



JunosE™ Software for E Series™ Broadband Services Routers

Hierarchical Policy Management

Release

13.1.x



Published: 2012-03-26

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

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

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

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.

JunosE™ Software for E Series™ Broadband Services Routers Hierarchical Policy Management
Release 13.1.x
Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

Revision History
April 2012—FRS JunosE 13.1.x

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

YEAR 2000 NOTICE

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

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
	E Series and JunosE Documentation and Release Notes	ix
	Audience	ix
	E Series and JunosE Text and Syntax Conventions	ix
	Obtaining Documentation	xi
	Documentation Feedback	xi
	Requesting Technical Support	xi
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xii
Part 1	Overview	
Chapter 1	Hierarchical Policies for Interface Groups	3
	Hierarchical Policies for Interface Groups Overview	3
	External Parent Groups	3
	Hierarchical Aggregation Nodes	4
	RADIUS and Profile Configuration for Hierarchical Policies	5
	Interface Profiles for Service Manager Overview	5
Part 2	Configuration	
Chapter 2	Configuration Overview	9
	Hierarchical Policy Configuration Considerations	9
Chapter 3	Examples	11
	Example: Configuring Hierarchical Policy Parameters	11
	Example: Hierarchical Policy Quick Configuration	13
	Example: Configuring Hierarchical Policies	13
	Example: VLAN Rate Limit Hierarchical Policy for Interface Groups Configuration	17
	Example: Wholesale L2TP Model Hierarchical Policy Configuration	20
	Example: Aggregate Rate Limit for All Nonvoice Traffic Hierarchical Policy Configuration	23
	Example: Arbitrary Interface Groups Hierarchical Policy Configuration	26
	Example: Service and User Rate-Limit Hierarchy Overlap Hierarchical Policy Configuration	29
	Example: Percentage-Based Hierarchical Rate-Limit Profile for External Parent Group	31
	Example: PPP Interfaces Hierarchical Policy Configuration	33

Part 3	Administration	
Chapter 4	Monitoring Tasks	41
	Monitoring External Parent Groups	41
Part 4	Index	
	Index	45

List of Figures

Part 2	Configuration	
Chapter 3	Examples	11
	Figure 1: Configuration Process	14
	Figure 2: VLAN Rate-Limit Configuration	17
	Figure 3: Interface Stack for Wholesale L2TP Mode	21
	Figure 4: Wholesale L2TP Configuration	22
	Figure 5: Interface Stack for Aggregate Rate Limit	23
	Figure 6: Aggregate Rate Limit for Nonvoice Traffic Configuration	25
	Figure 7: Interface Stack for Arbitrary Interface Groups	27
	Figure 8: Arbitrary Interface Groups Configuration	27
	Figure 9: Interface Stack for Service and User Rate-Limit Hierarchy Overlap	29
	Figure 10: Service and User Rate-Limit Hierarchy Overlap Configuration	30
	Figure 11: Interface Stack for Hierarchical Policy Configuration	35

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Part 2	Configuration	
Chapter 3	Examples	11
	Table 3: Shorthand Notation Mapping	12
Part 3	Administration	
Chapter 4	Monitoring Tasks	41
	Table 4: show parent-group Output Fields	41

About the Documentation

- E Series and JunosE Documentation and Release Notes on page ix
- Audience on page ix
- E Series and JunosE Text and Syntax Conventions on page ix
- Obtaining Documentation on page xi
- Documentation Feedback on page xi
- Requesting Technical Support on page xi

E Series and JunosE Documentation and Release Notes

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

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

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

Audience

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

E Series and JunosE Text and Syntax Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	<ul style="list-style-type: none"> Issue the clock source command. Specify the keyword exp-msg.
Bold text like this	Represents text that the user must type.	host1(config)#traffic class low-loss1
Fixed-width text like this	Represents information as displayed on your terminal's screen.	host1#show ip ospf 2 Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an Area Border Router (ABR)
<i>Italic text like this</i>	<ul style="list-style-type: none"> Emphasizes words. Identifies variables. Identifies chapter, appendix, and book names. 	<ul style="list-style-type: none"> There are two levels of access: <i>user</i> and <i>privileged</i>. <i>clusterId</i>, <i>ipAddress</i>. <i>Appendix A, System Specifications</i>
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
<i>Italic text like this</i>	Represents variables.	<i>mask</i> , <i>accessListName</i>

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

Convention	Description	Examples
(pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic line
[] (brackets)	Represent optional keywords or variables.	[internal external]
[]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 level2 l1]*
{ } (braces)	Represent required keywords or variables.	{ permit deny } { in out } { clusterId ipAddress }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at <http://www.juniper.net/>.

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

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

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

Documentation Feedback

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

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or 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

- [Hierarchical Policies for Interface Groups on page 3](#)

CHAPTER 1

Hierarchical Policies for Interface Groups

- [Hierarchical Policies for Interface Groups Overview on page 3](#)
- [External Parent Groups on page 3](#)
- [Hierarchical Aggregation Nodes on page 4](#)
- [RADIUS and Profile Configuration for Hierarchical Policies on page 5](#)
- [Interface Profiles for Service Manager Overview on page 5](#)

Hierarchical Policies for Interface Groups Overview

Hierarchical policies allow classifier groups and parent groups within a policy to point to line module global parent groups. The line module global parent groups (external parent groups) can point to other external parent groups. Full intra-interface policy hierarchies for all forwarding layer policies allow classified flows within a policy attachment to share bandwidth. Bandwidth-sharing between interfaces uses line module global parent group definitions and interface grouping. However, if you need to share bandwidth between two or more interfaces, rate-limits must be chained beyond a single attachment.

Policies for interface groups include external parent groups that are implicitly instantiated during policy attachment based on each unique interface group encountered.

Related Documentation

- [Hierarchical Policy Configuration Considerations on page 9](#)

External Parent Groups

Parent groups act as nonleaf nodes in a hierarchical policy. You can build a hierarchy of policers using classifier groups as leaf nodes and parent groups as parent nodes within a policy list. Each classifier group (with or without a rate limit) can point to a single parent group and that parent group can point to another parent group. To avoid undefined hierarchies, each node can only point to one other node.

The inter-interface hierarchical model includes references to parent groups that are defined externally from a policy list. This enables you to define hierarchical nodes outside the scope of a policy-list attachment. In Global Configuration mode, each external parent group can have a rate-limit profile defined and have a reference to another external parent group.

The classifier groups and parent groups within a policy list can point to external parent groups for all policies that implement hierarchical policies. Each external parent group reference must also have a policy parameter name.

External parent group names are global. Internal parent group names are local to each policy configuration. Because both of these name spaces are different, you can configure overlapping names.

**Related
Documentation**

- Parent Group Merge Algorithm
- [Monitoring External Parent Groups on page 41](#)

Hierarchical Aggregation Nodes

An internal parent group configured within a policy defines a hierarchical aggregation node template. An attachment of this policy creates an aggregation node for each internal parent group in a policy. Aggregation nodes are scoped within a single attachment and cannot be shared beyond a single attachment. An aggregation node stores a single rate-limit instance and statistics for this rate-limit. Aggregate nodes can be shared between two or more classified flows within a single attachment using the classifier group and parent group association.

Rate-limit aggregation nodes extend beyond a single attachment so classified flows across two or more attachments can reference the same aggregation node to share a single rate-limit instance. You can use external parent groups and policy parameters for sharing aggregate nodes across policy attachments. Each external parent group reference in a policy is accompanied by a parameter that is resolved during the attachment of the policy to an interface. An external rate-limit aggregation node can be defined by the 4-tuple (slot, direction, external parent group name, parameter value). The slot is the logical number of the line module location and the direction can be ingress or egress at the line module.

When you use hierarchical aggregation nodes, be aware of the following:

- VR/VRF—The hierarchical aggregate nodes based on external parent groups are not virtual router sensitive. The configuration allows interfaces from different virtual routers to have the same parameter name to value mapping, in which case both interfaces could share the same aggregate node created by an external parent group.
- Direction of Traffic—Hierarchical aggregate nodes are direction sensitive. The configuration does not allow input and output traffic at an interface to share the same rate-limit instance. Even when the input and output policy attachments refer to the same external parent group and parameter value, two separate aggregate nodes are created for each direction.
- Line Module—You should use hierarchical aggregate nodes. Rate limits cannot be shared across different line modules or service modules. Even when you configure the same parameter name to the same value for an external parent group, different rate-limit instances are instantiated if the interfaces are on different line modules.

- Related Documentation**
- [Policy Attachment Rules for Merged Policies](#)

RADIUS and Profile Configuration for Hierarchical Policies

You can use profiles to configure policy parameters. There is currently no RADIUS VSA support for policy parameters. Each reference to an external parent group and the chain of references from that group to other parent groups in a series requires one parent group resource for each reference and each attachment of the policy containing these references.

The rule that applies to external parent group resource count is: one resource per (interface, policy attachment type, policy name, external parent group name, parameter name) tuple; interface is the interface where the policy is attached and policy attachment type is the type of policy attachment.

A rate-limit instance for the external parent groups is created for each hierarchical aggregation node, which is a combination of (slot, direction, parent group name, parameter value) tuple; where slot is the slot number, direction is ingress or egress. A rate-limit resource will be consumed for each instance created.

If at least one policy attachment that uses an external parent group reference has statistics enabled, then statistics for the rate-limit configured within the external parent group is enabled. Each hierarchical aggregation node requires five statistics resources.

- Related Documentation**
- [Hierarchical Policies for Interface Groups Overview on page 3](#)

Interface Profiles for Service Manager Overview

Applying a profile to the interface where the subscriber sends and receives traffic activates service for a subscriber. Similarly, to deactivate a service, you reapply the respective profile with a negate flag.

You can use a profile to apply the policy parameters configuration for an interface. When you apply a profile containing relevant policy parameter commands to an interface, the parameter configuration is uniquely maintained for each dynamic interface created using this profile. The policy parameters are not deactivated when the corresponding service containing them is deactivated and can only be modified or created by service activations.

If you write service manager macros, you should define the rate-limit hierarchy when you create the policies and profiles associated with the services to be deployed.

- Related Documentation**
- [Hierarchical Policies for Interface Groups Overview on page 3](#)

PART 2

Configuration

- [Configuration Overview on page 9](#)
- [Examples on page 11](#)

CHAPTER 2

Configuration Overview

- [Hierarchical Policy Configuration Considerations on page 9](#)

Hierarchical Policy Configuration Considerations

When you configure hierarchical policies for interface groups, be aware of the following considerations:

- **Loops**—The system performs basic checks to prevent formation of loops when external parent groups refer to other external parent groups. Also, you cannot chain together more than four rate-limits in a hierarchy.
- **Asynchronous Policy Parameter Configuration**—You can individually configure the policy parameter configuration in an interface and the policy attachments. If a policy parameter is not configured in the interface before a policy is attached, the value configured in Global Configuration mode for this parameter is used. You can later change the parameter value for the interface.
- **Asynchronous Parent Group Rate Limit Configuration**—You can configure an external parent group without a rate-limit-profile reference. In this case, the system does not invoke a rate-limit for the external parent group (even if other nodes point to it) and calls the next node in the hierarchy.
- **Parent Group Reference**—The configuration fails if you do not first create an external parent group before it is referenced elsewhere.

**Related
Documentation**

- [Hierarchical Policies for Interface Groups Overview on page 3](#)

CHAPTER 3

Examples

- [Example: Configuring Hierarchical Policy Parameters on page 11](#)
- [Example: Hierarchical Policy Quick Configuration on page 13](#)
- [Example: Configuring Hierarchical Policies on page 13](#)
- [Example: VLAN Rate Limit Hierarchical Policy for Interface Groups Configuration on page 17](#)
- [Example: Wholesale L2TP Model Hierarchical Policy Configuration on page 20](#)
- [Example: Aggregate Rate Limit for All Nonvoice Traffic Hierarchical Policy Configuration on page 23](#)
- [Example: Arbitrary Interface Groups Hierarchical Policy Configuration on page 26](#)
- [Example: Service and User Rate-Limit Hierarchy Overlap Hierarchical Policy Configuration on page 29](#)
- [Example: Percentage-Based Hierarchical Rate-Limit Profile for External Parent Group on page 31](#)
- [Example: PPP Interfaces Hierarchical Policy Configuration on page 33](#)

Example: Configuring Hierarchical Policy Parameters

You configure policy parameters in Global Configuration mode. Only hierarchical policy parameters can have external parent group references. Each parameter has a single value, depending on the type of parameter. The hierarchical policy parameter can have a single numeric value or a keyword.

In Interface Configuration mode, you can override the value for a policy parameter for each interface. The value for a parameter configured in Interface Configuration mode supersedes the value configured for the parameter in Global Configuration mode. However, if a parameter is not configured in Interface Configuration mode, the value configured in Global Configuration mode is used.

Each reference to a policy parameter in a policy is substituted with its value for all attachments of this policy at the interface. The value can come from the interface or global configuration for the parameter. Therefore, the value configured for the parameters referenced in policies can be different for attachments at different interfaces. This enables you to have an attachment-specific configuration in a policy list that is deferred until the policy is attached.

There are two types of values that a hierarchical policy parameter can take: numeric and keyword. Keywords are resolved to numeric values during configuration of a policy parameter at the interface.

The following example assigns a value of 10 to policy parameter A in Global Configuration mode.

```
host1(config)#policy-parameter A hierarchical
host1(config-policy-parameter)#aggregation-node 10
host1(config-policy-parameter)#exit
```

The following example assigns value 1 to policy parameter A and value 2 to policy parameter B in Interface Configuration mode. Also, the value configured for parameter A in interface fast3/0.1 overrides the value configured in the previous example.

```
host1(config)#interface fastEthernet 3/0.1
host1(config-interface)#ip policy-parameter hierarchical A 1
host1(config-interface)#ip policy-parameter hierarchical B 2
host1(config-interface)#exit
```

The following example assigns keyword **vlan** to parameter C in Global Configuration mode.

```
host1(config)#policy-parameter C hierarchical
host1(config-policy-parameter)#aggregation-node vlan
host1(config-policy-parameter)#exit
```

The following example assigns keyword **atm-vc** to parameter C in Interface Configuration mode. Policy parameter C is assigned with interface type atm-vc for IP interface at atm3/0.1. The keyword **atm-vc** is resolved to the identifier of the ATM minor interface on which the IP interface atm3/0.1 is stacked.

```
host1(config)#interface atm 3/0.1
host1(config-interface)#ip policy-parameter hierarchical C atm-vc
host1(config-interface)#exit
```

The following keywords are supported: **atm-vc**, **atm-vp**, **atm**, **ethernet**, **vlan**, **svlan**, **fr-vc**, **forwarding**, and **ppp-interface**. [Table 3 on page 12](#) indicates the mapping of shorthand notation to actual value that are used internally.

Table 3: Shorthand Notation Mapping

Shorthand number	Shorthand	Value	Supported in
1	ATM-VP vpi	Identifier constructed from slot, adapter, port, ATM VP id.	IP, IPv6, L2TP, and MPLS policies
2	ATM-VC	Unique identifier of the ATM minor interface	IP, IPv6, and MPLS policies
3	Ethernet	Unique identifier of Ethernet major interface	IP, IPv6, and MPLS policies
4	VLAN	Unique identifier of VLAN interface	IP, IPv6, and MPLS policies
5	SVLAN	Identifier constructed from slot, adapter, port, SVLAN ID.	IP, IPv6, L2TP, and MPLS policies

Table 3: Shorthand Notation Mapping (*continued*)

Shorthand number	Shorthand	Value	Supported in
6	FR-VC	Unique identifier of frame relay minor interface	IP, IPv6, and MPLS policies
7	ATM	Unique identifier of ATM major interface	IP, IPv6, and MPLS policies
8	Forwarding	Unique identifier of the forwarding interface where the parameter is configured.	IP, IPv6, L2TP, and MPLS policies
9	ppp-interface	Identifier constructed from PPP interface.	IP, IPv6 policies

Example: Hierarchical Policy Quick Configuration

To configure hierarchical policies for interface groups, use the following steps:

1. In Global Configuration mode, create rate limit profiles of the type hierarchical.
2. In Global Configuration mode, create policy parameters of the type hierarchical.
3. In Global Configuration mode, create external parent groups.
4. In Global Configuration mode, create a policy list and use the external parent groups and policy parameters to create a hierarchy of rate limits.
5. In Interface Configuration mode, attach the policy list to the interface.
6. (Optional) In Interface Configuration mode, specify values for the hierarchical policy parameters used by the policy list.

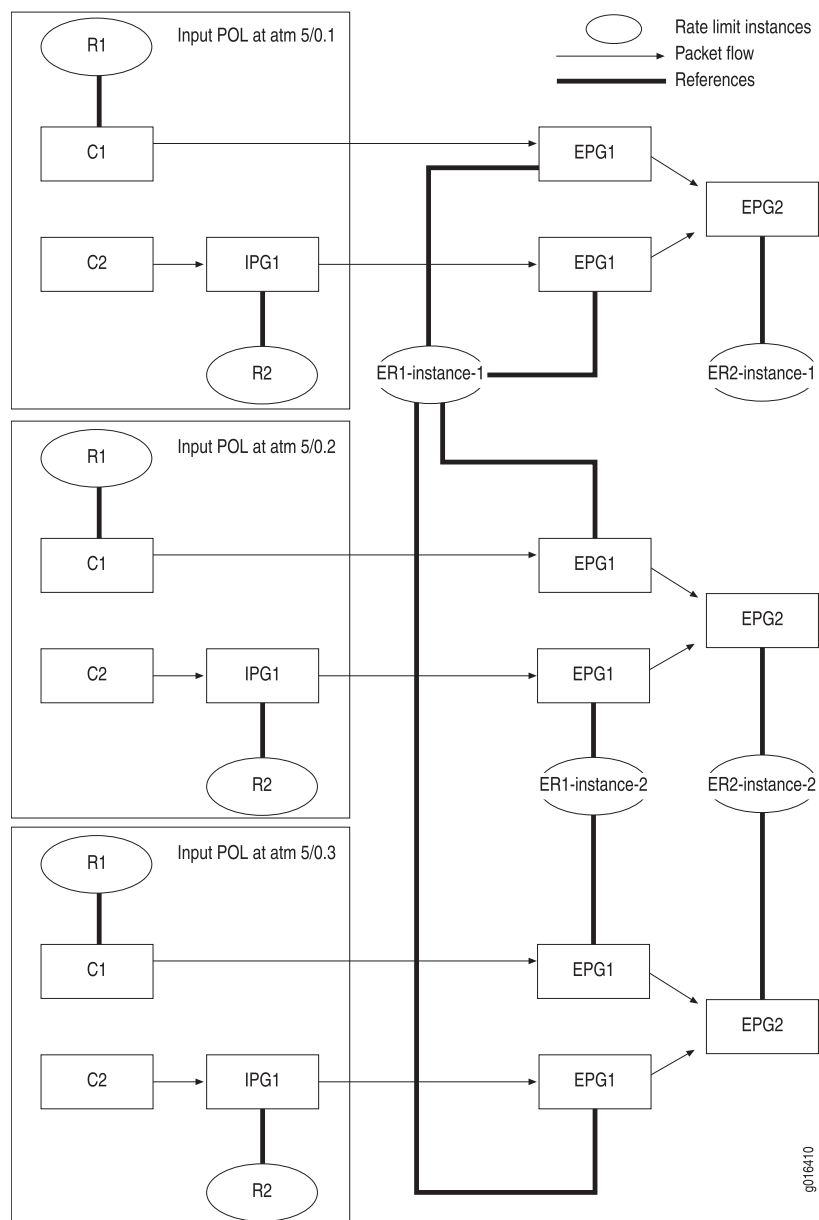
Related Documentation

- [Example: Configuring Hierarchical Policies on page 13](#)

Example: Configuring Hierarchical Policies

The configuration in [Figure 1 on page 14](#) requires four parent group resources for each atm5/0.1, atm5/0.2, and atm5/0.3 attachment. The rate-limit instance R1 is referenced by C1 and packet flows from C1 to EPG1 to EPG2.

Figure 1: Configuration Process



This procedure uses the following designations:

- EPG1 and EPG2 are external parent groups.
- IP1 and IP2 are internal parent groups.
- ER1, ER2, R1, and R2 are rate-limit profiles.
- POL is the name of the IP policy.
- C1 and C2 are classified flows.
- A, B, and C are policy parameters.

1. Configure two external parent groups EPG1 and EPG2. Create policy-parameter C and two external parent groups: EPG1 and EPG2.

```
host1(config)#policy-parameter C hierarchical
host1(config-policy-parameter)#exit
```

```
host1(config)#parent-group EPG2
host1(config-parent-group)#rate-limit-profile ER2
host1(config-parent-group)#exit
```

```
host1(config)#parent-group EPG1
host1(config-parent-group)#next-parent EPG2 parameter C
host1(config-parent-group)#rate-limit-profile ER1
host1(config-parent-group)#exit
```

EPG1 contains a rate-limit profile ER1 and points to EPG2 as the next parent group in series. The EPG2 reference is associated with policy parameter C. When you later use the **policy-parameter** command in Interface Configuration mode, actual values are substituted for the names. EPG2 contains a reference to rate-limit-profile ER2.

2. Configure IP policy list POL.

```
host1(config)#ip policy-list POL
host1(config-policy-list)#classifier-group C1 external parent-group EPG1 parameter
A
host1(config-policy-list-classifier-group)#rate-limit-profile R1
host1(config-policy-list-classifier-group)#exit
```

```
host1(config-policy-list)#classifier-group C2 parent-group IPG1
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
```

```
host1(config-policy-list)#parent-group IPG1 external parent-group EPG1 parameter
B
host1(config-parent-group)#rate-limit-profile R2
host1(config-policy-list-parent-group)#exit
```

A classified flow C1 references EPG1 as the next parent group to call in the hierarchy. This is an external parent group that is associated with policy parameter A. The C2 classified flow points to internal parent group IPG1, which contains rate-limit-profile R2 and points to EPG1 as the next parent group to call in the hierarchy. The EPG1 reference is associated with policy parameter B. When you later use the **policy-parameter** command in Interface Configuration mode, the policy parameters are given numeric values.

3. Attach POL to atm5/0.1 as an input policy.

```
host1(config)#interface atm 5/0.1
host1(config-interface)#ip policy-parameter hierarchical A 1
host1(config-interface)#ip policy-parameter hierarchical B 1
host1(config-interface)#ip policy-parameter hierarchical C 1
host1(config-interface)#ip policy input POL statistics enabled
host1(config-interface)#exit
```

Policy list POL contains three parameter names that must be substituted with actual values. This attachment contains two internal rate-limit instances, one for R1 and one for R2. This attachment also contains one parent group instance for IPG1, one parent-group instance for (EPG1, parameter A) tuple, one for (EPG1, parameter B) tuple, and one for (EPG2, parameter C) tuple. Value number 1 is substituted for parameters A, B, and C when you use the **policy-parameter** command. Because of this policy attachment and the **policy-parameter** command, the following aggregation nodes are created: (slot 5, ingress, EPG1, 1), (slot 5, ingress, EPG2, 1). The system creates a rate-limit instance for each aggregation node: ER1-instance-1 and ER2-instance-1, respectively. ER1-instance-1 is referenced in parent-group instances (EPG1, parameter A) and (EPG1, parameter B). ER2-instance-1 is referenced in the parent group instance (EPG2, parameter C).

4. Attach POL to atm5/0.2 as input policy.

```
host1(config)#interface atm 5/0.2
host1(config-interface)#ip policy-parameter hierarchical A 1
host1(config-interface)#ip policy-parameter hierarchical B 2
host1(config-interface)#ip policy-parameter hierarchical C 2
host1(config-interface)#ip policy input POL statistics enabled
host1(config-interface)#exit
```

Policy list POL contains three parameter names that must be substituted with actual values. This attachment consumes two internal rate-limit instances: one for R1 and one for R2. This attachment also consumes one parent group instance for IPG1, one parent-group instance for (EPG1, parameter A) tuple, one for (EPG1, parameter B) tuple, and one for (EPG2, parameter C) tuple as in Step 3. When you use the **policy-parameter** command, parameter A is substituted with value 1 and parameters B and C are substituted with value 2. Because of this policy attachment and the **policy-parameter** commands, the following aggregation nodes are identified: (slot 5, ingress, EPG1, 1), (slot 5, ingress, EPG1, 2), (slot 5, ingress, EPG2, 2). The (slot 5, ingress, EPG1, 1) node was already created in Step 3 and was named ER1-instance-1. The other two aggregation nodes are now created and named ER1-instance-2 and ER2-instance-2, respectively. ER1-instance-1 is referenced by parent-group instance (EPG1, parameter A), ER1-instance-2 is referenced by parent group instance (EPG1, parameter B), and ER2-instance-2 is referenced by the parent group instance (EPG2, parameter C).

5. Attach POL to atm5/0.3 as input policy.

```
host1(config)#interface atm 5/0.3
host1(config-interface)#ip policy-parameter hierarchical A 2
host1(config-interface)#ip policy-parameter hierarchical B 1
host1(config-interface)#ip policy-parameter hierarchical C 2
host1(config-interface)#ip policy input POL statistics enabled
host1(config-interface)#exit
```

Policy list POL contains three parameter names that need to be substituted with actual values. This attachment consumes two internal rate-limit instances: one for R1 and one for R2. This attachment also consumes one parent group instance for IPG1, one parent-group instance for (EPG1, parameter A) tuple, one for (EPG1, parameter B) tuple, and one for (EPG2, parameter C) tuple. When you use the **policy-parameter** command, parameters A and C are substituted with value 2 and parameter B is

substituted with value 1. Because of this policy attachment and use of the **policy-parameter** commands, the following aggregation nodes are identified; (slot 5, ingress, EPG1, 2), (slot 5, ingress, EPG1, 1), (slot 5, ingress, EPG2, 2). All three aggregation nodes were created in earlier steps and were named ER1-instance-2, ER1-instance-1, and ER2-instance-2, respectively. ER1-instance-2 is referenced by parent-group instances (EPG1, parameter A), ER1-instance-1 is referenced by parent-group instance (EPG1, parameter B), and ER2-instance-2 is referenced by the parent-group instance (EPG2, parameter C).

Related Documentation

- [Example: Hierarchical Policy Quick Configuration on page 13](#)

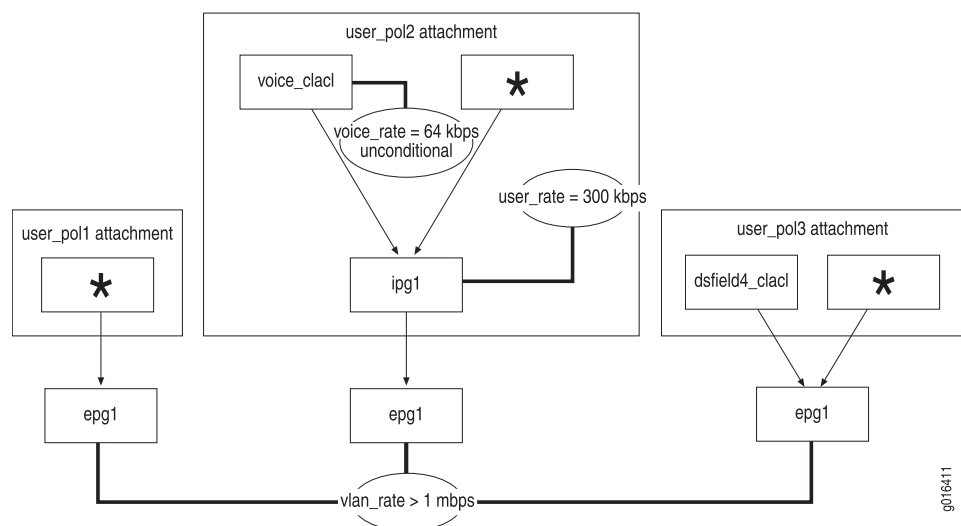
Example: VLAN Rate Limit Hierarchical Policy for Interface Groups Configuration

In this example, three users from a small business office are connected to an E Series router through the same VLAN interface. The contracted maximum for the business is 1 Mbps in the upstream direction. The downstream direction is served through QoS profiles and therefore is not shown here.

Figure 2 on page 17 shows the following:

- User user_pol1 is attached to the first user's IP interface and does not have a rate limit.
- User user_pol2 is attached the second user's interface and has an individual rate limit of 300Kbps and preferred voice traffic at 64Kbps.
- User user_pol3 is attached to the third user's interface and has some traffic marked with a low delay (Dsfield = 4), but there are no rate limitations applied.
- Policer instance VLAN_RATE is shared across all three instances of EPG1 and limits the total upstream traffic from three users to 1 Mbps.

Figure 2: VLAN Rate-Limit Configuration



1. Create a rate limit to enforce the contracted maximum for the small business. Create an external parent group to hold this rate limit.

```
host1(config)#rate-limit-profile VLAN_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 1000000
host1(config-rate-limit-profile)#committed-action transmit final
host1(config-rate-limit-profile)#exit
```

```
host1(config)#parent-group EPG1
host1(config-parent-group)#rate-limit-profile VLAN_RATE
host1(config-parent-group)#exit
```

Verify the parent group configuration.

```
host1#show parent-group EPG1
```

```

                                     Parent Group Table
                                -----
Parent Group EPG1
  Reference count: 0
  Rate limit profile: VLAN_RATE
```

2. Create a policy list to attach to user 1.

```
host1(config)#policy-parameter A hierarchical
host1(config-policy-parameter)#exit
```

```
host1(config)#ip policy-list USER_POL1
host1(config-policy-list)#classifier-group * external parent-group EPG1
  parameter A
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
```

Verify the policy list configuration.

```
host1#show policy-list USER_POL1
```

```

                                     Policy Table
                                -----
IP Policy USER_POL1
  Administrative state: enable
  Reference count:      0
  Classifier control list: *, precedence 100, external parent-group EPG1
  parameter A
    forward
```

3. Create a policy list to attach to user 2. Also, create a rate limit to police voice traffic and another rate limit to police all traffic for user 2. Because voice traffic is preferred, it borrows the tokens unconditionally from all aggregate policers in the hierarchy.

```
host1(config)#rate-limit-profile VOICE_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 64000
host1(config-rate-limit-profile)#committed-action transmit unconditional
host1(config-rate-limit-profile)#exit
```

```
host1(config)#rate-limit-profile USER_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 300000
```

```
host1(config-rate-limit-profile)#committed-action transmit conditional
host1(config-rate-limit-profile)#exit
```

```
host1(config)#ip classifier-list VOICE_CLACL udp any any eq 10000
```

```
host1(config)#ip policy-list USER_POL2
host1(config-policy-list)#classifier-group VOICE_CLACL parent-group IPG1
host1(config-policy-list-classifier-group)#rate-limit-profile VOICE_RATE
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group * parent-group IPG1
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#parent-group IPG1 external parent-group EPG1
parameter A
host1(config-policy-list-parent-group)#rate-limit-profile USER_RATE
host1(config-policy-list-parent-group)#exit
host1(config-policy-list)#exit
```

Verify the policy list configuration.

```
host1#show policy-list USER_POL1
```

```

                                Policy Table
                                -----
IP Policy USER_POL2
  Administrative state: enable
  Reference count:      0
  Classifier control list: VOICE_CLACL, precedence 100, parent-group IPG1

    rate-limit-profile VOICE_RATE
  Classifier control list: *, precedence 100, parent-group IPG1
    forward
  Parent group: IPG1, external parent-group EPG1 parameter A
    rate-limit-profile USER_RATE
```

4. Create a policy list to attach to user 3 and mark Dsfield=4 traffic with a special traffic class.

```
host1(config)#ip classifier-list DSFIELD4_CLACL ip any any dsfield 4
host1(config)#ip policy-list USER_POL3
host1(config-policy-list)#classifier-group DSFIELD4_CLACL external parent-group
EPG1 parameter A
host1(config-policy-list-classifier-group)#traffic-class LOW_DROP
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group * external parent-group EPG1
parameter A
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
```

The policies created earlier are attached statically to the user's corresponding entry interface in the E Series router. In this case, fast3/0.1 connects to user 1, fast3/0.2 connects to user 2, and fast3/0.3 connects to user 3.

5. Create the major interface.

```
host1(config)#interface fastEthernet 3/0
host1(config-interface)#encapsulation vlan
```

```
host1(config-interface)#exit
```

6. Create an interface for user 1, attach USER_POL1, and map parameter A to the VLAN interface stacked below the shared IP interface.

```
host1(config)#interface fastEthernet 3/0.1
host1(config-interface)#vlan id 1
host1(config-interface)#exit
```

```
host1(config)#interface ip 3/0.1.1
host1(config-interface)#ip policy-parameter hierarchical A vlan
host1(config-interface)#ip policy input USER_POL1 statistics enabled
host1(config-interface)#exit
```

7. Create the interface for user 2, attach USER_POL2, and map parameter A to the VLAN interface.

```
host1(config)#interface ip 3/0.1.2
host1(config-interface)#ip policy-parameter hierarchical A vlan
host1(config-interface)#ip policy input USER_POL2 statistics enabled
host1(config-interface)#exit
```

8. Create the interface for user 3, attach USER_POL3, and map parameter A to the VLAN interface.

```
host1(config)#interface ip 3/0.1.3
host1(config-interface)#ip policy-parameter hierarchical A vlan
host1(config-interface)#ip policy input USER_POL3 statistics enabled
host1(config-interface)#exit
```

9. For dynamic users, under each user's record in RADIUS, you can specify the ingress policy name. However, you can only specify the policy parameter through the profile.

```
host1(config)#profile PPPOE_PROF1
host1(config-profile)#ip policy-parameter hierarchical A vlan
host1(config-profile)#exit
```

```
host1(config)#interface fastEthernet 3/0.1
host1(config-interface)#vlan id 1
host1(config-interface)#encapsulation pppoe
host1(config-interface)#profile PPPOE_PROF1
host1(config-interface)#pppoe auto-configure
host1(config-interface)#exit
```

Related Documentation

- [Hierarchical Rate Limits Overview](#)

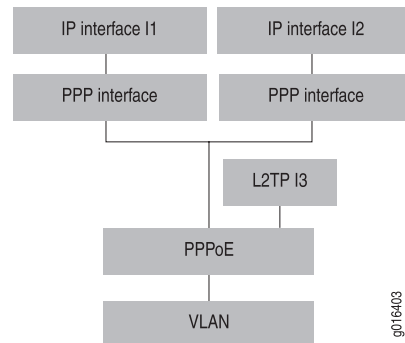
Example: Wholesale L2TP Model Hierarchical Policy Configuration

In this example:

- There are two terminated subscribers and their corresponding IP interfaces are I1 & I2 in the E-serier router.
- There is a single tunneled subscriber whose interface is I3.

- Interfaces I1 and I2 have dedicated 1 Mbps bandwidth each and interface I3 has dedicated 10 Mbps bandwidth. However, if interface I3 is not forwarding any traffic, then the allocated 10 Mbps can be shared by interfaces I1 and I2. Therefore, interfaces I1 and I2 can individually go up to a maximum of 11 Mbps if only one is actively sending traffic. If both interfaces are actively sending traffic, they can both get a maximum of 6 Mbps. However, any time interface I3 is actively sending traffic, it can forward up to the contracted 10 Mbps and interfaces I1 and I2 fall back to 1 Mbps.

Figure 3: Interface Stack for Wholesale L2TP Mode

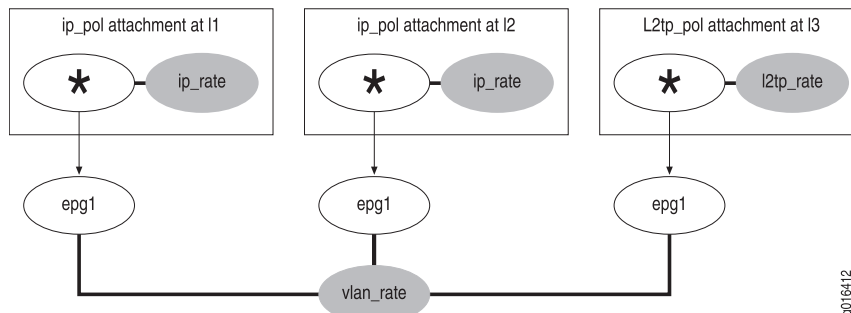


To use this example, you must configure the following:

- At interfaces I1 and I2:
 - IP_RATE, Committed Rate:1 Mbps
 - Peak Rate: 11 Mbps
 - Committed Action: transmit unconditional
 - Conformed Action: transmit conditional
 - Exceeded Action: drop
- At I3—L2TP_RATE:
 - Committed Rate: 10 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit unconditional
 - Conformed Action: drop
 - Exceeded Action: drop
- Policers at I1, I2, and I3 feed into a single policer that has the following configuration:
 - VLAN_RATE, Committed Rate: 12 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit final

- Conformed Action: drop
- Exceeded Action: drop
- IP policy USER_POL1 is attached as input to I1, IP policy USER_POL2 is attached as input to I2, and L2TP policy USER_POL3 is attached as input to I3.
- Policer instance VLAN_RATE is shared across all three instances of EPG1.

Figure 4: Wholesale L2TP Configuration



1. Create a rate-limit that can be shared across all forwarding interfaces. Create an external parent group to hold this rate limit.

```
host1(config)#rate-limit-profile VLAN_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 12000000
host1(config-rate-limit-profile)#committed-action transmit final
host1(config-rate-limit-profile)#exit
```

```
host1(config)#parent-group EPG1
host1(config-parent-group)#rate-limit-profile VLAN_RATE
host1(config-parent-group)#exit
```

2. Create a policy list to attach to users 1 and 2.

```
host1(config)#rate-limit-profile IP_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 1000000
host1(config-rate-limit-profile)#committed-action transmit unconditional
host1(config-rate-limit-profile)#peak-rate 11000000
host1(config-rate-limit-profile)#conformed-action transmit conditional
host1(config-rate-limit-profile)#exit
```

```
host1(config)#policy-parameter A hierarchical
host1(config-policy-parameter)#exit
host1(config)#ip policy-list IP_POL
host1(config-policy-list)#classifier-group * external parent-group EPG1
parameter A
host1(config-policy-list-classifier-group)#rate-limit-profile IP_RATE
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
```

3. Create a policy list to attach to user 3.

```
host1(config)#rate-limit-profile L2TP_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 10000000
host1(config-rate-limit-profile)#committed-action transmit unconditional
```

```
host1(config-rate-limit-profile)#exit
```

```
host1(config)#l2tp policy-list L2TP_POL
host1(config-policy-list)#classifier-group * external parent-group EPG1
parameter A
host1(config-policy-list-classifier-group)#rate-limit-profile L2TP_RATE
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
```

4. In both terminated users' record in RADIUS, you must specify the ingress policy name IP_POL. You must specify the ingress policy name L2TP_POL in the tunneled user's record in RADIUS. However, be sure to specify the policy parameter through a profile.

```
host1(config)#profile PPPOE_PROFI
host1(config-profile)#ip policy-parameter hierarchical A 1
host1(config-profile)#l2tp policy-parameter hierarchical A 1
host1(config-profile)#exit
```

```
host1(config)#interface fastEthernet 3/0.1
host1(config-interface)#vlan id 1
host1(config-interface)#encapsulation pppoe
host1(config-interface)#profile PPPOE_PROFI
host1(config-interface)#pppoe auto-configure
host1(config-interface)#exit
```

Related Documentation

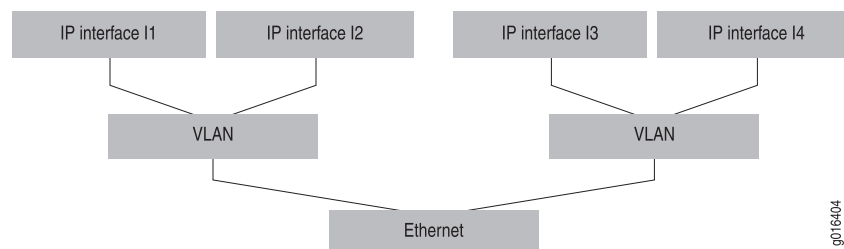
- Hierarchical Rate Limits Overview

Example: Aggregate Rate Limit for All Nonvoice Traffic Hierarchical Policy Configuration

In this example:

- There are four IP sessions and their corresponding interfaces are I1, I2, I3, and I4.
- Each interface corresponds to a dynamic user.
- All users can send a maximum of 1 Mbps video traffic each, but the total bandwidth for all video traffic combined is 1.5 Mbps for a specific VLAN.
- Similarly, all users can send a maximum of 5 Mbps data traffic, but the sum of all data traffic on an Ethernet port is 10 Mbps. Interfaces I1-I4 are interfaces where you can attach policies.

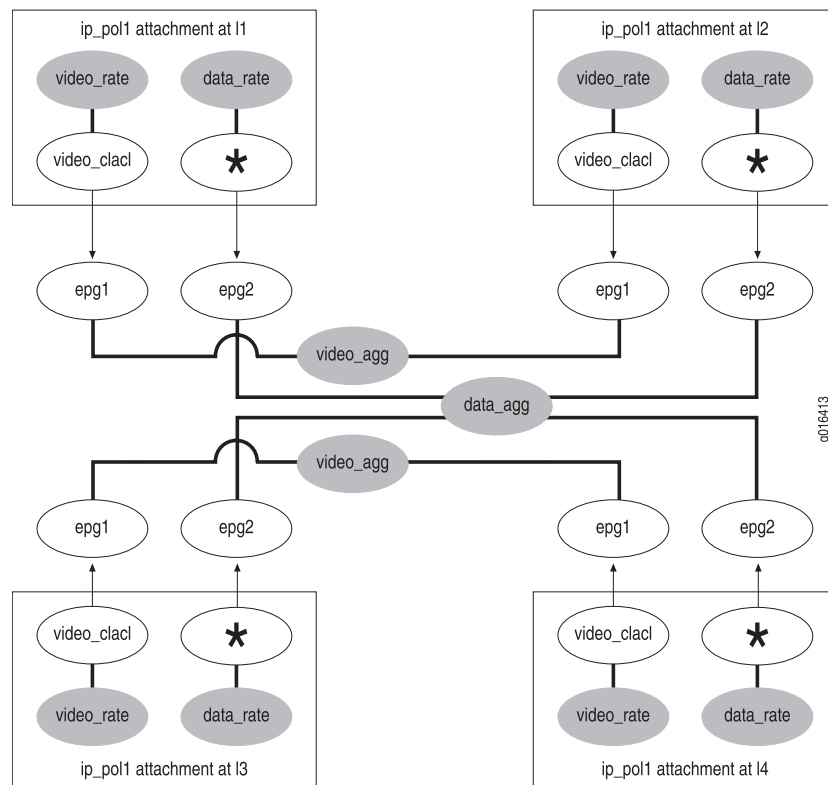
Figure 5: Interface Stack for Aggregate Rate Limit



This example uses the following:

- At I1, I2, I3, I4:
 - Classified Video Flow. VIDEO_RATE, Committed Rate: 1 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit conditional
 - Conformed Action: drop
 - Exceeded Action: drop
- At I1, I2, I3, I4:
 - Classified Data Flow. DATA_RATE, Committed Rate: 5 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit conditional
 - Conformed Action: drop
 - Exceeded Action: drop
- All classified video flow policers over each VLAN interface feed into a single policer with the following configuration:
 - VIDEO_AGG, Committed Rate: 1.5 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit final
 - Conformed Action: drop
 - Exceeded Action: drop
- All classified data flow policers over each Ethernet port feed into a single policer with the following configuration:
 - DATA_AGG, Committed Rate: 10 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit final
 - Conformed Action: drop
 - Exceeded Action: drop
- Policy IP_POL1 is attached to I1, I2, I3, and I4

Figure 6: Aggregate Rate Limit for Nonvoice Traffic Configuration



1. Create a rate limit that can be shared across all video streams. Create an external parent group to hold this rate limit.

```
host1(config)#rate-limit-profile VIDEO_AGG two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 1500000
host1(config-rate-limit-profile)#committed-action transmit final
host1(config-rate-limit-profile)#exit
```

```
host1(config)#parent-group EPG1
host1(config-parent-group)#rate-limit-profile VIDEO_AGG
host1(config-parent-group)#exit
```

2. Create a policy list to attach to all IP sessions.

```
host1(config)#rate-limit-profile VIDEO_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 1000000
host1(config-rate-limit-profile)#committed-action transmit conditional
host1(config-rate-limit-profile)#exit
```

```
host1(config)#rate-limit-profile DATA_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 5000000
host1(config-rate-limit-profile)#committed-action transmit conditional
host1(config-rate-limit-profile)#exit
```

```
host1(config)#policy-parameter A hierarchical
host1(config-policy-parameter)#exit
```

```
host1(config)#policy-parameter B hierarchical
host1(config-policy-parameter)#exit
```

```
host1(config)#ip policy-list IP_POL1
host1(config-policy-list)#classifier-group VIDEO_CLACL external parent-group EPG1
parameter A
host1(config-policy-list-classifier-group)#rate-limit-profile VIDEO_RATE
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group * external parent-group EPG2
parameter B
host1(config-policy-list-classifier-group)#rate-limit-profile DATA_RATE
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
```

3. In all users' records in RADIUS, specify the ingress policy name IP_POL1. However, be sure to specify the policy parameter through the profile.

```
host1(config)#profile PPPOE_PROF1
host1(config-profile)#ip policy-parameter hierarchical A vlan
host1(config-profile)#ip policy-parameter hierarchical B ethernet
host1(config-profile)#exit
```

```
host1(config)#interface fastEthernet 3/0.1
host1(config-interface)#vlan id 1
host1(config-interface)#encapsulation pppoe
host1(config-interface)#profile PPPOE_PROF1
host1(config-interface)#pppoe auto-configure
host1(config-interface)#exit
```

Related Documentation

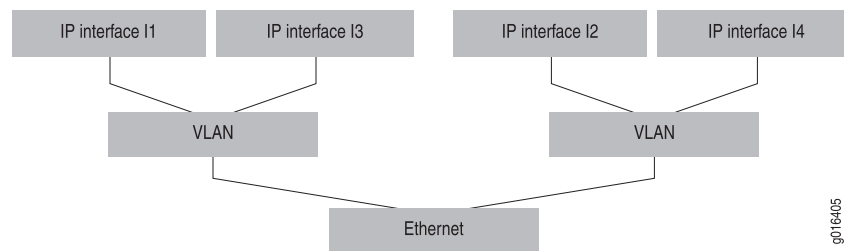
- [Hierarchical Rate Limits Overview](#)

Example: Arbitrary Interface Groups Hierarchical Policy Configuration

In this example, there are four terminated sessions and their corresponding IP interfaces are I1, I2, I3, and I4. [Figure 7 on page 27](#) shows the following:

- Sessions I1 and I2 are for the same subscriber: I1 carries only voice traffic and I2 carries all other traffic for this subscriber
- Sessions I3 and I4 are for another subscriber.
- Voice traffic has a contracted minimum of 64 Kbps, but the combined voice and other traffic for each subscriber has a contracted maximum of 1 Mbps.
- Interfaces I1-I4 are interfaces where you can attach policies.

Figure 7: Interface Stack for Arbitrary Interface Groups

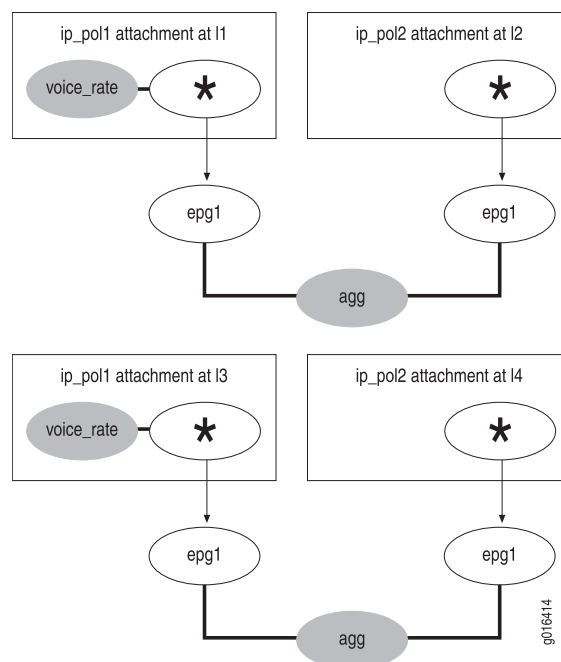


g016405

This example uses the following:

- At I1 and I3:
 - VOICE_RATE, Committed Rate: 64 Kbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit unconditional
 - Conformed Action: drop
 - Exceeded Action: drop
- At I2 and I4:
 - No policer configured
- I1 and I2 feed into a single policer with the following configuration: AGG, Committed Rate: 1 Mbps, Peak Rate: 0 Mbps, Committed Action: transmit, Conformed Action: drop, Exceeded Action: drop

Figure 8: Arbitrary Interface Groups Configuration



g016414

1. Create an aggregate rate limit that can be shared across multiple interfaces. Create an external parent group to hold this rate limit.

```
host1(config)#rate-limit-profile AGG two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 1000000
host1(config-rate-limit-profile)#committed-action transmit final
host1(config-rate-limit-profile)#exit
```

```
host1(config)#parent-group EPG1
host1(config-parent-group)#rate-limit-profile AGG
host1(config-parent-group)#exit
```

2. Create a policy list to be attached to all voice sessions.

```
host1(config)#rate-limit-profile VOICE_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 64000
host1(config-rate-limit-profile)#committed-action transmit unconditional
host1(config-rate-limit-profile)#exit
```

```
host1(config)#policy-parameter A hierarchical
host1(config-policy-parameter)#exit
```

```
host1(config)#ip policy-list IP_POL1
host1(config-policy-list)#classifier-group * external parent-group EPG1
parameter A
host1(config-policy-list-classifier-group)#rate-limit-profile VOICE_RATE
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
```

3. Create a policy list to attach to all other sessions.

```
host1(config)#ip policy-list IP_POL2
host1(config-policy-list)#classifier-group * external parent-group EPG1
parameter A
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
```

4. Attach IP_POL1 to the voice session of first user and attach IP_POL2 to the other session for the same user. Specify the same ID for parameter A.

```
host1(config)#interface fastEthernet 3/0.1
host1(config-interface)#vlan id 1
host1(config-interface)#exit
```

```
host1(config)#interface ip 3/0.1.1
host1(config-interface)#ip policy-parameter hierarchical A 1
host1(config-interface)#ip policy input IP_POL1 statistics enable
host1(config-interface)#exit
```

```
host1(config)#interface fastEthernet 3/0.2
host1(config-interface)#vlan id 2
host1(config-interface)#exit
```

```
host1(config)#interface ip 3/0.2.1
host1(config-interface)#ip policy-parameter hierarchical A 1
```



```
host1(config-interface)#ip policy input IP_POL2 statistics enable
host1(config-interface)#exit
```

5. Attach IP_POL1 to the voice session of the second user and attach IP_POL2 to the other session for the same user. Specify a different ID for parameter A.

```
host1(config)#interface ip 3/0.1.2
host1(config-interface)#ip policy-parameter hierarchical A 2
host1(config-interface)#ip policy input IP_POL1 statistics enable
host1(config-interface)#exit
```

```
host1(config)#interface ip 3/0.2.2
host1(config-interface)#ip policy-parameter hierarchical A 2
host1(config-interface)#ip policy input IP_POL2 statistics enable
host1(config-interface)#exit
```

Related Documentation

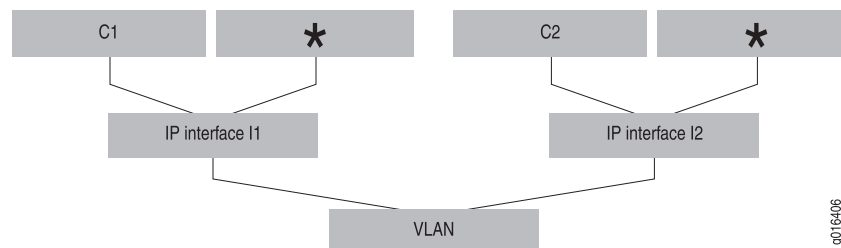
- Hierarchical Rate Limits Overview

Example: Service and User Rate-Limit Hierarchy Overlap Hierarchical Policy Configuration

In the service and user rate-limit hierarchy overlap configuration example:

- The service provider has to enforce a bandwidth limit on a video service over a VLAN and wants to limit the maximum bandwidth of each user's total traffic.
- There are two terminated sessions and their corresponding IP interfaces are I1 and I2.
- Each session contains a video flow classified by C1 and all other traffic is classified by an asterisk (*).
- All video flows over the VLAN are rate-limited to a common rate of 1Mbps.
- Each session is individually rate-limited by 2 Mbps.
- You can attach policies at interface I1-I2.

Figure 9: Interface Stack for Service and User Rate-Limit Hierarchy Overlap

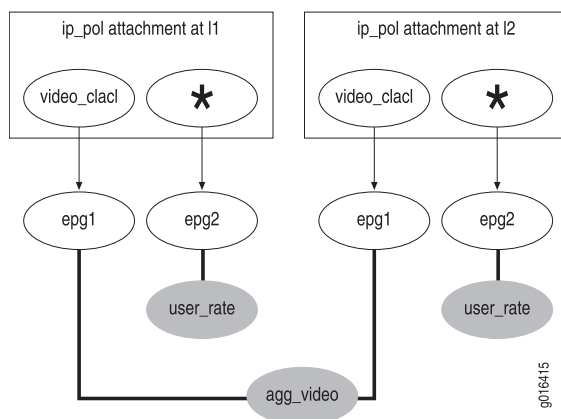


This example uses the following:

- At I1 and I2:
 - USER_RATE, Committed Rate: 2 Mbps
 - Peak Rate: 0 Mbps

- Committed Action: transmit final
- Conformed Action: drop
- Exceeded Action: drop
- Both C1 and C2 feed into a single policer with the following configuration:
 - AGG_VIDEO, Committed Rate: 1 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit conditional
 - Conformed Action: drop
 - Exceeded Action: drop

Figure 10: Service and User Rate-Limit Hierarchy Overlap Configuration



1. Create an aggregate rate limit that can be applied to each IP session. Create an external parent group to hold this rate limit.

```
host1(config)#rate-limit-profile USER_RATE two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 2000000
host1(config-rate-limit-profile)#committed-action transmit final
host1(config-rate-limit-profile)#exit
```

```
host1(config)#parent-group EPG2
host1(config-parent-group)#rate-limit-profile USER_RATE
host1(config-parent-group)#exit
```

2. Create an aggregate rate limit that can be shared across multiple video streams. Create an external parent group to hold this rate limit.

```
host1(config)#rate-limit-profile AGG_VIDEO two-rate hierarchical
host1(config-rate-limit-profile)#committed-rate 1000000
host1(config-rate-limit-profile)#committed-action transmit conditional
host1(config-rate-limit-profile)#exit
```

```
host1(config)#policy-parameter B hierarchical
host1(config-policy-parameter)#exit
```

```

host1(config)#parent-group EPG1
host1(config-parent-group)#next-parent EPG2 parameter B
host1(config-parent-group)#rate-limit-profile AGG_VIDEO
host1(config-parent-group)#exit

```

3. Create a policy list to be attached to each IP session.

```

host1(config)#ip classifier-list VIDEO_CLACL udp any any eq 4000

```

```

host1(config)#policy-parameter A hierarchical
host1(config-policy-parameter)#exit

```

```

host1(config)#ip policy-list IP_POL
host1(config-policy-list)#classifier-group VIDEO_CLACL external parent-group EPG1
parameter A
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#classifier-group * external parent-group EPG2
parameter B
host1(config-policy-list-classifier-group)#forward
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit

```

4. Attach IP_POL to each IP session. Specify the same ID for parameter A, but a different ID for parameter B.

```

host1(config)#interface fastEthernet 3/0.1
host1(config-interface)#vlan id 1
host1(config-interface)#exit

```

```

host1(config)#interface ip 3/0.1.1
host1(config-interface)#ip policy-parameter hierarchical A vlan
host1(config-interface)#ip policy-parameter hierarchical B forwarding
host1(config-interface)#ip policy input IP_POL statistics enable
host1(config-interface)#exit

```

```

host1(config)#interface ip 3/0.1.2
host1(config-interface)#ip policy-parameter hierarchical A vlan
host1(config-interface)#ip policy-parameter hierarchical B forwarding
host1(config-interface)#ip policy input IP_POL statistics enable
host1(config-interface)#exit

```

Related Documentation

- [Hierarchical Rate Limits Overview](#)

Example: Percentage-Based Hierarchical Rate-Limit Profile for External Parent Group

The following example creates rate-limit profiles with rate based on percentage and burst in milliseconds. You can create a policy using these rate-limit profiles and attach them to different interfaces using different parameter values.

1. Create a policy parameter refRlpRate.

```
host1(config)#policy-parameter refRlpRate reference-rate
host1(config-policy-parameter)#reference-rate 100000
host1(config-policy-parameter)#exit
```

2. Create a hierarchical rate-limit profile rlpData.

```
host1(config)#rate-limit-profile rlpData hierarchical
host1(config-rate-limit-profile)#committed-rate refRlpRate percentage 10
host1(config-rate-limit-profile)#peak-rate refRlpRate percentage 100
host1(config-rate-limit-profile)#exit
```

3. Associate this hierarchical rate-limit profile with the external parent group.

```
host1(config)#parent-group epg1
host1(config-parent-group)#rate-limit-profile rlpData
host1(config-parent-group)#exit
```

4. Create a hierarchical policy parameter.

```
host1(config)#policy-parameter A hierarchical
host1(config-policy-parameter)#aggregation-node forwarding
host1(config-policy-parameter)#exit
```

5. Create a policy that references the external parent group.

```
host1(config)#ip policy-list P
host1(config-policy)#classifier-group data external parent-group epg1 parameter A
host1(config-policy-classifier-group)#forward
host1(config-policy-classifier-group)#exit
host1(config-policy)#exit
```

6. Attach an IP policy P at interface atm5/0.1 by specifying a different reference-rate value.

```
host1(config)#interface atm 5/0.1
host1(config-if)#ip policy-parameter reference-rate refRlpRate 5000000
host1(config-if)#ip policy input P stats enabled
```

7. Attach an IP policy P at interface atm5/0.2 to use the default value.

```
host1(config)#interface atm 5/0.2
host1(config-if)#ip policy input P stats enabled
```

8. Display the policy list.

```
host1#show policy-list
```

```
Policy Table
```

```
-----
```

```
IP Policy P
```

```
Administrative state: enable
```

```
Reference count:      2
```

```
Classifier control list: c11, precedence 100, external parent-group
```

```
epg1 parameter A
```

```
forward
```

```
Referenced by interface(s):
```

```
ATM5/0.1 input policy, statistics disabled, virtual-router default
```

```
ATM5/0.2 input policy, statistics enabled, virtual-router default
```

```
Referenced by profile(s):
```

```
None
```

Referenced by merge policies:
None

9. Display the interface configuration to verify the reference rate (committed rate and peak rate) being different for both interface attachments (only the policy-related section of the output is shown).

```
host1#show ip interface atm 5/0.1
```

```
IP policy input P
  classifier-group data entry 1, external parent-group epg1
aggregate-node forwarding
  0 packets, 0 bytes
  forward
external parent-group epg1 aggregate-node forwarding
  rate-limit-profile rlpData
    committed rate: 500000 bps, committed burst: 8192 bytes (default)

    peak rate: 5000000 bps, peak burst: 62500 bytes (default)
    committed: 0 packets, 0 bytes, action: transmit conditional
    conformed: 0 packets, 0 bytes, action: transmit conditional
    exceeded: 0 packets, 0 bytes, action: drop
    unconditional: 0 packets, 0 bytes
    saturated: 0 packets, 0 bytes
```

```
host1#show ip interface atm 5/0.2
```

```
IP policy input P
  classifier-group data entry 1, external parent-group epg1
aggregate-node forwarding
  0 packets, 0 bytes
  forward
external parent-group epg1 aggregate-node forwarding
  rate-limit-profile rlpData
    committed rate: 10000 bps, committed burst: 8192 bytes (default)
    peak rate: 100000 bps, peak burst: 8192 bytes (default)
    committed: 0 packets, 0 bytes, action: transmit conditional
    conformed: 0 packets, 0 bytes, action: transmit conditional
    exceeded: 0 packets, 0 bytes, action: drop
    unconditional: 0 packets, 0 bytes
    saturated: 0 packets, 0 bytes
```

- Related Documentation**
- [External Parent Groups on page 3](#)
 - [Hierarchical Rate Limits Overview](#)

Example: PPP Interfaces Hierarchical Policy Configuration

Figure 11 on page 35 shows the following example:

- Two dual-stack PPP user sessions are configured over the same VLAN interface.
- Each PPP session corresponds to a dynamic user.
- Each PPP user can send a combined IPv4 and IPv6 video traffic with a maximum rate of 1 Mbps.

- One of the subscribers, PPP user1, can send a default maximum rate of 3 Mbps combined IPv4/IPv6 session traffic, whereas the other subscriber, PPP user2, can send a default maximum rate of 5 Mbps combined IPv4/IPv6 session traffic.
- I1 and I3 are interfaces where IPv4 policies are attached.
- I2 and I4 are interfaces where IPv6 policies are attached.
- PPP 1 is the PPP session of dynamic subscriber 1. I1 and I2 belong to this subscriber.
- PPP 2 is the PPP session of dynamic subscriber 2. I3 and I4 belong to this subscriber.
- vlan denotes the VLAN interface over which subscribers are configured.

This example uses the following:

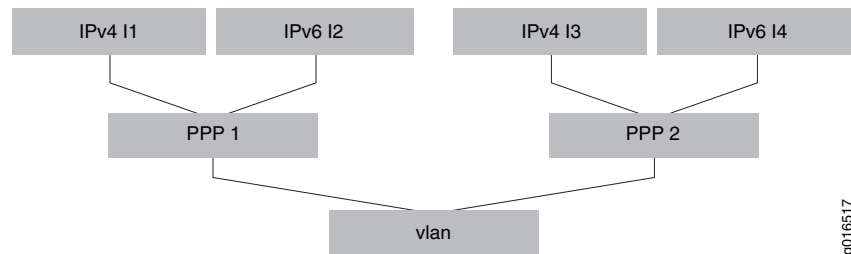
- At I1 and I3:
 - Classified Video Flow. VIDEO_RATE, Committed Rate: 1 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit unconditional
 - Conformed Action: drop
 - Exceeded Action: drop
- At I2 and I4:
 - Classified Video Flow. VIDEO_RATE, Committed Rate: 1 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit unconditional
 - Conformed Action: drop
 - Exceeded Action: drop

All classified video flow policers over each PPP interface feed into a single policer with the following configuration:

- At I1 and I3:
 - All Flows. SESSION_RATE, Committed Rate: 3 Mbps
 - Peak Rate: 0 Mbps
 - Committed Action: transmit conditional
 - Conformed Action: drop
 - Exceeded Action: drop
- At I2 and I4:

- All Flows. SESSION_RATE, Committed Rate: 5Mbps
- Peak Rate: 0 Mbps
- Committed Action: transmit conditional
- Conformed Action: drop
- Exceeded Action: drop

Figure 11: Interface Stack for Hierarchical Policy Configuration



1. Create a hierarchical policy parameter list for PPP interfaces.

```
host1(config)#policy-parameter P1_PPP hierarchical
host1(config-policy-parameter)#exit
```

2. Create a reference rate parameter to be used in external parent groups associated with PPP sessions.

```
host1(config)#policy-parameter sessionRlpRate reference-rate
host1(config-policy-parameter)#reference-rate 3000000
host1(config-policy-parameter)#exit
```

3. Create an aggregate session rate-limit (using reference-rate) that can be shared between IPv4 and IPv6 interfaces of each PPP session. Create an external parent group to hold this rate-limit.

```
host(config)#rate-limit-profile SESSION_AGG two-rate hierarchical
host(config-rate-limit-profile)#committed-rate sessionRlpRate percent 100
host(config-rate-limit-profile)#committed-action transmit conditional
host(config-rate-limit-profile)#exit
```

```
host(config)#parent-group EPG_SESSION
host(config-parent-group)#rate-limit-profile SESSION_AGG
host(config-parent-group)#exit
```

4. Create an aggregate video rate-limit that can be shared between IPv4 and IPv6 interfaces of each PPP session. Create an external parent group to hold this rate-limit.

```
host(config)#rate-limit-profile VIDEO_AGG two-rate hierarchical
host(config-rate-limit-profile)#committed-rate 1000000
host(config-rate-limit-profile)#committed-action transmit unconditional
host(config-rate-limit-profile)#exit
```

```
host(config)#parent-group EPG_VIDEO
host1(config-parent-group)#next-parent EPG_SESSION parameter P1_PPP
host(config-parent-group)#rate-limit-profile VIDEO_AGG
```

```
host(config-parent-group)#exit
```

5. Create IPv4/ IPv6 policy-lists to be attached to all PPP sessions.

```
host(config)#ip policy-list IP_POL1
host(config-policy-list)#classifier-group VIDEO_CLACL_V4 external parent-group
  EPG_VIDEO parameter P1_PPP
host(config-policy-list-classifier-group)#forward
host(config-policy-list-classifier-group)#exit
host(config-policy-list)#classifier-group * external parent-group EPG_SESSION
  parameter P1_PPP
host(config-policy-list-classifier-group)#forward
host(config-policy-list-classifier-group)#exit
host(config-policy-list)#exit
```

```
host(config)#ipv6 policy-list IP_POL2
host(config-policy-list)#classifier-group VIDEO_CLACL_V6 external parent-group
  EPG_VIDEO parameter P1_PPP
host(config-policy-list-classifier-group)#forward
host(config-policy-list-classifier-group)#exit
host(config-policy-list)#classifier-group * external parent-group EPG_SESSION
  parameter P1_PPP
host(config-policy-list-classifier-group)#forward
host(config-policy-list-classifier-group)#exit
host(config-policy-list)#exit
```

6. Specify the policy parameter and attachments through the profile.

```
host(config)#profile PPPOE_PROF1
host(config-profile)#ip policy-parameter hierarchical P1_PPP ppp-interface
host(config-profile)#ip policy input IP_POL1 sta enabled merge
host(config-profile)#ipv6 policy-parameter hierarchical P1_PPP ppp-interface
host(config-profile)#ipv6 policy input IP_POL2 sta enabled merge
host(config-profile)#exit
```

7. Use another profile for the second subscriber to specify a different session rate of 5 Mbps by overriding the default rate of 3 Mbps , and specify the policy parameter through the profile.

```
host(config)#profile PPPOE_PROF2
host(config-profile)#ip policy-parameter hierarchical P1_PPP ppp-interface
host(config-profile)#ip policy input IP_POL1 sta enabled merge
host(config-profile)#ipv6 policy-parameter hierarchical P1_PPP ppp-interface
host(config-profile)#ipv6 policy input IP_POL2 sta enabled merge
host(config-profile)#ip policy-parameter reference-rate sessionRlpRate 5000000
host(config-profile)#ipv6 policy-parameter reference-rate sessionRlpRate 5000000
host(config-profile)#exit
```

8. Configure the VLAN, PPPoE, and PPP encapsulation and specify unique profile to use for each PPP user.

```
host(config)#interface gig 2/1/0.1
host(config-interface)#vlan id 1
host(config-interface)#encapsulation pppoe
host(config)#interface gig 2/1/0.1.1
host(config-interface)#encapsulation ppp
host(config-interface)#profile PPPOE_PROF1
host(config)#interface gig 2/1/0.1.2
```



```
host(config-interface)#encapsulation ppp
host(config-interface)#profile PPPOE_PROF2
host(config-interface)#exit
```



NOTE: You can optionally specify an aggregation node for a policy parameter during its definition in Global Configuration mode. This example configures parameters at the interface level. However, you can also configure these same settings at the global level, without defining them at the interface or profile level. This feature supports both these methods of configurations.

Related Documentation

- [Hierarchical Rate Limits Overview](#)

PART 3

Administration

- [Monitoring Tasks on page 41](#)

Monitoring Tasks

- [Monitoring External Parent Groups on page 41](#)

Monitoring External Parent Groups

Purpose Display information about external parent groups.

Action To display information about external parent groups:

host1#show parent-group name EPG2

Parent Group Table

Parent Group EPG2
Reference count: 1
Rate limit profile: VLAN_RATE
Next parent group: EPG1 parameter C

Referenced by policies:
P1

Meaning [Table 4 on page 41](#) lists the **show parent-group** command output fields.

Table 4: show parent-group Output Fields

Field Name	Field Description
Reference count	Number of references within policies and other external parent groups.
Rate limit profile	Name of hierarchical rate limit profile.
Next parent group	Name of the next parent group and parameter.
Referenced by policies	List of policies where this parent group is referenced.
Referenced by parent groups	List of parent groups where the parent group is referenced.

Related Documentation

- [show parent-group](#)

PART 4

Index

- [Index on page 45](#)

Index

C

conventions	
notice icons.....	ix
text and syntax.....	x
customer support.....	xi
contacting JTAC.....	xi

D

documentation set	
comments on.....	xi

E

external parent groups.....	3
monitoring.....	41
percentage-based hierarchy.....	31
rate-limit profile.....	31

H

hierarchical aggregation nodes.....	4
hierarchical policies	
aggregate rate limits.....	23
arbitrary interface groups.....	26
external parent groups.....	3
L2TP.....	20
nonvoice traffic.....	23
policy parameters.....	11
PPP interfaces.....	33
Profile configuration.....	5
RADIUS configuration.....	5
service rate-limit.....	29
user rate-limit.....	29
VLAN rate limit.....	17
hierarchical policing	
configuration.....	9
for interface groups.....	3

M

manuals	
comments on.....	xi

N

notice icons.....	ix
-------------------	----

S

Service Manager	
interface profiles.....	5
show commands	
show parent-group.....	41
support, technical	See technical support

T

technical support	
contacting JTAC.....	xi
text and syntax conventions.....	x

