Junos® OS

Layer 2 Firewall Filters and Traffic Policers Feature Guide

Modified: 2017-05-17

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

Junos® OS Layer 2 Firewall Filters and Traffic Policers Feature Guide

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

List of Figures

List of Tables

About the Documentation

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.xsl;
       }
     }
   }
   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.xsl; }
   ```

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 CLI Explorer.

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 xii 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**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	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** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• 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** *metric***>;**
| (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** **(***string1* **|** *string2* **|** *string3***)**
# (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 [** *community-ids* **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

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

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (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 of the Juniper Networks TechLibrary 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 http://www.juniper.net/techpubs/feedback/.
- 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 Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

Configuring Layer 2 Firewall Filters

Understanding Firewall Filters Used to Control Traffic Within Bridge Domains and VPLS Instances

Juniper Networks MX Series 3D Universal Edge Routers support firewall filters for the **bridge** and **vpls** protocol families. You configure these firewall filters to control traffic within bridge domains and VPLS instances. This topic explores some of the ways that filters can be used in a Layer 2 environment to control traffic.

MX Series router firewall filters can be applied to:

- Input interfaces
- Output interfaces
- Input to the Layer 2 forwarding table

NOTE: **Broadcast, unicast unknown, and multicast (BUM) traffic are not affected by input and output policers. BUM traffic can only be filtered by forwarding table policies.**

You use a firewall filter after taking the following two steps:

1. You configure any policers and the firewall filter at the **[edit firewall]** hierarchy level.
2. You apply the properly configured firewall filter to an interface or bridge domain.

NOTE: You should deploy firewall filters carefully because it is easy to cause unforeseen side effects on all traffic, especially traffic that is not the intended target of the filter. For more information about configuring firewall filters, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide*.

NOTE: If the chassis is running in Enhanced IP mode, a single shared filter instance is created for a filter applied across bridge domains. However, if the chassis is not running in Enhanced IP mode, then separate filter instances are created for each bridge domain that the filter is applied to.

Related Documentation

- *Layer 2 Firewall Filters and Traffic Policers Feature Guide*
- Example: Configuring Policing and Marking of Traffic Entering a VPLS Core on page 20
- Example: Configuring Filtering of Frames by MAC Address on page 16
- Example: Configuring Filtering of Frames by IEEE 802.1p Bits on page 17
- Example: Configuring Filtering of Frames by Packet Loss Priority on page 19

Example: Configuring Filtering of Frames by MAC Address

This example firewall filter finds frames with a certain source MAC address (**88:05:00:29:3c:de/48**), then counts and silently discards them. For more information about configuring firewall filter match conditions, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide*. The filter is applied to the VLAN configured as **vlan100200** as an input filter on Router 1.

NOTE: This example does not present exhaustive configuration listings for all routers in the figures. However, you can use this example with a broader configuration strategy to complete the MX Series router network Ethernet Operations, Administration, and Maintenance (OAM) configurations.

To configure filtering of frames by MAC address:

1. Configure **evil-mac-address**, the firewall filter:

```
[edit firewall]
family bridge {
  filter evil-mac-address {
    term one {
      from {
        source-mac-address 88:05:00:29:3c:de/48;
      }
      then {
        count evil-mac-address; # Counts frame with the bad source MAC address
        discard;
```

```
        }
        term two {
            then accept; # Make sure to accept other traffic
        }
    }
  }
}
```

2. Apply **evil-mac-address** as an input filter to **vlan100200** on Router 1:

```
[edit routing-instances]
virtual-switch-R1-1 {
  bridge-domains {
    vlan100200 {
      domain-type bridge;
      forwarding-options {
        filter {
          input evil-mac-address;
        }
      }
    }
  }
}
```

Related Documentation

- *Layer 2 Firewall Filters Feature Guide*
- Understanding Firewall Filters Used to Control Traffic Within Bridge Domains and VPLS Instances on page 15
- Example: Configuring Policing and Marking of Traffic Entering a VPLS Core on page 20
- Example: Configuring Filtering of Frames by IEEE 802.1p Bits on page 17
- Example: Configuring Filtering of Frames by Packet Loss Priority on page 19

Example: Configuring Filtering of Frames by IEEE 802.1p Bits

For the **bridge** and **vpls** protocol families only, MX Series router firewall filters can be configured to provide matching on IEEE 802.1p priority bits in packets with VLAN tagging:

- To configure a firewall filter term that includes matching on IEEE 802.1p learned VLAN priority (in the outer VLAN tag), use the **learn-vlan-1p-priority** or **learn-vlan-1p-priority-except** match condition.
- To configure a firewall filter term that includes matching on IEEE 802.1p user priority (in the inner VLAN tag), use the **user-vlan-1p-priority** or **user-vlan-1p-priority-except** match condition.

For more detailed information about configuring firewall filters and configuring filter match conditions for Layer 2 bridging traffic on the MX Series routers, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide*.

NOTE: Layer 2 bridging is supported only on the MX Series routers. For more information about how to configure Layer 2 bridging, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide*.

This example Layer 2 bridging firewall filter finds any incoming frames with an IEEE 802.1p learned VLAN priority level of either 1 or 2, and then classifies the packet in the **best-effort** default forwarding class.

NOTE: This example does not present exhaustive configuration listings for all routers in the figures. However, you can use this example with a broader configuration strategy to complete the MX Series router network Ethernet Operations, Administration, and Maintenance (OAM) configurations.

To configure filtering of frames by IEEE 802.1p bits:

1. Configure the firewall filter **filter-learn-vlan-configure-forwarding**:

```
[edit firewall]
family bridge {
  filter filter-learn-vlan-configure-forwarding {
    term 0 {
      from {
        learn-vlan-1p-priority [1 2];
      }
      then forwarding-class best-effort;
    }
  }
}
```

2. Apply the firewall filter **filter-learn-vlan-configure-forwarding** as an input filter to **ge-0/0/0**:

```
[edit interfaces]
ge-0/0/0 {
  unit 0 {
    family bridge {
      filter {
        input filter-learn-vlan-configure-forwarding;
      }
    }
  }
}
```

Related Documentation

- *Layer 2 Firewall Filters Feature Guide*
- Understanding Firewall Filters Used to Control Traffic Within Bridge Domains and VPLS Instances on page 15
- Example: Configuring Policing and Marking of Traffic Entering a VPLS Core on page 20

- Example: Configuring Filtering of Frames by MAC Address on page 16
- Example: Configuring Filtering of Frames by Packet Loss Priority on page 19

Example: Configuring Filtering of Frames by Packet Loss Priority

To configure an MX Series router firewall filter to provide matching on the packet loss priority (PLP) level carried in the frame, use the **loss-priority** or **loss-priority-except** match condition. Packet loss priority matching is available for all protocols. For more detailed information about configuring firewall filters and configuring filter match conditions for Layer 2 bridging traffic on the MX Series routers, see the *Routing Policies, Firewall Filters, and Traffic Policers Feature Guide*.

NOTE: Layer 2 bridging is supported only on the MX Series routers. For more information about how to configure Layer 2 bridging, see the *Junos OS Routing Protocols Library*.

This example Layer 2 bridging firewall filter finds any incoming frames with a packet loss priority (PLP) level of **medium-high**, and then classifies the packet in the **expedited-forwarding** default forwarding class.

NOTE: This example does not present exhaustive configuration listings for all routers in the figures. However, you can use this example with a broader configuration strategy to complete the MX Series router network Ethernet Operations, Administration, and Maintenance (OAM) configurations.

To configure filtering of frames by packet loss priority:

1. Configure the firewall filter **filter-plp-configure-forwarding**:

```
[edit firewall]
family bridge {
  filter filter-plp-configure-forwarding {
    term 0 {
      from {
        loss-priority medium-high;
      }
      then forwarding-class expedited-forwarding;
    }
  }
}
```

2. Configure a Layer 2 bridging domain **bd** for the **ge-0/0/0** interface (that has already been configured at the **[edit interfaces]** hierarchy level):

```
[edit bridge-domains]
bd {
  domain-type bridge {
```

```
        interface ge-0/0/0;
    }
}
```

3. Apply the filter **filter-plp-configure-forwarding** as an input filter to the **ge-0/0/0** interface:

```
[edit interfaces]
ge-0/0/0 {
    unit 0 {
        family bridge {
            filter {
                input filter-plp-configure-forwarding;
            }
        }
    }
}
```

Related Documentation

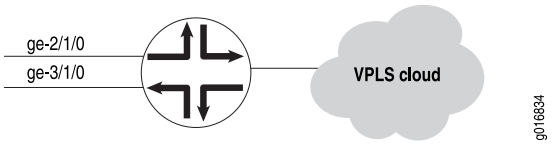
- *Layer 2 Firewall Filters Feature Guide*
- Understanding Firewall Filters Used to Control Traffic Within Bridge Domains and VPLS Instances on page 15
- Example: Configuring Policing and Marking of Traffic Entering a VPLS Core on page 20
- Example: Configuring Filtering of Frames by MAC Address on page 16
- Example: Configuring Filtering of Frames by IEEE 802.1p Bits on page 17

Example: Configuring Policing and Marking of Traffic Entering a VPLS Core

This example firewall filter allows a service provider to limit the aggregate broadcast traffic entering the virtual private LAN service (VPLS) core. The broadcast, unknown unicast, and non-IP multicast traffic received from one of the service provider's customers on a logical interface has a policer applied. The service provider has also configured a two-rate, three-color policer to limit the customer's IP multicast traffic. For more information on the configuration of policers, see the *Class of Service Feature Guide for Routing Devices*.

The position of the router is shown in Figure 1 on page 20.

Figure 1: Policing and Marking Traffic Entering a VPLS Core



There are four major parts to the configuration:

- The policer for broadcast, unknown unicast, and non-IP multicast traffic. This example marks the loss priority as high if this type of traffic exceeds 50 Kbps.
- The two-rate, three-color policer for IP multicast traffic. This example configures a committed information rate (CIR) of 4 Mbps, a committed burst size of 256 Kbytes, a peak information rate of 4.1 Mbps, and a peak burst size of 256 Kbytes (the same as the CIR).
- The filter that applies the two policers to VPLS.
- The application of the filter to the customer interface configuration as an input filter.

NOTE: This example does not present exhaustive configuration listings for all routers in the figures. However, you can use this example with a broader configuration strategy to complete the MX Series router network Ethernet Operations, Administration, and Maintenance (OAM) configurations.

To configure policing and marking of traffic entering a VPLS core:

1. Configure **policer bcast-unknown-unicast-non-ip-mcast-policer**, a firewall policer to limit the aggregate broadcast, unknown unicast, and non-IP multicast to 50 kbps:

```
[edit firewall]
policer bcast-unknown-unicast-non-ip-mcast-policer {
  if-exceeding {
    bandwidth-limit 50k;
    burst-size-limit 150k;
  }
  then loss-priority high;
}
```

2. Configure **three-color-policer ip-multicast-traffic-policer**, a three-color policer to limit the IP multicast traffic:

```
[edit firewall]
three-color-policer ip-multicast-traffic-policer {
  two-rate {
    color-blind;
    committed-information-rate 4m;
    committed-burst-size 256k;
    peak-information-rate 4100000;
    peak-burst-size 256k;
  }
}
```

3. Configure **customer-1**, a firewall filter that uses the two policers to limit and mark customer traffic. The first term marks the IP multicast traffic based on the destination MAC address, and the second term polices the broadcast, unknown unicast, and non-IP multicast traffic:

```
[edit firewall]
```

```
family vpls {
  filter customer-1 {
    term t0 {
      from {
        destination-mac-address {
          01:00:5e:00:00:00/24;
        }
      }
      then {
        three-color-policer {
          two-rate ip-multicast-traffic-policer;
        }
        forwarding-class expedited-forwarding;
      }
    }
    term t1 {
      from {
        traffic-type [ broadcast unknown-unicast multicast ];
      }
      then policer bcast-unknown-unicast-non-ip-mcast-policer;
    }
  }
}
```

4. Apply the firewall filter as an input filter to the customer interface at **ge-2/1/0**:

```
[edit interfaces]
ge-2/1/0 {
  vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 5 {
    encapsulation vlan-vpls;
    vlan-id 9;
    family vpls {
      filter {
        input customer-1;
      }
    }
  }
}
```

Related Documentation

- *Layer 2 Firewall Filters Feature Guide*
- Understanding Firewall Filters Used to Control Traffic Within Bridge Domains and VPLS Instances on page 15
- Example: Configuring Filtering of Frames by MAC Address on page 16
- Example: Configuring Filtering of Frames by IEEE 802.1p Bits on page 17
- Example: Configuring Filtering of Frames by Packet Loss Priority on page 19

CHAPTER 2

Configuring Layer 2 Traffic Policers

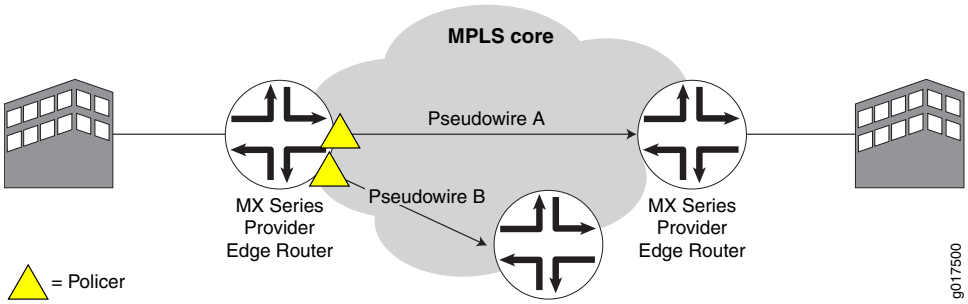
Layer 2 Traffic Policing at the Pseudowire Overview

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 2 on page 24 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 2: 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

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 23
- Configuring a Three-Color Layer 2 Policer for the Pseudowire on page 25
- Applying the Policers to Dynamic Profile Interfaces on page 26
- Attaching Dynamic Profiles to Routing Instances on page 27

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 23
- *Two-Rate Three-Color Policer Overview*
- Configuring a Two-Color Layer 2 Policer for the Pseudowire on page 24
- Applying the Policers to Dynamic Profile Interfaces on page 26
- Attaching Dynamic Profiles to Routing Instances on page 27

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 25
- Configuring a Two-Color Layer 2 Policer for the Pseudowire on page 24

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 23
- Configuring a Three-Color Layer 2 Policer for the Pseudowire on page 25
- Configuring a Two-Color Layer 2 Policer for the Pseudowire on page 24
- Attaching Dynamic Profiles to Routing Instances on page 27

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 23
- Configuring a Three-Color Layer 2 Policer for the Pseudowire on page 25
- Configuring a Two-Color Layer 2 Policer for the Pseudowire on page 24
- Applying the Policers to Dynamic Profile Interfaces on page 26

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 23
- Configuring a Policer for the Complex Configuration on page 28
- Creating a Dynamic Profile for the Complex Configuration on page 29
- Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 30

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 23
- Using Variables for Layer 2 Traffic Policing at the Pseudowire Overview on page 28
- Creating a Dynamic Profile for the Complex Configuration on page 29
- Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 30

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 23
- Using Variables for Layer 2 Traffic Policing at the Pseudowire Overview on page 28
- Configuring a Policer for the Complex Configuration on page 28
- Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 30

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# setprofile-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 23
- Using Variables for Layer 2 Traffic Policing at the Pseudowire Overview on page 28
- Configuring a Policer for the Complex Configuration on page 28
- Creating a Dynamic Profile for the Complex Configuration on page 29

Verifying 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 23

CHAPTER 3

Configuration Statements for Layer 2 Traffic Policing

associate-profile

Syntax

```
associate-profile {
  dynamic-profile-name;
  profile-variable-set profile-variable-set-name;
}
```

Hierarchy Level

[edit routing-instances *routing-instance-name* protocols vpls],
[edit routing-instances *routing-instance-name* protocols vpls mesh-group *mesh-group-name*],
[edit routing-instances *routing-instance-name* protocols vpls mesh-group *mesh-group-name* neighbor neighbor-id]

Release Information

Statement introduced in Junos OS Release 11.1.

Description

Associate a dynamic profile or a profile variable set with a VPLS instance.

Options

dynamic-profile-name—Name of the dynamic profile to attach to this routing instance.

The remaining option is explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Attaching Dynamic Profiles to Routing Instances on page 27
- Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 30

family vpls (Layer 2 Pseudowires)

Syntax

```
family vpls;
```

Hierarchy Level

[edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information

Statement introduced in Junos OS Release 11.1.

Description

Specify that the protocol family for the logical interface is VPLS.

Required Privilege Level

router—To view this statement in the configuration.
router-control—To add this statement to the configuration.

Related Documentation

- Applying the Policers to Dynamic Profile Interfaces on page 26
- Creating a Dynamic Profile for the Complex Configuration on page 29

firewall

Syntax

```
firewall {
  atm-policer atm-policer-name {
    ... atm-policer-configuration ...
  }
  family protocol-family-name {
    ... protocol-family-configuration ...
  }
  filter ipv4-filter-name {
    ... ipv4-filter-configuration ...
  }
  hierarchical-policer hierarchical-policer-name {
    ... hierarchical-policer-configuration ...
  }
  interface-set interface-set-name {
    ... interface-set-configuration ...
  }
  policer two-color-policer-name {
    ... two-color-policer-configuration ...
  }
  three-color-policer three-color-policer-name {
    ... three-color-policer-configuration ...
  }
}
```

Hierarchy Level

[edit],
[edit logical-systems *logical-system-name*]
[edit dynamic-profiles *profile-name*],

Release Information

Statement introduced before Junos OS Release 7.4.
Logical systems support introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure firewall filters.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- *Guidelines for Configuring Firewall Filters*
- *Guidelines for Configuring Service Filters*
- *Guidelines for Configuring Simple Filters*
- *Configuring Multifield Classifiers*
- *Using Multifield Classifiers to Set Packet Loss Priority*

layer2-policer

Syntax

```
layer2-policer {
  output-policer policer-name;
  output-three-color policer-name;
}
```

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Junos OS Release 11.1.

Description Specify the output policers to be used in the dynamic profile.

Options

output-policer ***policer-name***—Two-color output policer to associate with the interface. You define this policer at the **[edit firewall policer]** hierarchy level.

output-three-color ***policer-name***—Tricolor output policer to associate with the interface. You define this policer at the **[edit firewall]** hierarchy level.

Required Privilege Level

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

Related Documentation

- Applying the Policers to Dynamic Profile Interfaces on page 26
- Creating a Dynamic Profile for the Complex Configuration on page 29

logical-interface-policer

Syntax logical-interface-policer;

Hierarchy Level [edit dynamic-profiles *profile-name* firewall policer *policer-name*],
[edit dynamic-profiles *profile-name* firewall three-color-policer *name*],
[edit firewall atm-policer*atm-policer-name*],
[edit firewall policer *policer-name*],
[edit firewall policer *policer-template-name*],
[edit firewall three-color-policer *policer-name*],
[edit logical-systems *logical-system-name* firewall policer *policer-name*],
[edit logical-systems *logical-system-name* firewall three-color-policer *name*]

Release Information Statement introduced before Junos OS Release 7.4.
Support at the **[edit firewall three-color-policer *policer-name*]** hierarchy level introduced in Junos OS Release 8.2.
Logical systems support introduced in Junos OS Release 9.3.
Support at the **[edit dynamic-profiles ... policer *policer-name*]** and **[edit dynamic-profiles ... three-color-policer *name*]**hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description Configure a logical interface policer.

NOTE: 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.

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

Related Documentation

- *Two-Color and Three-Color Logical Interface Policers*
- *Traffic Policer Types*
- *Configuring and Applying Tricolor Marking Policers*
- *action*
- *Configuring Gigabit Ethernet Two-Color and Tricolor Policers*
- *action*

policer (Configuring)

Syntax

```
policer policer-name {
  filter-specific;
  if-exceeding {
    bandwidth-limit bps;
    bandwidth-percent number;
    burst-size-limit bytes;
  }
  logical-bandwidth-policer;
  logical-interface-policer;
  physical-interface-policer;
  shared-bandwidth-policer;
  then {
    policer-action;
  }
}
```

Hierarchy Level

[edit dynamic-profiles *profile-name* firewall],
[edit firewall],
[edit logical-systems *logical-system-name* firewall]

Release Information

Statement introduced before Junos OS Release 7.4.
The **out-of-profile** policer action added in Junos OS Release 8.1.
The **logical-bandwidth-policer** statement added in Junos OS Release 8.2.
Logical systems support introduced in Junos OS Release 9.3.
The **physical-interface-policer** statement introduced in Junos OS Release 9.6.
The **shared-bandwidth-policer** statement added in Junos OS Release 11.2.
Support at the **[edit dynamic-profiles ... firewall]** 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 firewall]** hierarchy level, the **policer** 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 **policer-action** modifier in the **then** statement in a firewall filter term or on an interface.

Options

policer-action—One or more actions to take:

- **discard**—Discard traffic that exceeds the rate limits.
- **forwarding-class** *class-name*—Specify the particular forwarding class.
- **loss-priority**—Set the packet loss priority (PLP) to **low**, **medium-low**, **medium-high**, or **high**.

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. See CLI Explorer.

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

Related Documentation
- *Bandwidth Policer Overview*
- *Configuring Firewall Filters and Policers for VPLS*
- *Configuring Multifield Classifiers*
- *Logical Interface (Aggregate) Policer Overview*
- *Physical Interface Policer Overview*
- *Single-Rate Two-Color Policer Overview*
- *Using Multifield Classifiers to Set Packet Loss Priority*
- *filter (Configuring)*
- *priority (Schedulers)*

profile-variable-set (Dynamic Profiles)

Syntax
```
profile-variable-set {
  variable-set-name {
    junos-layer2-output-policer policer-name;
  }
}
```

Hierarchy Level
[edit dynamic-profiles *profile-name*]

Release Information
Statement introduced in Junos OS Release 11.1.

Description
Specify the policer used in the variable set.

Options
junos-layer2-output-policer *policer-name*—Layer 2 policer that you want to substitute in the dynamic profile. You define this policer at the **[edit firewall policer]** hierarchy level.

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

Related Documentation
- Applying the Policers to Dynamic Profile Interfaces on page 26
- Creating a Dynamic Profile for the Complex Configuration on page 29

profile-variable-set (Routing Instances)

Syntax profile-variable-set *variable-set-name*

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 ***variable-set-name***—Name of the variable set to use when this dynamic profile is applied to the routing instance. You define this variable set at the **[edit dynamic-profiles *profile-name*]** hierarchy level.

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

Related Documentation

- Attaching Dynamic Profiles to Routing Instances for the Complex Configuration on page 30

