



---

# Layer 2 Traffic Policing Feature Guide for MX Series Routers



---

Published: 2013-07-31

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*Layer 2 Traffic Policing Feature Guide for MX Series Routers*

Copyright © 2013, 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
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Layer 2 Traffic Policing at the Pseudowire . . . . .</b>	<b>3</b>
	Layer 2 Traffic Policing at the Pseudowire Overview . . . . .	3
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Basic Configuration: Configuring Layer 2 Traffic Policing at the Pseudowire . . . . .</b>	<b>7</b>
	Configuring a Three-Color Layer 2 Policer for the Pseudowire . . . . .	7
	Configuring a Two-Color Layer 2 Policer for the Pseudowire . . . . .	8
	Applying the Policers to Dynamic Profile Interfaces . . . . .	8
	Attaching Dynamic Profiles to Routing Instances . . . . .	10
<b>Chapter 3</b>	<b>Complex Configuration: Configuring Layer 2 Traffic Policing at the Pseudowire Using Variables . . . . .</b>	<b>11</b>
	Using Variables for Layer 2 Traffic Policing at the Pseudowire Overview . . . . .	11
	Configuring a Policer for the Complex Configuration . . . . .	12
	Creating a Dynamic Profile for the Complex Configuration . . . . .	12
	Attaching Dynamic Profiles to Routing Instances for the Complex Configuration . . . . .	13
<b>Chapter 4</b>	<b>Configuration Statements for Layer 2 Traffic Policing at the Pseudowire . . . . .</b>	<b>15</b>
	associate-profile . . . . .	15
	family vpls (Layer 2 Pseudowires) . . . . .	16
	firewall . . . . .	17
	layer2-policer . . . . .	18
	logical-interface-policer . . . . .	19
	policer (Configuring) . . . . .	20

	profile-variable-set (Dynamic Profiles) . . . . .	22
	profile-variable-set (Routing Instances) . . . . .	22
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 5</b>	<b>Verifying Your Layer 2 Policers at the Pseudowire on VPLS Connections . . . . .</b>	<b>25</b>
	Verifying Your Layer 2 Traffic Policers on VPLS Connections . . . . .	25

# List of Figures

Part 1	Overview	
Chapter 1	Layer 2 Traffic Policing at the Pseudowire .....	3
	Figure 1: Limiting Traffic to the Core Using Layer 2 Policers at the Pseudowire Level .....	3



# List of Tables

<b>About the Documentation</b> .....	<b>ix</b>
Table 1: Notice Icons .....	xi
Table 2: Text and Syntax Conventions .....	xi





# 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:

- MX 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.

Table 2 on page xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active

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

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<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@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	<b>stub</b> <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.	<b>broadcast   multicast</b>  ( <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.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	<b>community name members [</b> <i>community-ids</i> <b>]</b>
Indentation and braces ( { } )	Identify 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.	
<b>GUI Conventions</b>		
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (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: <https://www.juniper.net/alerts/>

- 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

- [Layer 2 Traffic Policing at the Pseudowire on page 3](#)





# Layer 2 Traffic Policing at the Pseudowire

- [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)

## Layer 2 Traffic Policing at the Pseudowire Overview

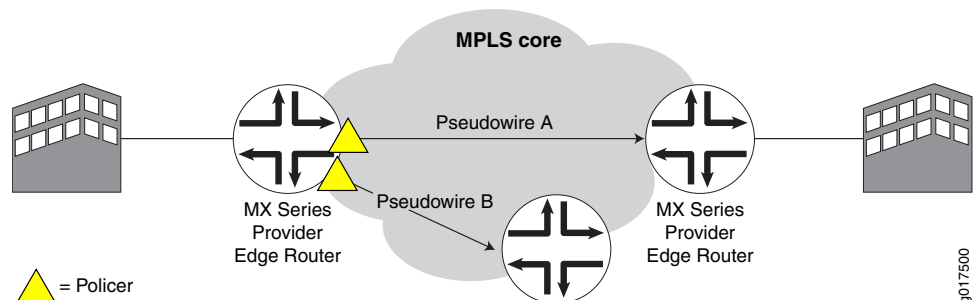
This feature limits traffic that is sent over the core by policing traffic at the Layer 2 pseudowire level. It uses dynamic profiles to attach two- or three-color policers to pseudowire logical interfaces. You apply the dynamic profiles to core-facing egress interfaces so that they can police unicast, multicast, and broadcast traffic that is going over the MPLS core network.



**NOTE:** Pseudowire policer statistics collected by the Routing Engine, kernel, and Packet Forwarding Engine can be displayed on the Routing Engine when you execute the `show interfaces` command.

[Figure 1 on page 3](#) shows an MX Series 3D Universal Edge Router configured as a provider edge (PE) router. It communicates with other PE routers over pseudowires. It can aggregate both unicast and multicast traffic and send it over pseudowires. To limit traffic over the pseudowires, you can set up policers on each pseudowire that faces the MPLS core network.

**Figure 1: Limiting Traffic to the Core Using Layer 2 Policers at the Pseudowire Level**



**NOTE:** This feature is supported only on pseudowire logical interfaces at the egress. It is not supported on tunnel interfaces.

**Related  
Documentation**

## PART 2

# Configuration

- [Basic Configuration: Configuring Layer 2 Traffic Policing at the Pseudowire on page 7](#)
- [Complex Configuration: Configuring Layer 2 Traffic Policing at the Pseudowire Using Variables on page 11](#)
- [Configuration Statements for Layer 2 Traffic Policing at the Pseudowire on page 15](#)



## CHAPTER 2

# Basic Configuration: Configuring Layer 2 Traffic Policing at the Pseudowire

- [Configuring a Three-Color Layer 2 Policer for the Pseudowire on page 7](#)
- [Configuring a Two-Color Layer 2 Policer for the Pseudowire on page 8](#)
- [Applying the Policers to Dynamic Profile Interfaces on page 8](#)
- [Attaching Dynamic Profiles to Routing Instances on page 10](#)

## Configuring a Three-Color Layer 2 Policer for the Pseudowire

---

For the basic configuration of Layer 2 policers for pseudowires, create a three-color policer. This scenario shows a two-rate three-color-marking (trTCM) policer.

To configure a three-color policer:

1. Create a three-color policer.

```
[edit firewall]  
user@host# edit three-color-policer trTCM-policer
```

2. Specify that the policer is to be used on a logical interface.

```
[edit firewall three-color-policer trTCM-policer]  
user@host# set logical-interface-policer
```

3. Set the action for the policer.

```
[edit firewall three-color-policer trTCM-policer]  
user@host# set action loss-priority high then discard
```

4. Specify that the policer is a two-rate policer and configure the policer.

```
[edit firewall three-color-policer trTCM-policer]  
user@host# edit two-rate  
user@host# set color-aware  
user@host# set committed-information-rate 10m  
user@host# set committed-burst-size 50m  
user@host# set committed-burst-size 150k  
user@host# set peak-information-rate 50m  
user@host# set peak-burst-size 450k
```

- Related Documentation**
- [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)
  - [Two-Rate Three-Color Policer Overview](#)
  - [Configuring a Two-Color Layer 2 Policer for the Pseudowire on page 8](#)
  - [Applying the Policers to Dynamic Profile Interfaces on page 8](#)
  - [Attaching Dynamic Profiles to Routing Instances on page 10](#)

---

## Configuring a Two-Color Layer 2 Policer for the Pseudowire

---

For the basic configuration of Layer 2 policers for pseudowires, create a two-color policer.

To configure a two-color policer:

1. Create a two-color policer.

```
[edit firewall]  
user@host# edit policer 2color-l2-policer
```

2. Specify that the policer is to be used on a logical interface.

```
[edit firewall policer 2color-l2-policer]  
user@host# set logical-interface-policer
```

3. Configure the policer.

```
[edit firewall policer 2color-l2-policer]  
user@host# edit if-exceeding  
[edit firewall policer 2color-l2-policer if-exceeding]  
user@host# set bandwidth-limit 30m  
user@host# set burst-size-limit 300k
```

4. Set the action that the policer takes to loss-priority and specify that the packet loss priority (PLP) is high.

```
[edit firewall policer 2color-l2-policer]  
user@host# set then loss-priority high
```

- Related Documentation**
- [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)
  - [Configuring a Three-Color Layer 2 Policer for the Pseudowire on page 7](#)
  - [Applying the Policers to Dynamic Profile Interfaces on page 8](#)
  - [Attaching Dynamic Profiles to Routing Instances on page 10](#)

---

## Applying the Policers to Dynamic Profile Interfaces

---

This configuration shows how to apply policers to a dynamic profile.

Before you can apply policers, you need to have configured your policers as described in:

- [Configuring a Three-Color Layer 2 Policer for the Pseudowire on page 7](#)
- [Configuring a Two-Color Layer 2 Policer for the Pseudowire on page 8](#)

To configure the dynamic profiles:

1. Create a dynamic profile for the three-color policer.

```
[edit dynamic-profiles]
user@host# edit pw-trTCM-policer
```

2. Create a dynamic profile interface that has a dynamic underlying interface unit.

```
[edit dynamic-profiles pw-trTCM-policer]
user@host# edit interfaces $junos-interface-ifd-name unit
$junos-underlying-interface-unit
```

3. Specify that VPLS is the protocol family.

```
[edit dynamic-profiles pw-trTCM-policer interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit"]
user@host# set family vpls
```

4. Assign the three-color policer to the dynamic profile.

```
[edit dynamic-profiles pw-trTCM-policer interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit"]
user@host# set layer2-policer output-three-color trTCM-policer
```

5. Create a dynamic profile for the two-color policer.

```
[edit dynamic-profiles]
user@host# edit pw-2color-l2-policer
```

6. Create a dynamic profile interface that has a dynamic underlying interface unit.

```
[edit dynamic-profiles pw-2color-l2-policer]
user@host# edit interfaces $junos-interface-ifd-name unit
$junos-underlying-interface-unit
```

7. Specify that VPLS is the protocol family.

```
[edit dynamic-profiles pw-2color-l2-policer interfaces "$junos-interface-ifd-name"
unit "$junos-underlying-interface-unit"]
user@host# set family vpls
```

8. Assign the two-color policer to the dynamic profile.

```
[edit dynamic-profiles pw-2color-l2-policer interfaces "$junos-interface-ifd-name"
unit "$junos-underlying-interface-unit"]
user@host# set layer2-policer output-policer 2color-l2-policer
```

**Related  
Documentation**

- [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)
- [Configuring a Three-Color Layer 2 Policer for the Pseudowire on page 7](#)
- [Configuring a Two-Color Layer 2 Policer for the Pseudowire on page 8](#)
- [Attaching Dynamic Profiles to Routing Instances on page 10](#)

## Attaching Dynamic Profiles to Routing Instances

---

To bind the dynamic profile to the pseudowire, attach it to a routing instance. The routing instance can be a VPLS instance type or a virtual switch instance type. You can attach dynamic profiles to the routing instance at the VPLS protocol level, at the mesh-group level, or at the neighbor level.

Because this feature is not supported on tunnel interfaces, for VPLS routing interfaces, you must include the **no-tunnel-services** statement at the **[edit routing-instances routing-instance-name protocols vpls]** hierarchy level.

- To attach the dynamic profile at the VPLS protocol level:

```
[edit routing-instances]
user@host# edit green protocols vpls associate-profile
[edit routing-instances green protocols vpls associate-profile]
user@host# set pw-2color-l2-policer
```

- To attach the dynamic profile at the mesh-group level.

```
[edit routing-instances]
user@host# edit green protocols vpls mesh-group lata-1 associate-profile
[edit routing-instances green protocols vpls mesh-group lata-1 associate-profile]
user@host# set pw-trTCM-policer
```

- To attach the dynamic profile at the neighbor level.

```
[edit routing-instances]
user@host# edit green protocols vpls mesh-group lata-1 neighbor 10.10.1.1
associate-profile
[edit routing-instances green protocols vpls mesh-group lata-1 neighbor 10.10.1.1
associate-profile]
user@host# set pw-2color-l2-policer
```

### Related Documentation

- [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)
- [Configuring a Three-Color Layer 2 Policer for the Pseudowire on page 7](#)
- [Configuring a Two-Color Layer 2 Policer for the Pseudowire on page 8](#)
- [Applying the Policers to Dynamic Profile Interfaces on page 8](#)



## CHAPTER 3

# Complex Configuration: Configuring Layer 2 Traffic Policing at the Pseudowire Using Variables

- [Using Variables for Layer 2 Traffic Policing at the Pseudowire Overview on page 11](#)
- [Configuring a Policer for the Complex Configuration on page 12](#)
- [Creating a Dynamic Profile for the Complex Configuration on page 12](#)
- [Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 13](#)

## Using Variables for Layer 2 Traffic Policing at the Pseudowire Overview

---

To reduce the number of dynamic profiles needed to police traffic at the core, you can use a variable for the output policer in your dynamic profiles. The variable that you define is called **junos-layer2-output-policer**. The variable is a placeholder that gets filled in when the dynamic profile obtains the value from the routing instance.

To use variables for policers for Layer 2 pseudowires:

1. Create policers.
2. Create a dynamic profile and add a profile variable set to the dynamic profile.
3. In the profile variable set, assign a value to the **junos-layer2-output-policer** variable. This value is the name of one of your policers.
4. In the dynamic profile interface configuration at the **[edit dynamic-profiles *profile-name* interfaces "\$junos-interface-ifd-name" unit "\$junos-underlying-interface-unit"]** hierarchy, assign **junos-layer2-output-policer** as one of your Layer 2 policers.
5. When you attach the dynamic profile to a routing instance, assign the profile variable set that you configured in the dynamic profile as the **associate-profile** value.
6. Attach the dynamic profile and the profile variable set to the routing instance.

### Related Documentation

- [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)
- [Configuring a Policer for the Complex Configuration on page 12](#)

- [Creating a Dynamic Profile for the Complex Configuration on page 12](#)
- [Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 13](#)

---

## Configuring a Policer for the Complex Configuration

For the complex configuration of Layer 2 policers for pseudowires, create a two-color policer.

To configure a two-color policer:

1. Create a two-color policer.

```
[edit firewall]  
user@host# edit policer 10m-policer
```

2. Specify that the policer is to be used on a logical interface.

```
[edit firewall policer 10m-policer]  
user@host# set logical-interface-policer
```

3. Configure the policer.

```
[edit firewall policer 10m-policer]  
user@host# edit if-exceeding  
[edit firewall policer 10m-policer if-exceeding]  
user@host# set bandwidth-limit 10m  
user@host# set burst-size-limit 100k
```

4. Set the action that the policer takes to loss-priority and specify that the packet loss priority (PLP) is high.

```
[edit firewall policer 10m-policer]  
user@host# set then loss-priority high
```

### Related Documentation

- [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)
- [Using Variables for Layer 2 Traffic Policing at the Pseudowire Overview on page 11](#)
- [Creating a Dynamic Profile for the Complex Configuration on page 12](#)
- [Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 13](#)

---

## Creating a Dynamic Profile for the Complex Configuration

For this configuration, the dynamic profile defines a profile variable set and then assigns the variable to the output policer.

To configure dynamic profiles:

1. Create a dynamic profile.

```
[edit dynamic-profiles]  
user@host# edit pw-policer
```

2. Create a profile variable set and define the **junos-layer2-output-policer** variable. In this scenario, set the variable to the **10m-policer**.

```
[edit dynamic-profiles pw-policer]
user@host# edit profile-variable-set pw-policer-var-set
user@host# set junos-layer2-output-policer 10m-policer
```

3. Create a dynamic profile interface that has a dynamic underlying interface unit.

```
[edit dynamic-profiles pw-policer]
user@host# edit interfaces $junos-interface-ifd-name unit
$junos-underlying-interface-unit
```

4. Assign the **junos-layer2-output-policer** variable to the two-color output policer.

```
[edit dynamic-profiles pw-policer interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit"]
user@host# set layer2-policer output-policer $junos-layer2-output-policer
```

5. Specify that VPLS is the protocol family.

```
[edit dynamic-profiles pw-2color-l2-policer interfaces "$junos-interface-ifd-name"
unit "$junos-underlying-interface-unit"]
user@host# set family vpls
```

#### Related Documentation

- [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)
- [Using Variables for Layer 2 Traffic Policing at the Pseudowire Overview on page 11](#)
- [Configuring a Policer for the Complex Configuration on page 12](#)
- [Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 13](#)

---

## Attaching Dynamic Profiles to Routing Instances for the Complex Configuration

To bind the dynamic profile to the pseudowire, attach it to a routing instance. When your dynamic profile contains variables, you assign one of the profile variable sets that you configured in your dynamic profile when you associate the profile with the routing instance.

The routing instance can be a VPLS instance type or a virtual switch instance type. You can attach the dynamic profile and the profile variable set to the routing instance at the VPLS protocol level, at the mesh-group level, or at the neighbor level.

Because this feature is not supported on tunnel interfaces, for VPLS routing interfaces, you must include the **no-tunnel-services** statement at the **[edit routing-instances routing-instance-name protocols vpls]** hierarchy level.

- To attach the dynamic profile and the profile variable set at the VPLS protocol level:

```
[edit routing-instances]
user@host# edit green protocols vpls associate-profile
[edit routing-instances green protocols vpls associate-profile]
user@host# set profile-variable-set pw-policer
user@host# set profile-variable-set pw-policer-var-set
```

- To attach the dynamic profile and the profile variable set at the mesh-group level:

```
[edit routing-instances]
user@host# edit green protocols vpls mesh-group lata-1 associate-profile
[edit routing-instances green protocols vpls mesh-group lata-1 associate-profile]
user@host# set profile-variable-set pw-policer
user@host# set profile-variable-set pw-policer-var-set
```

- To attach the dynamic profile and the profile variable set at the neighbor level:

```
[edit routing-instances]
user@host# edit green protocols vpls mesh-group lata-1 neighbor 10.10.1.1
associate-profile
[edit routing-instances green protocols vpls mesh-group lata-1 neighbor 10.10.1.1
associate-profile]
user@host# profile-variable-set pw-policer
user@host# profile-variable-set pw-policer-var-set
```

#### Related Documentation

- [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)
- [Using Variables for Layer 2 Traffic Policing at the Pseudowire Overview on page 11](#)
- [Configuring a Policer for the Complex Configuration on page 12](#)
- [Creating a Dynamic Profile for the Complex Configuration on page 12](#)

## CHAPTER 4

# Configuration Statements for Layer 2 Traffic Policing at the Pseudowire

### associate-profile

---

<b>Syntax</b>	<pre>associate-profile {     <i>dynamic-profile-name</i>;     profile-variable-set <i>profile-variable-set-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit routing-instances <i>routing-instance-name</i> protocols vpls], [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> ], [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i> neighbor <i>neighbor-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	Associate a dynamic profile or a profile variable set with a VPLS instance.
<b>Options</b>	<i>dynamic-profile-name</i> —Name of the dynamic profile to attach to this routing instance.  The remaining option is explained separately.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Attaching Dynamic Profiles to Routing Instances on page 10</a></li><li>• <a href="#">Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 13</a></li></ul>

## family vpls (Layer 2 Pseudowires)

---

<b>Syntax</b>	family vpls;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	Specify that the protocol family for the logical interface is VPLS.
<b>Required Privilege Level</b>	router—To view this statement in the configuration. router-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying the Policers to Dynamic Profile Interfaces on page 8</a></li><li>• <a href="#">Creating a Dynamic Profile for the Complex Configuration on page 12</a></li></ul>

## firewall

<b>Syntax</b>	<pre> firewall {     atm-policer <i>atm-policer-name</i> {         ... <i>atm-policer-configuration</i> ...     }     family <i>protocol-family-name</i> {         ... <i>protocol-family-configuration</i> ...     }     filter <i>ipv4-filter-name</i> {         ... <i>ipv4-filter-configuration</i> ...     }     hierarchical-policer <i>hierarchical-policer-name</i> {         ... <i>hierarchical-policer-configuration</i> ...     }     interface-set <i>interface-set-name</i> {         ... <i>interface-set-configuration</i> ...     }     policer <i>two-color-policer-name</i> {         ... <i>two-color-policer-configuration</i> ...     }     three-color-policer <i>three-color-policer-name</i> {         ... <i>three-color-policer-configuration</i> ...     } } </pre>
<b>Hierarchy Level</b>	[edit], [edit logical-systems <i>logical-system-name</i> ] [edit dynamic-profiles <i>profile-name</i> ],
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Logical systems support introduced in Junos OS Release 9.3.
<b>Description</b>	Configure firewall filters.  The statements are explained separately.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Guidelines for Configuring Firewall Filters</i></li> <li>• <i>Guidelines for Configuring Service Filters</i></li> <li>• <i>Guidelines for Configuring Simple Filters</i></li> <li>• <i>Configuring Multifield Classifiers</i></li> <li>• <i>Using Multifield Classifiers to Set PLP</i></li> </ul>


## layer2-policer

---

<b>Syntax</b>	<pre>layer2-policer {     output-policer <i>policer-name</i>;     output-three-color <i>policer-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	Specify the output policers to be used in the dynamic profile.
<b>Options</b>	<p><b>output-policer <i>policer-name</i></b>—Two-color output policer to associate with the interface. You define this policer at the <b>[edit firewall policer]</b> hierarchy level.</p> <p><b>output-three-color <i>policer-name</i></b>—Tricolor output policer to associate with the interface. You define this policer at the <b>[edit firewall]</b> hierarchy level.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Applying the Policers to Dynamic Profile Interfaces on page 8</a></li><li>• <a href="#">Creating a Dynamic Profile for the Complex Configuration on page 12</a></li></ul>



## logical-interface-policer

<b>Syntax</b>	logical-interface-policer;
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> <b>firewall</b> <b>policer</b> <i>policer-name</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> <b>firewall</b> three-color-policer <i>name</i>],</p> <p>[edit firewall atm-policer <i>atm-policer-name</i>]</p> <p>[edit <b>firewall</b> <b>policer</b> <i>policer-name</i>],</p> <p>[edit firewall policer <i>policer-template-name</i>],</p> <p>[edit <b>firewall</b> three-color-policer <i>policer-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> <b>firewall</b> <b>policer</b> <i>policer-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> <b>firewall</b> three-color-policer <i>name</i>]</p>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Support at the [edit firewall three-color-policer <i>policer-name</i>] hierarchy level introduced in Junos OS Release 8.2.</p> <p>Logical systems support introduced in Junos OS Release 9.3.</p> <p>Support at the [edit dynamic-profiles ... policer <i>policer-name</i>] and [edit dynamic-profiles ... three-color-policer <i>name</i>] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
<b>Description</b>	Configure a logical interface policer.
	<div>  <p><b>NOTE:</b> Starting in Junos OS Release 12.2R2, on T Series Core Routers only, you can configure an MPLS LSP policer for a specific LSP to be shared across different protocol family types. You must include the logical-interface-policer statement to do so.</p> </div>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>Two-Color and Three-Color Logical Interface Policers</i></li> <li>• <i>Traffic Policer Types</i></li> <li>• <i>Configuring Tricolor Marking Policers</i></li> <li>• <i>action</i></li> <li>• <i>Configuring Gigabit Ethernet Two-Color and Tricolor Policers</i></li> <li>• <i>action</i></li> </ul>

## policer (Configuring)

---

Syntax	<pre>policer <i>policer-name</i> {     filter-specific;     if-exceeding {         bandwidth-limit <i>bps</i>;         bandwidth-percent <i>number</i>;         burst-size-limit <i>bytes</i>;     }     logical-bandwidth-policer;     logical-interface-policer;     physical-interface-policer;     shared-bandwidth-policer;     then {         <i>policer-action</i>;     } }</pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> <b>firewall</b> ], [edit <b>firewall</b> ], [edit logical-systems <i>logical-system-name</i> <b>firewall</b> ]
Release Information	Statement introduced before Junos OS Release 7.4. The <b>out-of-profile</b> policer action added in Junos OS Release 8.1. The <b>logical-bandwidth-policer</b> statement added in Junos OS Release 8.2. Logical systems support introduced in Junos OS Release 9.3. The <b>physical-interface-policer</b> statement introduced in Junos OS Release 9.6. The <b>shared-bandwidth-policer</b> statement added in Junos OS Release 11.2. Support at the [edit dynamic-profiles ... <b>firewall</b> ] hierarchy level introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure policer rate limits and actions. When included at the [edit <b>firewall</b> ] hierarchy level, the <b>policer</b> statement creates a template, and you do not have to configure a policer individually for every firewall filter or interface. To activate a policer, you must include the <b>policer-action</b> modifier in the <b>then</b> statement in a firewall filter term or on an interface.
Options	<b><i>policer-action</i></b> —One or more actions to take: <ul style="list-style-type: none"><li>• <b>discard</b>—Discard traffic that exceeds the rate limits.</li><li>• <b>forwarding-class <i>class-name</i></b>—Specify the particular forwarding class.</li><li>• <b>loss-priority</b>—Set the packet loss priority (PLP) to <b>low</b>, <b>medium-low</b>, <b>medium-high</b>, or <b>high</b>.</li><li>• <b>out-of-profile</b>—On J Series routers with strict priority queuing, prevent starvation of other queues by rate limiting the data stream entering the strict priority queue, marking the packets that exceed the rate limit as out-of-profile, and dropping the out-of-profile packets if the physical interface is congested.</li></ul>

***policer-name***—Name that identifies the policer. The name can contain letters, numbers, and hyphens (-), and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" "). Policer names cannot begin with an underscore in the form *\_\**.

**then**—Actions to take on matching packets.

The remaining statements are explained separately.

<b>Required Privilege</b>	firewall—To view this statement in the configuration.
<b>Level</b>	firewall-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <i>Bandwidth Policer Overview</i></li><li>• <i>Configuring Firewall Filters and Policers for VPLS</i></li><li>• <i>Configuring Multifield Classifiers</i></li><li>• <i>Logical Interface (Aggregate) Policer Overview</i></li><li>• <i>Physical Interface Policer Overview</i></li><li>• <i>Statement Hierarchy for Configuring Policers</i></li><li>• <i>Single-Rate Two-Color Policer Overview</i></li><li>• <i>Using Multifield Classifiers to Set PLP</i></li><li>• <i>filter (Configuring)</i></li><li>• <i>priority (Schedulers)</i></li></ul>
------------------------------	--

## profile-variable-set (Dynamic Profiles)

---

Syntax	<pre>profile-variable-set {     variable-set-name {         junos-layer2-output-policer <i>policer-name</i>;     } }</pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> ]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	Specify the policer used in the variable set.
Options	<b>junos-layer2-output-policer <i>policer-name</i></b> —Layer 2 policer that you want to substitute in the dynamic profile. You define this policer at the <b>[edit firewall policer]</b> hierarchy level.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Applying the Policers to Dynamic Profile Interfaces on page 8</a></li><li>• <a href="#">Creating a Dynamic Profile for the Complex Configuration on page 12</a></li></ul>

## profile-variable-set (Routing Instances)

---

Syntax	<pre>profile-variable-set <i>variable-set-name</i></pre>
Hierarchy Level	[edit routing-instances routing-instance-name protocols vpls associate-profile]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	Specify the variable set to apply to the dynamic profile for the routing instance.
Options	<b><i>variable-set-name</i></b> —Name of the variable set to use when this dynamic profile is applied to the routing instance. You define this variable set at the <b>[edit dynamic-profiles <i>profile-name</i>]</b> hierarchy level.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"><li>• <a href="#">Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 13</a></li></ul>

## PART 3

# Administration

- [Verifying Your Layer 2 Policers at the Pseudowire on VPLS Connections on page 25](#)



## CHAPTER 5

# Verifying Your Layer 2 Policers at the Pseudowire on VPLS Connections

- [Verifying Your Layer 2 Traffic Policers on VPLS Connections on page 25](#)

## Verifying Your Layer 2 Traffic Policers on VPLS Connections

---

**Purpose** Display VPLS connections to verify that the dynamic profile is running on the Layer 2 VPN connection.

**Action** user@host> **show vpls connections**  
Layer-2 VPN connections:

```
...
Instance: vpls-10gige
Local site: 10Gige-PE (2)
  connection-site      Type  St    Time last up      # Up trans
  1                    rmt   Up    Mar 28 21:27:57 2010      1
    Remote PE: 10.10.1.1, Negotiated control-word: No
    Incoming label: 262145, Outgoing label: 262146
    Local interface: lsi.1048576, Status: Up, Encapsulation: VPLS
    Dynamic profile: pw-policer
    Description: Intf - vpls vpls-10gige local site 2 remote site 1
```

**Meaning** The Dynamic profile field displays the policer that is currently running on the VPLS connection.

**Related Documentation** • [Layer 2 Traffic Policing at the Pseudowire Overview on page 3](#)

