. The classifier **exp-class-red** is applied to **vpn-red**.

Configuring a Wildcard Routing Instance

```

[edit routing-instances]
vpn-red {
    vrf-table-label;
}
vpn-yellow {
    vrf-table-label;
}
vpn-green {
    vrf-table-label;
}

[edit class-of-service routing-instances]
vpn* {
    classifiers {
        exp exp-class-wildcard;
    }
}
vpn-red {
    classifiers {
        exp exp-class-red;
    }
}

```

Display the MPLS EXP classifiers associated with two routing instances:

Monitoring a Configuration

```

[edit class-of-service routing-instances]
vpn1 {
    classifiers {
        exp default;
    }
}
vpn2 {
    classifiers {
        exp class2;
    }
}

```

```
user@host> show class-of-service routing-instances
```

Routing Instance : vpn1			
Object	Name	Type	Index
Classifier	exp-default	exp	8

Routing Instance :	vpn2		
Object	Name	Type	Index
Classifier	class2	exp	57507

Applying MPLS EXP Classifiers for Explicit-Null Labels

When you configure MPLS explicit-null labels, label 0 is advertised to the egress router of an LSP. When label 0 is advertised, the egress router (instead of the penultimate router) removes the label. Ultimate-hop popping ensures that any packets traversing an MPLS network include a label. For more information about explicit-null labels and ultimate-hop popping, see the *MPLS Applications Feature Guide for Routing Devices*.

On M320 and T Series routers, when you configure MPLS explicit-null labels with an MPLS EXP classifier, the MPLS EXP classifier can be different from an IPv4 or IPv6 classifier configured on the same logical interface. In other words, you can apply separate classifiers for MPLS EXP, IPv4, and IPv6 packets per logical interface. To combine an EXP classifier with a distinct IPv6 classifier, the PIC must be mounted on an Enhanced FPC.



NOTE: For M Series routers, MPLS explicit-null labels with MPLS EXP classification are supported if you set the same classifier for EXP and IPv4 traffic, or EXP and IPv6 traffic.

For more information about how IPv4 and IPv6 packet classification is handled, see [“Applying DSCP IPv6 Classifiers” on page 33](#).

To configure an MPLS EXP classifiers for explicit-null labels, include the **exp** statement at the [edit class-of-service classifiers] and [edit class-of-service interfaces *interface-name* unit *logical-unit-number* classifiers] hierarchy levels:

```
[edit class-of-service classifiers]
exp classifier-name {
  import (classifier-name | default);
  forwarding-class class-name {
    loss-priority level code-points [ aliases ] [ bit-patterns ];
  }
}
[edit class-of-service interfaces interface-name unit logical-unit-number classifiers]
exp (classifier-name | default);
```


CHAPTER 7

Configuration Task for IEEE 802.1ad Classifiers

- [Configuring and Applying IEEE 802.1ad Classifiers on page 41](#)

Configuring and Applying IEEE 802.1ad Classifiers

For Juniper Networks MX Series 3D Universal Edge Router interfaces or IQ2 PICs with IEEE 802.1ad frame formats or EX Series switches, you can set the forwarding class and loss priority for traffic on the basis of the three IEEE 802.1p bits and the DEI bit. You can apply the default map or customize one or more of the default values.

You then apply the classifier to the interface on which you configure IEEE 802.1ad frame formats.

Defining Custom IEEE 802.1ad Maps

You can customize the default IEEE 802.1ad map by defining values for IEEE 802.1ad code points.

```
class-of-service {
  classifiers {
    ieee-802.1ad dot1p_dei_class {
      forwarding-class best-effort {
        loss-priority low code-points [ 0000 1101 ];
      }
    }
  }
}
```

Applying Custom IEEE 802.1ad Maps

You then apply the classifier map to the logical interface:

```
interfaces {
  ge-2/0/0 {
    unit 0 {
      classifiers {
        ieee-802.1ad dot1p_dei_class;
      }
    }
  }
}
```

}

Verifying Custom IEEE 802.1ad Map Configuration

To verify your configuration, you can issue the following operational mode commands:

- **show class-of-service forwarding-table loss-priority-map**
- **show class-of-service forwarding-table loss-priority-map mapping**
- **show chassis forwarding**
- **show pfe fwdd**

CHAPTER 8

Configuration Statements

- [\[edit class-of-service\] Hierarchy Level](#) on page 43
- [classifiers \(Logical Interface\)](#) on page 48
- [classifiers \(Routing Instance\)](#) on page 49
- [classifiers \(Definition\)](#) on page 50
- [classifiers \(Physical Interface\)](#) on page 51
- [code-points](#) on page 52
- [copy-plp-all](#) on page 52
- [dscp \(AS PIC Classifiers\)](#) on page 53
- [dscp \(CoS Interfaces\)](#) on page 53
- [dscp-ipv6 \(CoS Rewrite Rules\)](#) on page 54
- [exp](#) on page 55
- [forwarding-class \(BA Classifiers\)](#) on page 56
- [ieee-802.1 \(Rewrite Rules on Logical Interface\)](#) on page 57
- [ieee-802.1 \(Classifier on Physical Interface\)](#) on page 58
- [ieee-802.1ad](#) on page 59
- [import \(Classifiers\)](#) on page 60
- [inet-precedence \(CoS Rewrite Rules\)](#) on page 60
- [inet-precedence \(Classifier on Physical Interface\)](#) on page 61
- [interfaces \(CoS\)](#) on page 62
- [loss-priority \(BA Classifiers\)](#) on page 64
- [routing-instances \(CoS\)](#) on page 65
- [system-defaults](#) on page 66
- [unit](#) on page 67

[\[edit class-of-service\] Hierarchy Level](#)

```
class-of-service {  
  classifiers {  
    type classifier-name {  
      forwarding-class class-name {
```

```

        loss-priority (high | low | medium-high | medium-low) code-points [ aliases bits ];
    }
    import (classifier-name | default);
}
}
code-point-aliases {
    (dscp | dscp-ipv6 | exp | ieee-802.1 | ieee-802.1ad | inet-precedence) {
        alias-name bits;
    }
}
drop-profiles {
    profile-name {
        fill-level percentage drop-probability percentage;
        interpolate {
            drop-probability value;
            fill-level value;
        }
    }
}
fabric {
    scheduler-map {
        priority (high | low) scheduler scheduler-name;
    }
}
forwarding-class-map {
    map-name {
        class class-name queue-num queue-number <restricted-queue queue-number>;
    }
}
forwarding-classes {
    class class-name policing-priority (normal | premium) queue-num queue-number
        priority (high | low);
    queue queue-number class-name policing-priority (normal | premium) priority (high |
        low);
}
forwarding-policy {
    class class-name {
        classification-override {
            forwarding-class class-name;
        }
    }
    next-hop-map map-name {
        forwarding-class class-name {
            discard;
            lsp-next-hop [ lsp-regular-expressions ];
            next-hop [ next-hop-names ];
            non-lsp-next-hop;
        }
    }
}
fragmentation-maps {
    map-name {
        forwarding-class class-name {
            drop-timeout milliseconds;
            fragment-threshold bytes;
            multilink-class number;
        }
    }
}

```

```

        no-fragmentation;
    }
}
host-outbound-traffic {
    dscp-code-point value;
    forwarding-class class-name;
    ieee-802.1 {
        default value;
        rewrite-rules;
    }
    tcp {
        raise-internet-control-priority;
    }
}
interfaces {
    ... the interfaces subhierarchy appears after the main [edit class-of-service] hierarchy
    ...
}
restricted-queues {
    forwarding-class class-name queue-number;
}
rewrite-rules {
    (dscp | dscp-ipv6 | exp | frame-relay-de | ieee-802.1 | ieee-802.1ad | inet-precedence)
    rewrite-rule {
        forwarding-class class-name {
            loss-priority level code-point (alias | bits);
        }
        import (rewrite-rule | default);
    }
}
routing-instances routing-instance-name {
    classifiers {
        dscp (classifier-name | default);
        dscp-ipv6 (classifier-name | default);
        exp (classifier-name | default);
        ieee-208.1 (classifier-name | default | encapsulated | vlan-tag (inner | outer));
    }
}
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}
schedulers {
    scheduler-name {
        adjust-minimum value;
        adjust-percent value;
        buffer-size (exact | percent percentage | remainder);
        drop-profile-map loss-priority (any | high | low | medium-high | medium-low)
            protocol any;
        excess-priority (high | low | medium-high | medium-low);
        excess-rate (percent percentage | proportion proportion);
        priority (high | low | medium-high | medium-low | strict-high);
        shaping-rate (bps | percent percentage | burst-size size);
    }
}

```

```

        transmit-rate (bps | percent percentage | remainder) <exact | rate-limit>;
    }
}
traceoptions {
    file <files number> <match regular-expression> <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
traffic-control-profiles {
    profile-name {
        adjust-minimum rate;
        delay-buffer-rate (bps | cps cps | percent percentage);
        excess-rate (percent percentage | proportion value);
        guaranteed-rate (bps | percent percentage) <burst-size bytes>;
        overhead-accounting (frame-mode | cell-mode) <bytes byte-value>;
        scheduler-map map-name;
        shaping-rate (bps | percent percentage) <burst-size bytes>;
    }
}
tri-color;
}

class-of-service {
    interfaces {
        interface-name {
            excess-bandwidth-share (equal | proportional value);
            input-excess-bandwidth-share (equal | proportional value);
            input-scheduler-map map-name;
            input-shaping-rate bps;
            input-traffic-control-profile profile-name;
            output-forwarding-class-map map-name;
            output-traffic-control-profile profile-name;
            scheduler-map map-name;
            scheduler-map-chassis (map-name | derived);
            shaping-rate bps;
            unit (logical-unit-number | *) {
                classifiers {
                    dscp (classifier-name | default) {
                        family [ inet mpls ];
                    }
                    dscp-ipv6 (classifier-name | default) {
                        family [ inet mpls ];
                    }
                    exp (classifier-name | default);
                    ieee-208.1 (classifier-name | default) <vlan-tag (inner | outer)>;
                    ieee-208.1ad (classifier-name | default);
                    inet-precedence (classifier-name | default);
                }
                forwarding-class class-name;
                input-scheduler-map map-name;
                input-shaping-rate bps;
                input-traffic-control-profile profile-name shared-instance instance-name;
                loss-priority-maps {
                    (map-name | default);
                }
            }
        }
    }
}

```

```


    loss-priority-rewrites {
        (map-name | default);
    }
    output-forwarding-class-map map-name;
    output-traffic-control-profile profile-name shared-instance instance-name;
    rewrite-rules {
        dscp (rule-name | default) <protocol mpls>;
        dscp-ipv6 (rule-name | default);
        exp (rule-name | default) <protocol [ mpls-any | mpls-inet-both |
            mpls-inet-both-non-vpn ]>;
        exp-push-push-push default;
        exp-swap-push-push default;
        ieee-802.1 (rewrite-name | default) <vlan-tag (outer | outer-and-inner)>;
        ieee-802.1ad (rewrite-name | default) <vlan-tag (outer | outer-and-inner)>;
        inet-precedence (rewrite-name | default) <protocol mpls>;
    }
    scheduler-map map-name;
    shaping-rate bps;
    translation-table (to-dscp-from-dscp | to-dscp-ipv6-from-dscp-ipv6 |
        to-exp-from-exp | to-inet-precedence-from-inet-precedence) table-name;
    }
}
interface-set interface-set-name {
    excess-bandwidth-share (equal | proportional value);
    input-excess-bandwidth-share (equal | proportional value);
    input-traffic-control-profile profile-name;
    input-traffic-control-profile-remaining profile-name;
    internal-node;
    output-traffic-control-profile profile-name;
    output-traffic-control-profile-remaining profile-name;
}
}
}

```

Related Documentation

- *Notational Conventions Used in Junos OS Configuration Hierarchies*


classifiers (Logical Interface)

Syntax	<pre>classifiers { type (classifier-name default) family (mpls inet); }</pre>
Hierarchy Level	[edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 14.2 for PTX Series Packet Transport Routers.
Description	Apply a CoS aggregate behavior classifier to a logical interface. You can apply a default classifier or one that is previously defined.
Options	<p>classifier-name—Name of the aggregate behavior classifier.</p> <p>type—Traffic type.</p> <p>Values: dscp, dscp-ipv6, exp, ieee-802.1, inet-precedence</p>
<hr/> <div> NOTE: You can only specify a family for the dscp and dscp-ipv6 types.</div> <hr/>	
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling Default DSCP and DSCP IPv6 Classifiers on page 12• Applying Classifiers to Logical Interfaces on page 20

classifiers (Routing Instance)

Syntax	<pre> classifiers { exp (classifier-name default); dscp (classifier-name default); dscp-ipv6 (classifier-name default); } </pre>
Hierarchy Level	[edit class-of-service routing-instances <i>routing-instance-name</i>]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>dscp and dscp-ipv6 support introduced in Junos OS Release 9.6.</p>
Description	For routing instances with VRF table labels enabled, apply a custom Multiprotocol Label Switching (MPLS) EXP classifier or DSCP classifier to the routing instance. You can apply the default classifier or one that is previously defined.
Options	classifier-name —Name of the behavior aggregate MPLS EXP or DSCP classifier.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Applying MPLS EXP Classifiers to Routing Instances on page 35 • Applying Classifiers to Logical Interfaces on page 20

classifiers (Definition)

Syntax	<pre> classifiers { type classifier-name { import (classifier-name default); forwarding-class class-name { loss-priority level code-points [aliases] [bit-patterns]; } } } </pre>
Hierarchy Level	[edit class-of-service], [edit class-of-service routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. ieee-802.1ad option introduced in Junos OS Release 9.2.
Description	Define a CoS behavior aggregate (BA) classifier for classifying packets. You can associate the classifier with a forwarding class or code-point mapping, and import a default classifier or one that is previously defined.
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The [edit class-of-service routing-instances <i>routing-instance-name</i>] hierarchy level and the dscp-ipv6 and ieee-802.1ad classifier types are not supported on ACX Series routers.</p> </div> </div>	
Options	<p>classifier-name—Name of the aggregate behavior classifier.</p> <p>type—Traffic type: dscp, dscp-ipv6, exp, ieee-802.1, ieee-802.1ad, inet-precedence.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic on page 4

classifiers (Physical Interface)

Syntax	<code>classifiers { type (classifier-name default) ; }</code>
Hierarchy Level	[edit class-of-service interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access routers.
Description	Apply a CoS aggregate behavior classifier to a physical interface. You can apply a default classifier or one that is previously defined.
Options	<p>classifier-name—Name of the aggregate behavior classifier.</p> <p>type—Traffic type.</p> <p>Values: <code>dscp</code>, <code>ieee-802.1</code>, and <code>inet-precedence</code></p>
Required Privilege Level	<p><code>interface</code>—To view this statement in the configuration.</p> <p><code>interface-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • dscp on page 53 • inet-precedence on page 61 • ieee-802.1 on page 58

code-points

Syntax	<code>code-points ([<i>aliases</i>] [<i>bit-patterns</i>]);</code>
Hierarchy Level	<code>[edit class-of-service classifiers type <i>classifier-name</i> forwarding-class <i>class-name</i> loss-priority <i>level</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.2 for SRX Series devices. Statement introduced in Junos OS Release 14.2 for PTX Series Packet Transport Routers.
Description	Specify one or more DSCP code-point aliases or bit sets for association with a forwarding class.
Options	<i>aliases</i> —Name of the DSCP alias. <i>bit-patterns</i> —Value of the code-point bits, in six-bit binary form.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic on page 4• Example: Configuring a Custom DSCP Behavior Aggregate Classifier

copy-plp-all

Syntax	<code>copy-plp-all;</code>
Hierarchy Level	<code>[edit class-of-service]</code>
Release Information	Statement introduced in Junos OS Release 10.3.
Description	Enable PLP bit copying for ingress and egress for unicast and multicast traffic when traffic is ingressing one FPC and egressing the other (from E3-FPC to non-E3 FPC on M320 routers, or from ES-FPC to non-ES FPC on T Series routers).
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Managing Congestion by Setting Packet Loss Priority for Different Traffic Flows on page 26

dscp (AS PIC Classifiers)

Syntax	<code>dscp (<i>alias</i> <i>bits</i>);</code>
Hierarchy Level	[edit services cos application-profile <i>profile-name</i> (ftp sip) (data video voice)], [edit services cos rule <i>rule-name</i> term <i>term-name</i> then], [edit services cos rule <i>rule-name</i> term <i>term-name</i> then (reflexive reverse)]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	Define the Differentiated Services code point (DSCP) mapping that is applied to the packets.
Options	<i>alias</i> —Name assigned to a set of CoS markers. <i>bits</i> —Mapping value in the packet header.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Actions in a CoS Rule</i>

dscp (CoS Interfaces)

Syntax	<code>dscp (<i>classifier-name</i> default);</code>
Hierarchy Level	[edit class-of-service interfaces <i>interface-name</i> classifiers]
Release Information	Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access routers.
Description	For ACX Series Universal Access routers, map the DSCP field of the incoming packet to the forwarding class and packet loss priority based on the specified DSCP classifier.
Options	<i>classifier-name</i> —Name of the previously defined DSCP behavior aggregate classifier. default —Default DSCP behavior aggregate classifier.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

dscp-ipv6 (CoS Rewrite Rules)

Syntax	<code>dscp-ipv6 (rewrite-name <default>) protocol mpls;</code>
Hierarchy Level	[edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]
Release Information	Statement introduced before Junos OS Release 7.4. Support for protocol mpls option introduced in Junos OS Release 10.4R2.
Description	<p>For IPv6 traffic, apply a DSCP rewrite rule.</p> <p>Logical interfaces do not support multiple dscp-ipv6 rewrite rules for the same protocol.</p> <p>DSCP and DSCP IPv6 rewrite rules are supported on M Series and T Series routers when non-queuing PICs are installed, but are disabled when queuing PICs are installed with the following exceptions:</p> <ul style="list-style-type: none">• On M320 routers, DSCP rewrite is supported on IQ, IQ2, IQE, and IQ2E PICs when used with the Enhanced III FPC.• On M120 routers, DSCP rewrite is supported on IQ, IQ2, IQE, and IQ2E PICs. <p>DSCP and DCSP IPv6 rewrite rules are supported on MIC and MPC interfaces on MX Series routers.</p> <p>DSCP rewrite rules are not supported on T Series routers when IQ, IQ2, IQE, IQ2E, SONET/SDH OC48/STM16 IQE, or PD-5-10XGE-SFPP PICs are installed.</p>
Options	<p>rewrite-name—Name of a rewrite-rules mapping configured at the [edit class-of-service rewrite-rules dscp-ipv6] hierarchy level.</p> <p>default—Default mapping.</p> <p>protocol mpls—(Optional for ingress MPLS tunnel nodes) For interfaces on MX Series routers or hosted on Enhanced III FPCs in M120 or M320 routers only, rewrite the MPLS EXP bits in the MPLS header independently of the IPv6 DSCP value for IPv6 packets entering an MPLS tunnel.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Rewrite Rules</i>• <i>protocol</i>• <i>Setting IPv6 DSCP and MPLS EXP Values Independently</i>• <i>Configuring DSCP Values for IPv6 Packets Entering the MPLS Tunnel</i>• <i>Applying Rewrite Rules to Output Logical Interfaces</i>• <i>rewrite-rules (Definition)</i>

exp

Syntax	<code>exp (rewrite-name default) protocol protocol-types;</code>
Hierarchy Level	<code>[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced before Junos OS Release 12.2. for ACX series
Description	Apply an MPLS experimental (EXP) rewrite rule.
Options	<p>rewrite-name—Name of a rewrite-rules mapping configured at the <code>[edit class-of-service rewrite-rules exp]</code> hierarchy level.</p> <p>default—The default mapping.</p> <p>By default, IP precedence rewrite rules alter the first three bits on the type-of-service (ToS) byte while leaving the last three bits unchanged. This default behavior applies to rewrite rules you configure for MPLS packets with IPv4 payloads. You configure these types of rewrite rules by including the mpls-inet-both or mpls-inet-both-non-vpn option at the <code>[edit class-of-service interfaces interface interface-name unit logical-unit-number rewrite-rules exp rewrite-rule-name protocol]</code> hierarchy level. The IP precedence rewrite rules explanation does not apply to ACX Series Universal Access routers.</p> <p>On interfaces configured on Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs) on MX Series 3D Universal Edge Routers and EX Series switches, we highly recommend that you configure the default option when you configure a behavior aggregate (BA) classifier that does not include a specific rewrite rule for MPLS packets. Doing so ensures that MPLS exp value is rewritten according to the BA classifier rules configured for forwarding or packet loss priority. This does not apply to ACX Series Universal Access routers.</p> <p>protocol-types—Specify one or more protocol matching criteria:</p> <ul style="list-style-type: none"> • mpls-any—Apply to MPLS packets, write MPLS header only. • mpls-inet-both—Apply to IPv4 MPLS packets, write MPLS and IPv4 header. • mpls-inet-both-non-vpn—Apply to IPv4 MPLS packets, write MPLS and IPv4 header for only non VPN traffic.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Rewrite Rules</i> • <i>Rewriting the EXP Bits of All Three Labels of an Outgoing Packet</i> • <i>Applying Rewrite Rules to Output Logical Interfaces</i> • <i>protocol (Rewrite Rules)</i>

- *rewrite-rules (Definition)*

forwarding-class (BA Classifiers)

Syntax	<code>forwarding-class <i>class-name</i> { <code>loss-priority level code-points</code> [<i>aliases</i>] [<i>bit-patterns</i>]; }</code>
Hierarchy Level	[edit class-of-service classifiers <i>type classifier-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 14.2 for PTX Series Packet Transport Routers.
Description	Define forwarding class name and option values.
Options	<i>class-name</i> —Name of the forwarding class. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Defining Classifiers on page 19

ieee-802.1 (Rewrite Rules on Logical Interface)

Syntax	<code>ieee-802.1 (<i>rewrite-name</i> default) vlan-tag (outer outer-and-inner);</code>
Hierarchy Level	<code>[edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]</code>
Release Information	Statement introduced before Junos OS Release 7.4. vlan-tag statement introduced in Junos OS Release 8.1.
Description	Apply an IEEE-802.1 rewrite rule. For IQ PICs, you can only configure one IEEE 802.1 rewrite rule on a physical port. All logical ports (units) on that physical port should apply the same IEEE 802.1 rewrite rule.
Options	<i>rewrite-name</i> —Name of a rewrite-rules mapping configured at the <code>[edit class-of-service rewrite-rules ieee-802.1]</code> hierarchy level. default —The default mapping.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Rewrite Rules</i> • <i>dscp (Rewrite Rules)</i> • dscp-ipv6 (CoS Rewrite Rules) on page 54 • exp on page 55 • <i>exp-push-push-push</i> • <i>exp-swap-push-push</i> • ieee-802.1ad on page 59 • inet-precedence (CoS Rewrite Rules) on page 60 • <i>rewrite-rules (Definition)</i>

ieee-802.1 (Classifier on Physical Interface)

Syntax	ieee-802.1 (<i>classifier-name</i> default) vlan-tag (inner outer);
Hierarchy Level	[edit class-of-service interfaces <i>interface-name</i> classifiers]
Release Information	Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access routers.
Description	For ACX Series Universal Access routers and EX Series switches, map the ieee-802.1p field of the incoming packet to the forwarding class and packet loss priority based on the specified 802.1p classifier. In the case of double tagged packets, you can configure whether to use the 802.1p of the outer or inner VLAN tag.
Options	<p>vlan-tag inner—In the case of double tagged packets, classify based on the 802.1p of the inner VLAN tag.</p> <p>vlan-tag outer—Classify based on the 802.1p of the outermost VLAN tag.</p> <p>classifier-name—Name of the previously defined ieee-802.1p behavior aggregate classifier.</p> <p>default—Default ieee-802.1p behavior aggregate classifier.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

ieee-802.1ad

Syntax	ieee-802.1ad (<i>rewrite-name</i> default) vlan-tag (outer outer-and-inner);
Hierarchy Level	[edit class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Apply a IEEE-802.1ad rewrite rule.
Options	<p>rewrite-name—Name of a rewrite-rules mapping configured at the [edit class-of-service rewrite-rules ieee-802.1ad] hierarchy level.</p> <p>default—The default rewrite bit mapping.</p> <p>vlan-tag—The rewrite rule is applied to the outer or outer-and-inner VLAN tag.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Rewrite Rules</i> • <i>dscp (Rewrite Rules)</i> • dscp-ipv6 (CoS Rewrite Rules) on page 54 • exp on page 55 • <i>exp-push-push-push</i> • <i>exp-swap-push-push</i> • ieee-802.1 (Rewrite Rules on Logical Interface) on page 57 • inet-precedence (CoS Rewrite Rules) on page 60 • <i>rewrite-rules (Definition)</i>

import (Classifiers)

Syntax	<code>import (classifier-name default);</code>
Hierarchy Level	<code>[edit class-of-service classifiers type classifier-name]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify a default or previously defined classifier.
Options	classifier-name —Name of the classifier mapping configured at the <code>[edit class-of-service classifiers]</code> hierarchy level. default —The default classifier mapping.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic on page 4

inet-precedence (CoS Rewrite Rules)

Syntax	<code>inet-precedence (rewrite-name default);</code>
Hierarchy Level	<code>[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Apply a IPv4 precedence rewrite rule.
Options	rewrite-name —Name of a <code>rewrite-rules</code> mapping configured at the <code>[edit class-of-service rewrite-rules inet-precedence]</code> hierarchy level. default —The default mapping. By default, IP precedence rewrite rules alter the first three bits on the type of service (ToS) byte while leaving the last three bits unchanged.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Rewrite Rules• Applying Rewrite Rules to Output Logical Interfaces• protocol (Rewrite Rules)• rewrite-rules (Definition)

inet-precedence (Classifier on Physical Interface)

Syntax	<code>inet-precedence (classifier-name default);</code>
Hierarchy Level	[edit class-of-service interfaces <i>interface-name</i> classifiers]
Release Information	Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access routers.
Description	On ACX Series Universal Access routers and EX Series switches, map the inet-precedence field of the incoming packet to the forwarding class and packet loss priority, based on the specified inet-precedence classifier. When no classifier is configured on the physical interface, the default ipprec-compatibility inet-precedence classifier is applied on the physical interface.
Options	classifier-name —Name of the previously defined inet-precedence behavior aggregate classifier. default —Default inet-precedence behavior aggregate classifier.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.

interfaces (CoS)

```
Syntax interfaces {
    interface-name {
        classifiers{
            dscp(classifier-name | default) {
            }
            ieee-802.1 (classifier-name | default) vlan-tag (inner | outer | classifier-name);
            inet-precedence (rewrite-name | default);
        }
        input-scheduler-map map-name;
        input-shaping-rate rate;
        irb {
            unit logical-unit-number {
                classifiers {
                    type (classifier-name | default);
                }
                rewrite-rules {
                    dscp (rewrite-name | default);
                    dscp-ipv6 (rewrite-name | default);
                    exp (rewrite-name | default) protocol protocol-types;
                    ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
                    inet-precedence (rewrite-name | default);
                }
            }
        }
        member-link-scheduler (replicate | scale);
        rewrite-rules {
            dscp (rewrite-name | default);
            ieee-802.1 (rewrite-name | default) vlan-tag (outer);
            inet-precedence (rewrite-name | default);
        }
        scheduler-map map-name;
        scheduler-map-chassis map-name;
        shaping-rate rate;
        unit logical-unit-number {
            classifiers {
                type (classifier-name | default) family (mpls | inet);
            }
            forwarding-class class-name;
            fragmentation-map map-name;
            input-shaping-rate (percent percentage | rate);
            input-traffic-control-profile profile-name shared-instance instance-name;
            output-traffic-control-profile profile-name shared-instance instance-name;
            per-session-scheduler;
            rewrite-rules {
                dscp (rewrite-name | default);
                dscp-ipv6 (rewrite-name | default);
                exp (rewrite-name | default) protocol protocol-types;
                exp-push-push-push default;
                exp-swap-push-push default;
                ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
                inet-precedence (rewrite-name | default);
            }
        }
    }
}
```

```

    }
    scheduler-map map-name;
    shaping-rate rate;
    translation-table (to-dscp-from-dscp | to-dscp-ipv6-from-dscp-ipv6 | to-exp-from-exp
    | to-inet-precedence-from-inet-precedence) table-name;
  }
}
interface-set interface-set-name {
  excess-bandwidth-share;
  internal-node;
  output-traffic-control-profile profile-name;
  output-traffic-control-profile-remaining profile-name;
}
}

```

Hierarchy Level	[edit class-of-service]
Release Information	Statement introduced before Junos OS Release 7.4. Interface-set level added in Junos OS Release 8.5.
Description	Configure interface-specific CoS properties for incoming packets.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic on page 4 • Configuring Rewrite Rules

loss-priority (BA Classifiers)

Syntax	<code>loss-priority <i>level</i>;</code>
Hierarchy Level	[edit class-of-service classifiers <i>type classifier-name</i> forwarding-class <i>class-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 14.2 for PTX Series Packet Transport Routers.
Description	Specify packet loss priority value for a specific set of code-point aliases and bit patterns.
Options	<i>level</i> can be one of the following: <ul style="list-style-type: none">• high—Packet has high loss priority.• medium-high—Packet has medium-high loss priority.• medium-low—Packet has medium-low loss priority.• low—Packet has low loss priority.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic on page 4• Configuring Tricolor Marking

routing-instances (CoS)

Syntax	<pre> routing-instances <i>routing-instance-name</i> { classifiers { dscp (<i>classifier-name</i> default); dscp-ipv6 (<i>classifier-name</i> default); exp (<i>classifier-name</i> default); } }</pre>
Hierarchy Level	[edit class-of-service]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	For routing instances with VRF table labels enabled, apply a custom MPLS EXP classifier or DSCP classifier to the routing instance. You can apply the default MPLS EXP classifier or one that is previously defined.
Default	If you do not include this statement, the default MPLS EXP classifier is applied to the routing instance. When no DSCP classifier is configured, the default MPLS EXP classifier is applied.
Options	<p><i>routing-instance-name</i>—Name of a routing instance.</p> <p><i>classifier-name</i>—Name of the behavior aggregate MPLS EXP classifier or DSCP classifier.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Forwarding Classes</i> • <i>Applying Custom MPLS EXP Classifiers to Routing Instances in Layer 3 VPNs</i>

system-defaults

Syntax `system-defaults {
 classifiers{
 type classifier-name;
 }
 }`

Hierarchy Level [edit class-of-service]

Release Information Statement introduced in Junos OS Release 12.2.

Description Define a CoS classifier to support global classifiers.

Options *classifier-name*—Name of the behavior aggregate (BA) classifier.

 type—Traffic type: dscp, dscp-ipv6, or exp.



NOTE: The `dscp` and `dscp-ipv6` classifier types are not supported on ACX Series routers.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

unit

Syntax `unit logical-unit-number {`
 `classifiers {`
 `type (classifier-name | default) family (mpls | all);`
 `}`
 `forwarding-class class-name;`
 `fragmentation-map map-name;`
 `input-traffic-control-profile profile-name shared-instance instance-name;`
 `output-traffic-control-profile profile-name shared-instance instance-name;`
 `per-session-scheduler;`
 `rewrite-rules {`
 `dscp (rewrite-name | default);`
 `dscp-ipv6 (rewrite-name | default);`
 `exp (rewrite-name | default) protocol protocol-types;`
 `exp-push-push-push default;`
 `exp-swap-push-push default;`
 `ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);`
 `inet-precedence (rewrite-name | default);`
 `}`
 `scheduler-map map-name;`
 `shaping-rate rate;`
`}`

Hierarchy Level [edit class-of-service [interfaces](#) *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options *logical-unit-number*—Number of the logical unit.

Range: 0 through 16,384

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Understanding How Behavior Aggregate Classifiers Prioritize Trusted Traffic on page 4](#)
- [Configuring Rewrite Rules](#)

